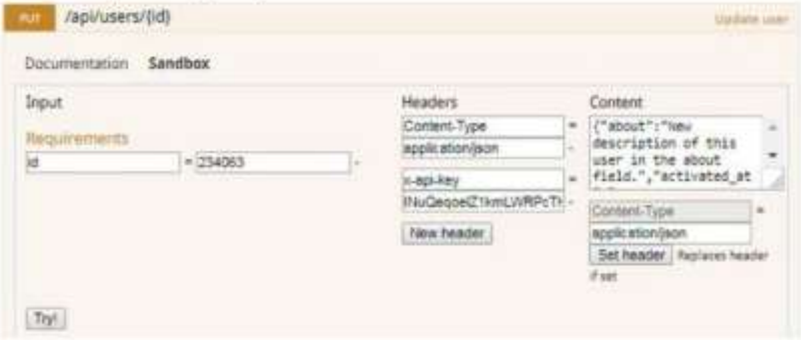
The PUT /api/users/{id} Request



id = 234063

Content-Type = application/json

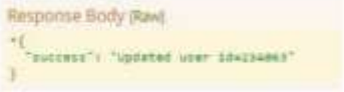
x-api-key = lNuQeqoelZ1kmLWRPcT

```
{"about":"New
description of this
user in the about
field.","activated_at
```

Content-Type = application/json

If the request is successful the **Response Body** indicates the user record was updated.

Response body



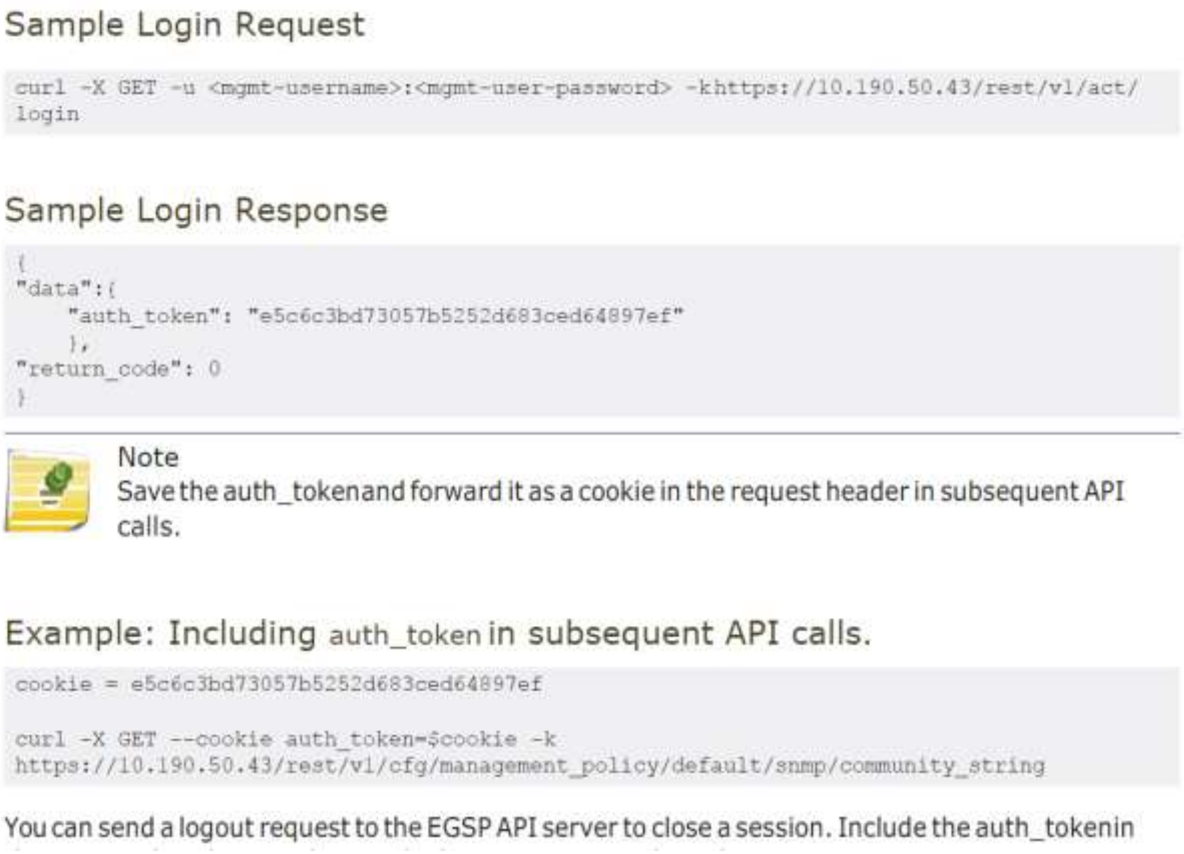
```
▾{
  "success": "Updated user id=234063"
}
```

API Response Codes

The EGSP API returns standard HTTP status codes in addition to JSON-based error codes and messages in the response body.

Table 3: HTTP Response Status Codes

Code	Description
200 OK	The request was successful
201 Created	The resource was created successfully
204 No Content	Success with no response body
400 Bad Request	The operation failed because the request is syntactically incorrect or violated schema
401 Unauthorized	The authentication credentials are invalid or the user is not authorized to use the API
404 Not Found	The server did not find the specified resource that matches the request URL
405 Method Not Allowed	The API does not support the requested HTTP method



Sample Login Request

```
curl -X GET -u <mgmt-username>:<mgmt-user-password> -khttps://10.190.50.43/rest/v1/act/
login
```

Sample Login Response

```
{
"data":{
    "auth_token": "e5c6c3bd73057b5252d683ced64897ef"
    },
"return_code": 0
}
```

Note
Save the auth_tokenand forward it as a cookie in the request header in subsequent API calls.

Example: Including auth_token in subsequent API calls.

```
cookie = e5c6c3bd73057b5252d683ced64897ef

curl -X GET --cookie auth_token=$cookie -k
https://10.190.50.43/rest/v1/cfg/management_policy/default/snmp/community_string
```

You can send a logout request to the EGSP API server to close a session. Include the auth_tokenin

Delete an Asset

To delete a specific VLAN from a WLAN:

1 Log in to the REST API server using valid management user credentials.

Note
You must forward the `auth_token` as a cookie with each API call.

2 Use the DELETE method to access the /cfg/wlan/ URI and delete VLAN 101 from test-1. Sample

Request

```
curl -X DELETE --cookie auth_token=$cookie https://10.190.50.43/rest/v1/
cfg/wlan/test-1/vlans/101
```

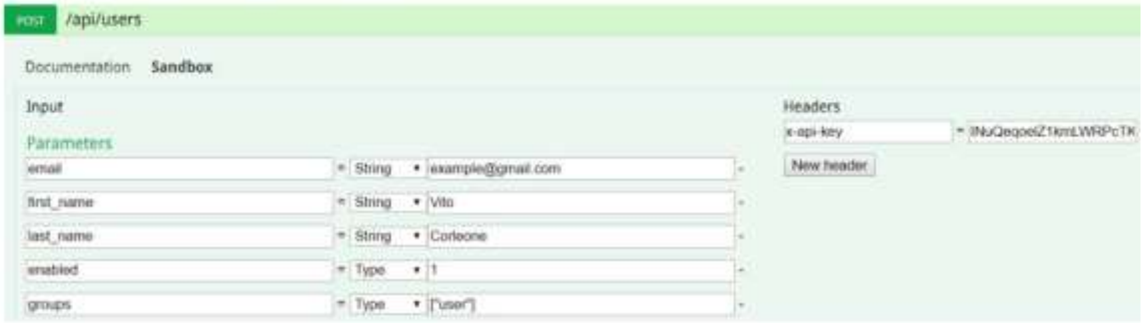
Sample Response (200 OK)

```
{
"return_code": 0
}
```

1.10 Risks and Mitigation

Risk	Mitigation
Invoices with marks and cuts in the images giving wrong output	Ensuring clean and mark less invoices are uploaded for data extraction Setting up a minimum confidence threshold in the lambda function to ensure if the API has low confidence in certain data value then that invoice is flagged and saved in failure
Data from the DynamoDB can either be taken or tampered	Encrypting the DynamoDB taken and using the AWS KMS(key management service) to save the keys. This provides an additional layer of data protection by securing your data from unauthorized access to the underlying storage .
Data of invoices saved in s3 is not protected	IAM roles should be assigned to users and applications that require Amazon s3 access
Lack of support from business, existing partner	Manage project timelines through regular governance agreed mutually by partner and customer at the time of project initiation. Escalate in timely fashion in case of any issues/risks
Lack of testing assets and tools to validate the implementations	customer to provide the input & output for comparison testing from their existing application
Technical issues while executing the textract API	AWS Business support plan will be purchased

The POST /api/users/ Request



/api/users

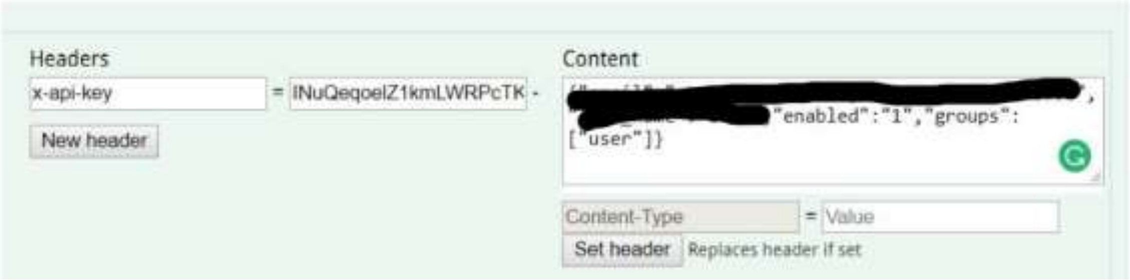
email	= String	example@gmail.com
first_name	= String	Vito
last_name	= String	Corleone
enabled	= Type	1
groups	= Type	["user"]

x-api-key = INuQeqoelZ1kmLWRPcTK

3. The **Response Body** shows the JSON results.

Note that the **user_id** field uniquely identifies a user. Make a note of this value to use for identifying the user in later examples.

Note: If the response header is **"400 Bad Request"** try sending the request as a JSON through the Content Textarea



x-api-key = INuQeqoelZ1kmLWRPcTK

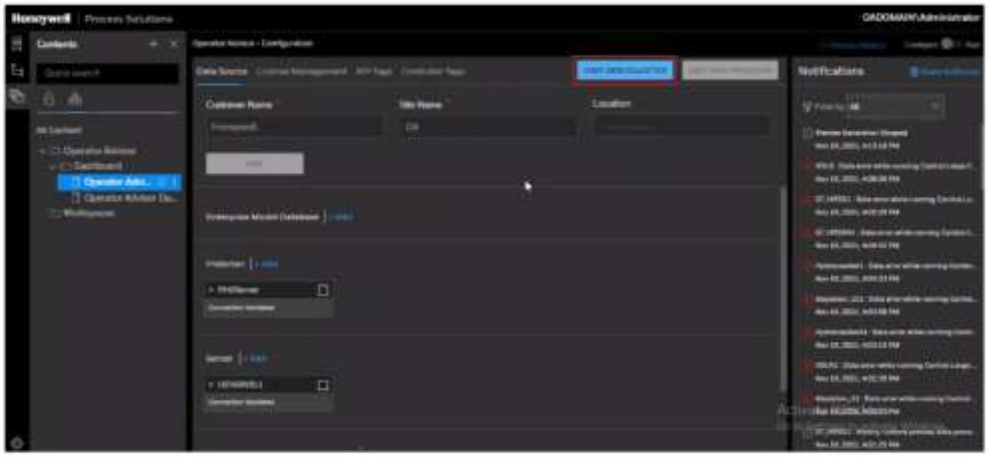
```
[redacted] "enabled":"1","groups":
["user"]}
```

Content-Type = Value

Start Data Collection

> **NOTE:** This option is enabled only if all the data source connections are successfully validated.

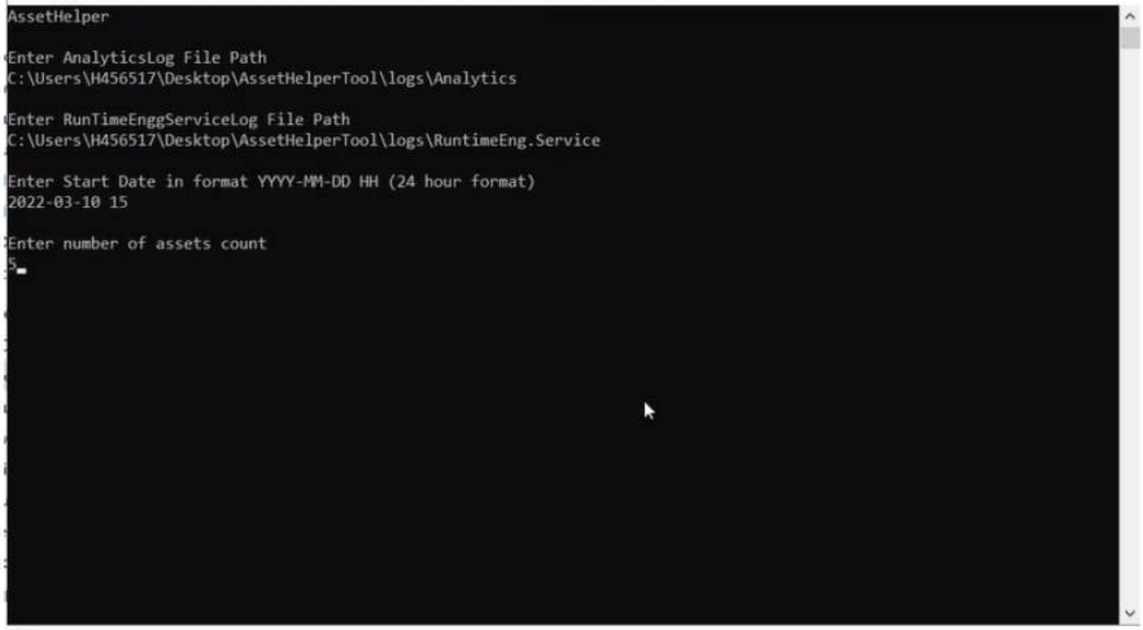
1. After providing all the required details and all the connections are validated under **Data Source**, click **START DATA COLLECTION**.



C:\ProgramData\Honeywell\HaloOperatorAdvisor\Logs\Application\RuntimeEng.Service

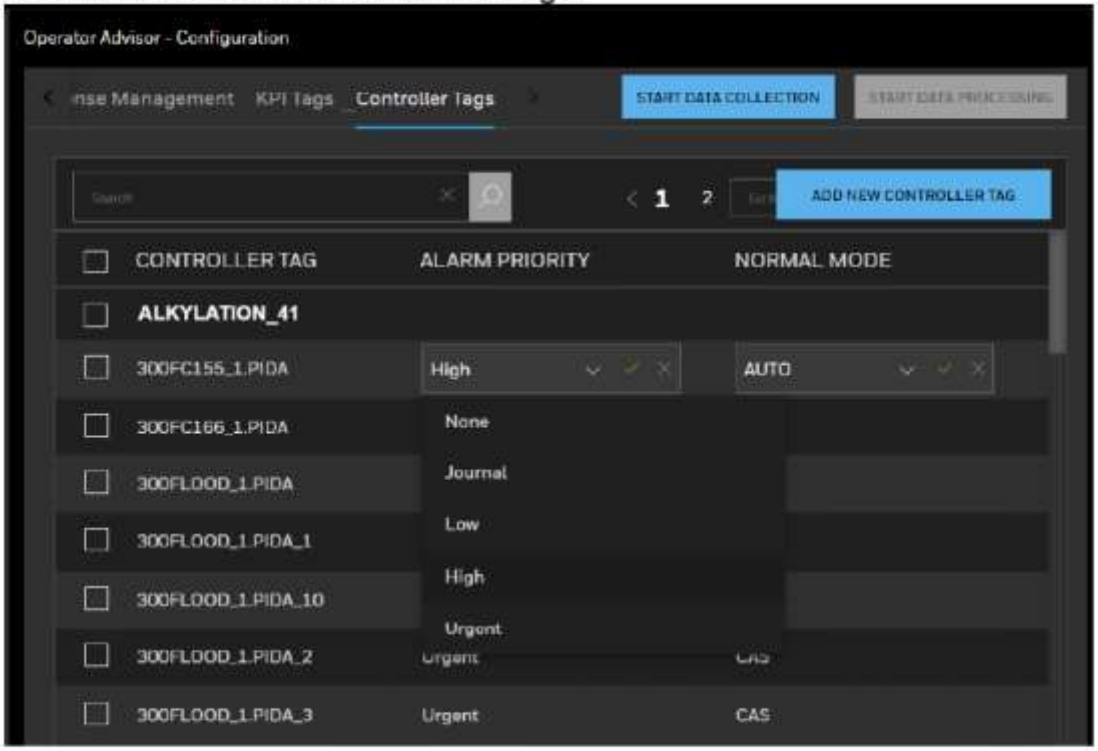
The AssetHelpertool is available in the folder
C:\ProgramData\Honeywell\HaloOperatorAdvisor\Services\Tools

1. Double-click on *Honeywell.Halo.OA.AssetHelper.exe* file.
2. Enter AnalyticsLog File Path, RuntimeEnggServiceLog File Path, Start Time (actual Preview start time) in YYYY-MM-DD HH format (24 hour format), and number of assets count (Integer).

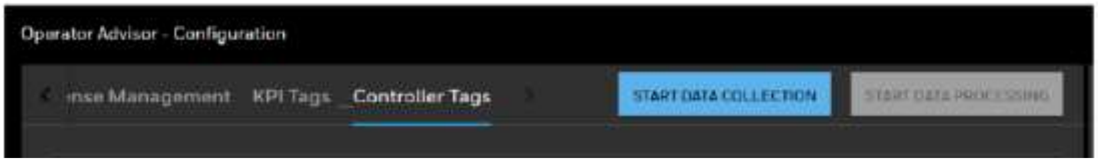


```
AssetHelper

Enter AnalyticsLog File Path
C:\Users\H456517\Desktop\AssetHelperTool\logs\Analytics

Enter RunTimeEnggServiceLog File Path
C:\Users\H456517\Desktop\AssetHelperTool\logs\RuntimeEng.Service

Enter Start Date in format YYYY-MM-DD HH (24 hour format)
2022-03-10 15

Enter number of assets count
5
```

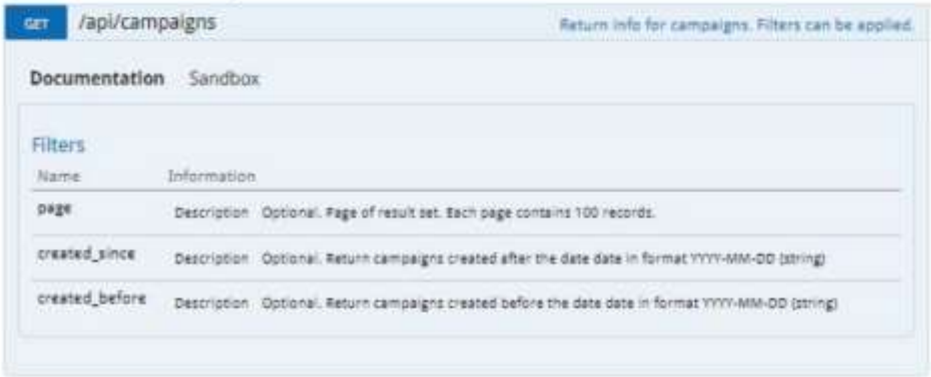
7. You can also make changes to **ALARM PRIORITY** and **NORMAL MODE** under **Controller Tags**.



□	CONTROLLER TAG	ALARM PRIORITY	NORMAL MODE
□	**ALKYLATION_41**		
□	300FC155_1.PIDA	High	AUTO
□	300FC166_1.PIDA		
□	300FLOOD_1.PIDA		
□	300FLOOD_1.PIDA_1		
□	300FLOOD_1.PIDA_10		
□	300FLOOD_1.PIDA_2	Urgent	CAS
□	300FLOOD_1.PIDA_3	Urgent	CAS



An API Reference Page



/api/campaigns

Return info for campaigns. Filters can be applied.

Filters

Name	Information
page	Description Optional. Page of result set. Each page contains 100 records.
created_since	Description Optional. Return campaigns created after the date date in format YYYY-MM-DD (string)
created_before	Description Optional. Return campaigns created before the date date in format YYYY-MM-DD (string)

Note, for a **GET /api/campaigns/** request the **page** parameter indicates which set of results to return. The default **page** value is 1 representing the first 100 results.

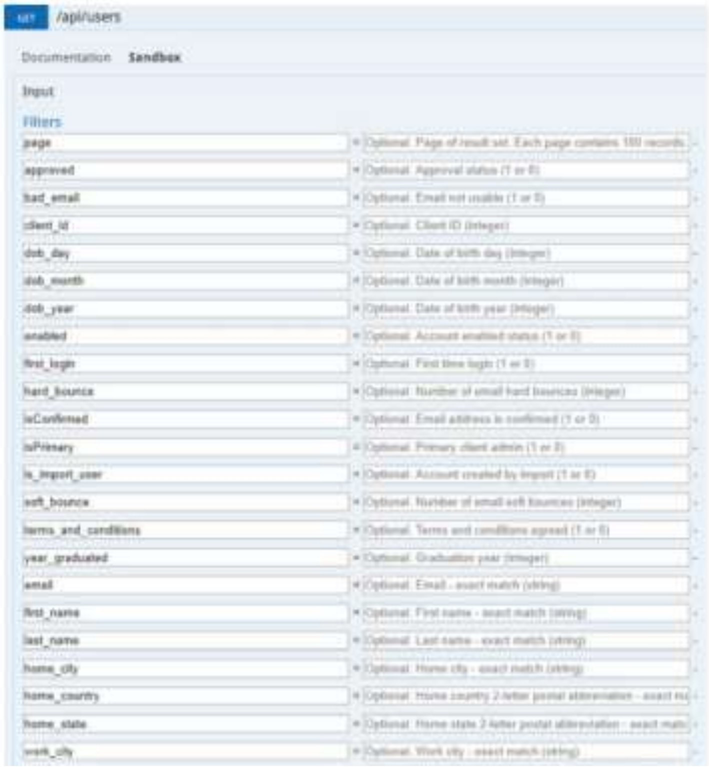
A page represents up to 100 results returned in a JSON array.

2. Click **Sandbox** to display a form for entering values and trying the request.

3. Enter your API key in an HTTP request header.
    1. Use the header name **x-api-key**.
    2. Use the value obtained from your 360Alumni representative.

The following steps walk you through using filter parameters to get data on users.

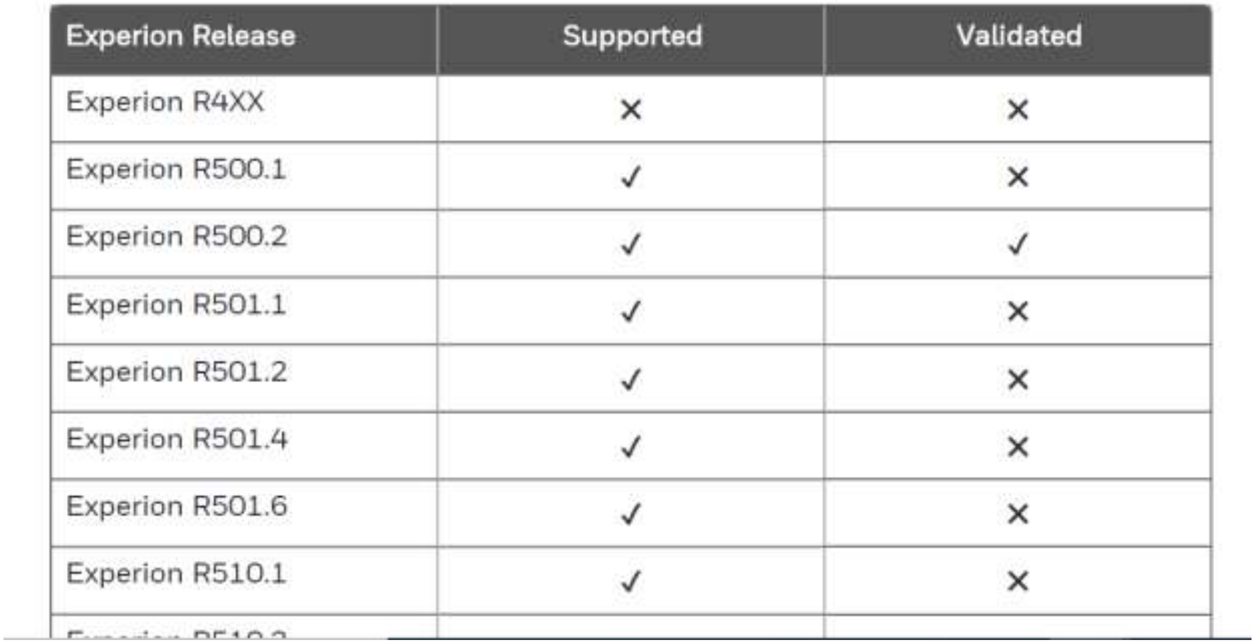
1. Click the **GET /api/users/** method.
2. Click **Sandbox** to display the form for entering values and trying requests.
3. Note there are a great number of optional parameters available to filter the results.



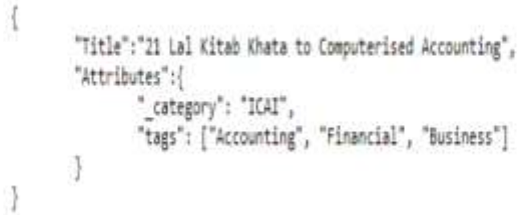
page	Optional. Page of result set. Each page contains 100 records
approved	Optional. Approval status (1 or 0)
bad_email	Optional. Email not usable (1 or 0)
client_id	Optional. Client ID (integer)
dob_day	Optional. Date of birth day (integer)
dob_month	Optional. Date of birth month (integer)
dob_year	Optional. Date of birth year (integer)
enabled	Optional. Account enabled status (1 or 0)
first_login	Optional. First time login (1 or 0)
hard_bounce	Optional. Number of email hard bounces (integer)
isConfirmed	Optional. Email address is confirmed (1 or 0)
isPrimary	Optional. Primary client admin (1 or 0)
is_import_user	Optional. Account created by import (1 or 0)
soft_bounce	Optional. Number of email soft bounces (integer)
terms_and_conditions	Optional. Terms and conditions agreed (1 or 0)
year_graduated	Optional. Graduation year (integer)
email	Optional. Email - exact match (string)
first_name	Optional. First name - exact match (string)
last_name	Optional. Last name - exact match (string)
home_city	Optional. Home city - exact match (string)
home_country	Optional. Home country 2-letter postal abbreviation - exact ma
home_state	Optional. Home state 2-letter postal abbreviation - exact matc
work_city	Optional. Work city - exact match (string)

7 COMPATIBILITY MATRIX

The following tables describes the compatibiliy matrix for HALO OA R100.1 release.

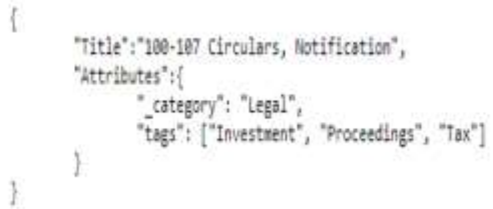


Experion Release	Supported	Validated
Experion R4XX	×	×
Experion R500.1	✓	×
Experion R500.2	✓	✓
Experion R501.1	✓	×
Experion R501.2	✓	×
Experion R501.4	✓	×
Experion R501.6	✓	×
Experion R510.1	✓	×
Experion R510.2		



```
{
    "Title":"21 Lal Kitab Khata to Computerised Accounting",
    "Attributes":{
            "_category": "ICAI",
            "tags": ["Accounting", "Financial", "Business"]
    }
}
```

Fig. Metadata file for category 1

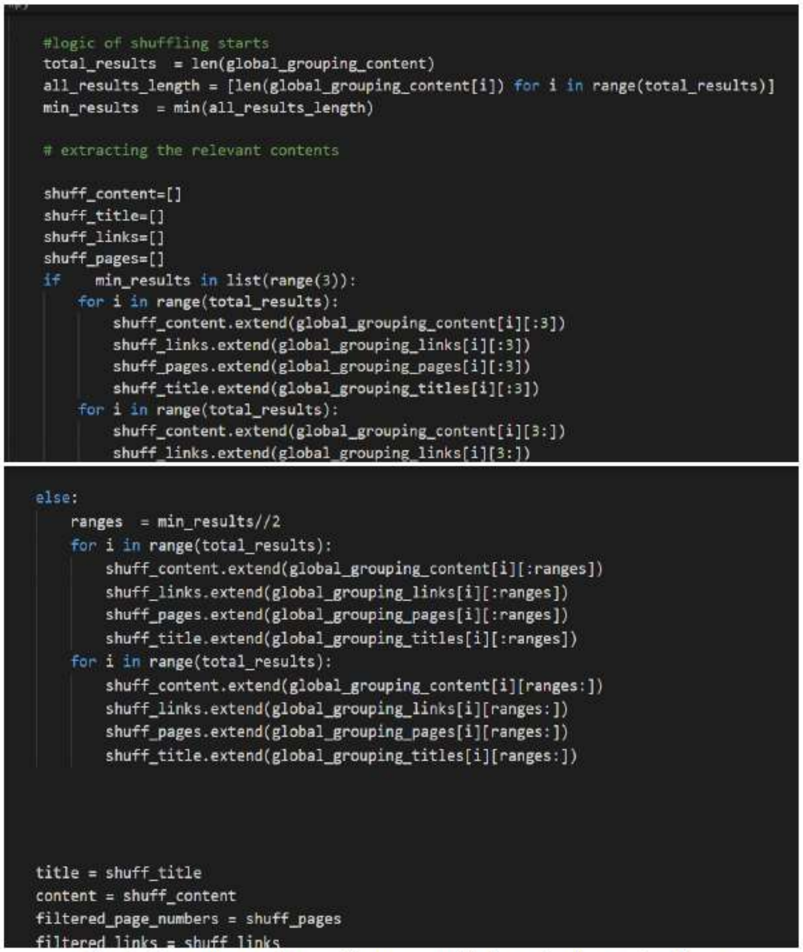


```
{
    "Title":"100-107 Circulars, Notification",
    "Attributes":{
            "_category": "Legal",
            "tags": ["Investment", "Proceedings", "Tax"]
    }
}
```

Fig. Metadata file for category 2

Category 1- Legal
Tags for category 1- Investment, Proceedings, Tax
Document set- 96-99 Legal Decisions.pdf, 100-107 Circulars, Notifications.pdf

Category 2- ICAI
Tags for category 2- Accounting, Financial, Business
Document set- 26 Manual verification to Audit tools.pdf, 53 Financial Reporting to Integrated Reporting.pdf, 21 Lal Kitab Khata to Computerised Accounting.pdf



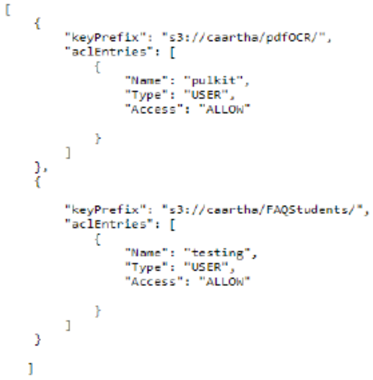
```
#logic of shuffling starts
total_results  = len(global_grouping_content)
all_results_length = [len(global_grouping_content[i]) for i in range(total_results)]
min_results  = min(all_results_length)

# extracting the relevant contents

shuff_content=[]
shuff_title=[]
shuff_links=[]
shuff_pages=[]
if    min_results in list(range(3)):
    for i in range(total_results):
        shuff_content.extend(global_grouping_content[i][:3])
        shuff_links.extend(global_grouping_links[i][:3])
        shuff_pages.extend(global_grouping_pages[i][:3])
        shuff_title.extend(global_grouping_titles[i][:3])
    for i in range(total_results):
        shuff_content.extend(global_grouping_content[i][3:])
        shuff_links.extend(global_grouping_links[i][3:])
```

```
else:
    ranges  = min_results//2
    for i in range(total_results):
        shuff_content.extend(global_grouping_content[i][:ranges])
        shuff_links.extend(global_grouping_links[i][:ranges])
        shuff_pages.extend(global_grouping_pages[i][:ranges])
        shuff_title.extend(global_grouping_titles[i][:ranges])
    for i in range(total_results):
        shuff_content.extend(global_grouping_content[i][ranges:])
        shuff_links.extend(global_grouping_links[i][ranges:])
        shuff_pages.extend(global_grouping_pages[i][ranges:])
        shuff_title.extend(global_grouping_titles[i][ranges:])



title = shuff_title
content = shuff_content
filtered_page_numbers = shuff_pages
filtered_links = shuff_links
```

Fig 4. Search results ranking on multiple selections at a time

7. API Gateway is setup for frontend backend interaction/ Rest API which calls a Lambda function. Basically, an API Gateway endpoint is required that is called by the client application.

- For FAQ file format, choose JSON file.
- For S3, browse Amazon S3 to find the Student FAQ folder
- Choose the custom CSV file.
- For IAM role, choose Create a new role to allow Amazon Kendra to access your S3 bucket.
- For Role name, enter a name and choose Add.



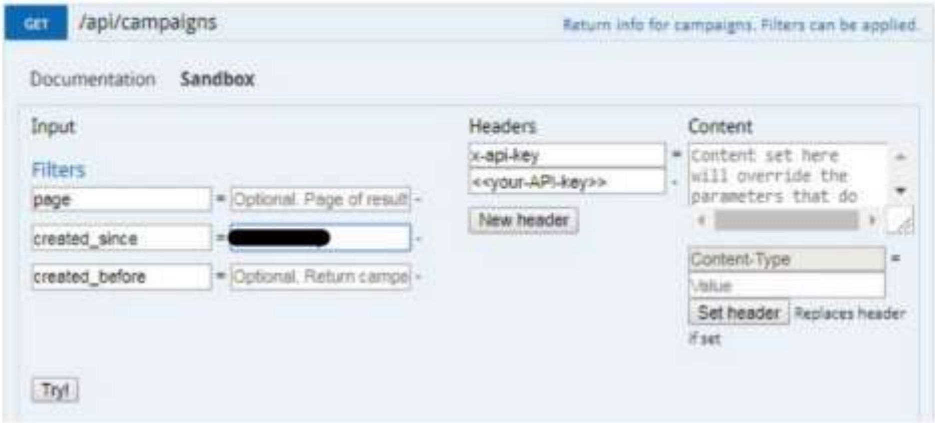
```
[
    {
        "keyPrefix": "s3://caartha/pdfOCR/",
        "aclEntries": [
            {
                "Name": "pulkit",
                "Type": "USER",
                "Access": "ALLOW"

            }
        ]
    },
    {

        "keyPrefix": "s3://caartha/FAQStudents/",
        "aclEntries": [
            {
                "Name": "testing",
                "Type": "USER",
                "Access": "ALLOW"

            }
        ]
    }

   ]
```

Fig 3. ACL config.json file

4. We have controlled access to documents in an S3 data source using a configuration file. We specify the file in the console, the configuration file contains a JSON structure that identifies an S3

2. Click **Sandbox** to display the form for entering values and trying the request. For this example we'll narrow the results to those campaigns created since [redacted]

A. Enter your API key in an HTTP request header.
B. Enter the value [redacted] for the **created_since** parameter.
C. Click **Try!** to execute the API request.



page = Optional. Page of result

created_since = [redacted]

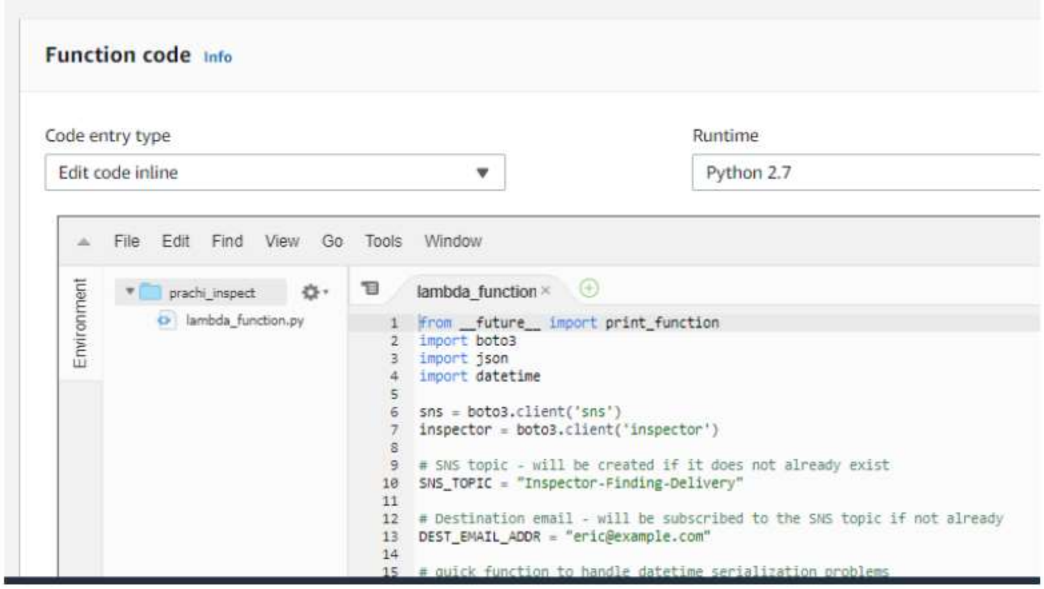
created_before = Optional. Return campa

x-api-key = <<your-API-key>>

Content set here will override the parameters that do

Content-Type = Value

3. The **Response Body** shows the JSON results.
Note the values for the **createdAt** field are more recent than the value input for **created_since.**



Function code

Code entry type: Edit code inline

Runtime: Python 2.7

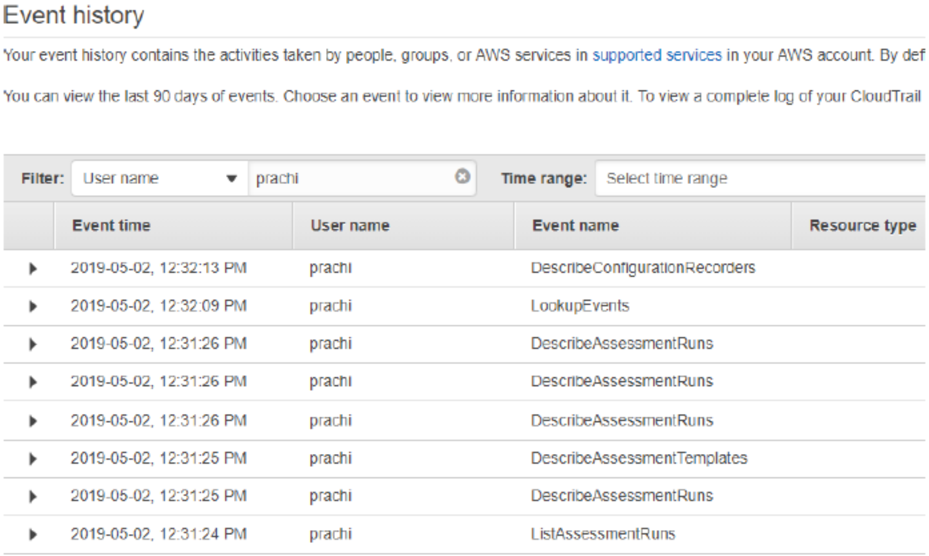
```python
from __future__ import print_function
import boto3
import json
import datetime

sns = boto3.client('sns')
inspector = boto3.client('inspector')

# SNS topic - will be created if it does not already exist
SNS_TOPIC = "Inspector-Finding-Delivery"

# Destination email - will be subscribed to the SNS topic if not already
DEST_EMAIL_ADDR = "eric@example.com"

# quick function to handle datetime serialization problems
```

Figure 10. Lambda for automated updation

2) Configure an Amazon Inspector assessment template to post finding notifications to the SNS topic:

An *assessment template* is a configuration that tells Amazon Inspector how to construct a specific security evaluation. For example, an assessment template can tell Amazon Inspector which EC2 instances to target and which rules packages to evaluate. You can configure a actions taken by a user, role, or an AWS service in Amazon Inspector. CloudTrail captures all API calls for Amazon Inspector as events, including calls from the Amazon Inspector console and code calls to the Amazon Inspector API operations.

The major difference noticed between CloudWatch and CloudTrail monitoring is that Cloudwatch logs focus on what is happening, which resources and services are being used. Whereas CloudTrail focusses on revealing who did the activity and when was it done.



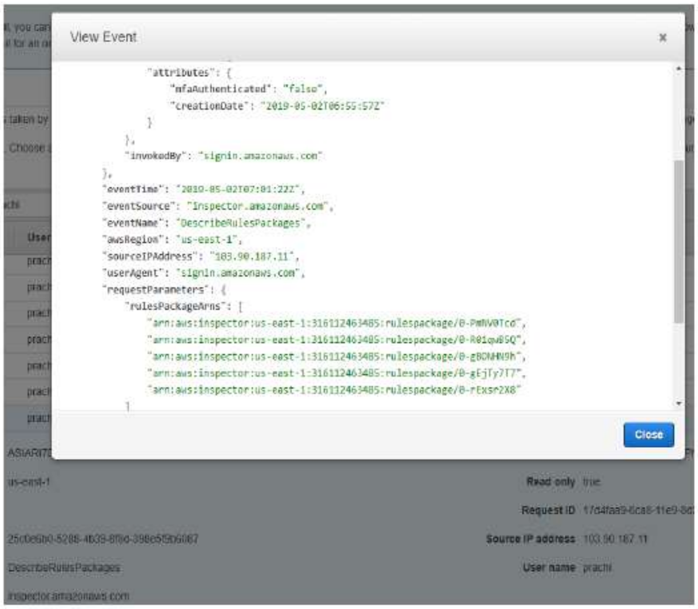
Event history

Your event history contains the activities taken by people, groups, or AWS services in supported services in your AWS account. By def

You can view the last 90 days of events. Choose an event to view more information about it. To view a complete log of your CloudTrail

Filter: User name ▼ prachi ⊗ Time range: Select time range

	Event time	User name	Event name	Resource type
▸	2019-05-02, 12:32:13 PM	prachi	DescribeConfigurationRecorders	
▸	2019-05-02, 12:32:09 PM	prachi	LookupEvents	
▸	2019-05-02, 12:31:26 PM	prachi	DescribeAssessmentRuns	
▸	2019-05-02, 12:31:26 PM	prachi	DescribeAssessmentRuns	
▸	2019-05-02, 12:31:26 PM	prachi	DescribeAssessmentRuns	
▸	2019-05-02, 12:31:25 PM	prachi	DescribeAssessmentTemplates	
▸	2019-05-02, 12:31:25 PM	prachi	DescribeAssessmentRuns	
▸	2019-05-02, 12:31:24 PM	prachi	ListAssessmentRuns	



```
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2019-05-02T06:55:57Z"
            }
        },
        "invokedBy": "signin.amazonaws.com"
    },
    "eventTime": "2019-05-02T07:01:22Z",
    "eventSource": "inspector.amazonaws.com",
    "eventName": "DescribeRulesPackages",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "103.90.187.11",
    "userAgent": "signin.amazonaws.com",
    "requestParameters": {
        "rulesPackageArns": [
            "arn:aws:inspector:us-east-1:316112463485:rulespackage/0-PmNV0Tcd",
            "arn:aws:inspector:us-east-1:316112463485:rulespackage/0-R01qwB5Q",
            "arn:aws:inspector:us-east-1:316112463485:rulespackage/0-gBONHN9h",
            "arn:aws:inspector:us-east-1:316112463485:rulespackage/0-gEjTy7T7",
            "arn:aws:inspector:us-east-1:316112463485:rulespackage/0-rExsr2X8"
        ]
```

us-east-1 | Read only true

Request ID 17d4faa9-6ca8-11e9-8d

25c0e6b0-5288-4b39-8f8d-398e55b6087 | Source IP address 103.90.187.11

DescribeRulesPackages | User name prachi

inspector.amazonaws.com

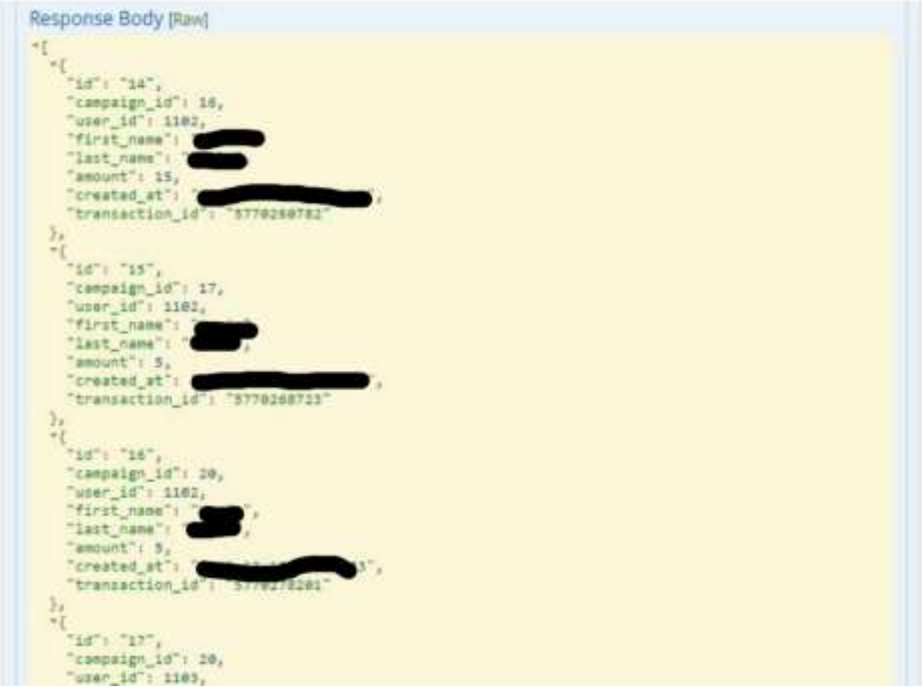
Figure 7. CloudTrail event triggered details

6. Report findings and Remediation

The reports generated were studied and the remediations were segregated and proceeded as per below priorities:

Priority 1: Critical Risk Profile and can be addressed Quick in Time

- The **created_at** field determines the results of a **GET /api/**[redacted] request if you use the [redacted] filter parameters.



Response Body [Raw]

```
-[
  -{
    "id": "14",
    "campaign_id": 16,
    "user_id": 1102,
    "first_name": [redacted]
    "last_name": [redacted]
    "amount": 15,
    "created_at": [redacted],
    "transaction_id": "5770260782"
  },
  -{
    "id": "15",
    "campaign_id": 17,
    "user_id": 1102,
    "first_name": [redacted]
    "last_name": [redacted],
    "amount": 5,
    "created_at": [redacted],
    "transaction_id": "5770268723"
  },
  -{
    "id": "16",
    "campaign_id": 20,
    "user_id": 1102,
    "first_name": [redacted]",
    "last_name": [redacted],
    "amount": 5,
    "created_at": [redacted]3",
    "transaction_id": [redacted]"
  },
  -{
    "id": "17",
    "campaign_id": 20,
    "user_id": 1103,
```

4. Monitoring Amazon Inspector Using Amazon CloudWatch

The Amazon Inspector namespace includes the following metrics. And can be monitored for real-time metrics using Amazon CloudWatch, which collects and processes raw data into readable. By default, Amazon Inspector sends metric data to CloudWatch in 5-minute periods. And can be used with the AWS Management Console, the AWS CLI, or an API to view the metrics that Amazon Inspector sends to CloudWatch. Here, console is used.

1) AssessmentTargetARN metrics:

Metric	Description
TotalMatchingAgents	Number of agents that match this target
TotalHealthyAgents	Number of agents that match this target that are healthy
TotalAssessmentRuns	Number of assessment runs for this target
TotalAssessmentRunFindings	Number of findings for this target

2) AssessmentTemplateARN metrics:

Metric	Description
TotalMatchingAgents	Number of agents that match this template
TotalHealthyAgents	Number of agents that match this template that are healthy

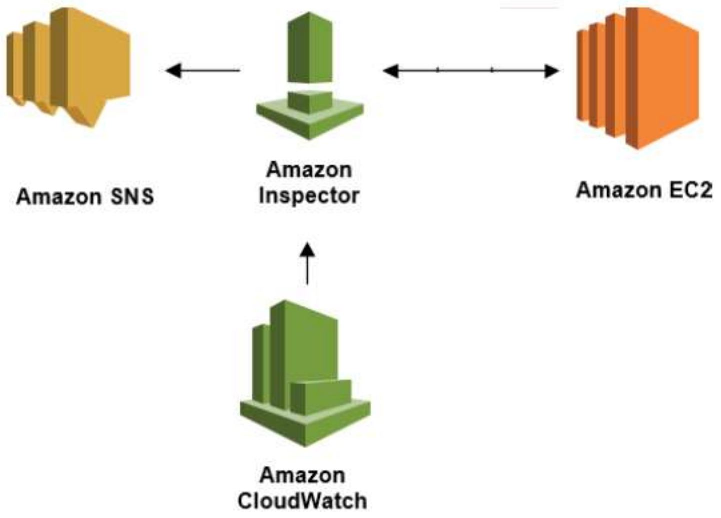
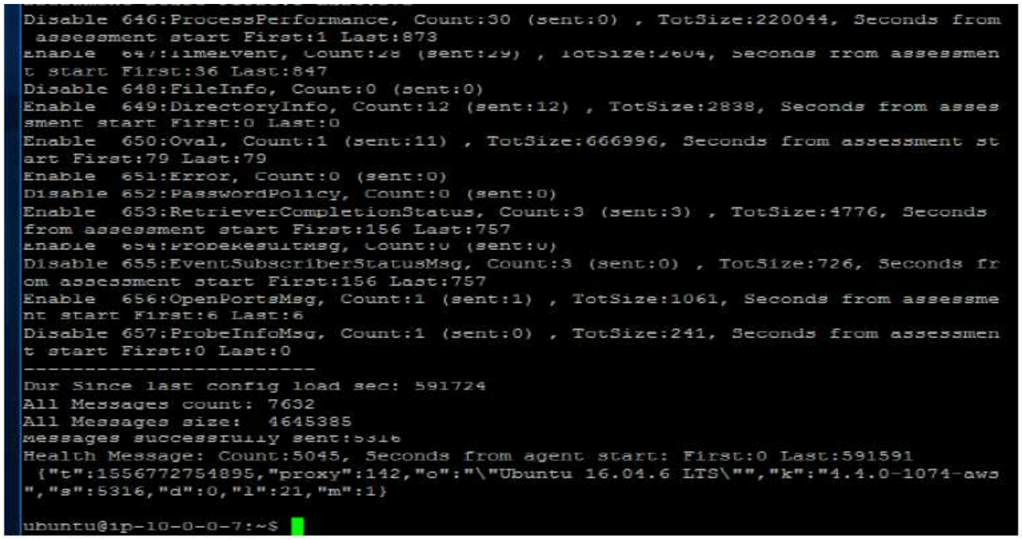


Figure 1. Architectural Overview

2. Installing SSM and Inspector agent on the EC2 instance

Amazon Inspector uses assessment targets to designate the AWS resources to evaluate and to create an assessment target and install a Systems Manager Agent and inspector agent on the EC2 instance using run command which will be restricted otherwise. To verify that the agent is installed and running, sign in to your EC2 instance and run the following command:

```
sudo /opt/aws/awsagent/bin/awsagent status
```



```
Disable 646:ProcessPerformance, Count:30 (sent:0) , TotSize:220044, Seconds from
 assessment start First:1 Last:873
Enable  647:TimeEvent, Count:28 (sent:29) , TotSize:2604, Seconds from assessmen
t start First:36 Last:847
Disable 648:FileInfo, Count:0 (sent:0)
Enable  649:DirectoryInfo, Count:12 (sent:12) , TotSize:2838, Seconds from asses
sment start First:0 Last:0
Enable  650:Oval, Count:1 (sent:11) , TotSize:666996, Seconds from assessment st
art First:79 Last:79
Enable  651:Error, Count:0 (sent:0)
Disable 652:PasswordPolicy, Count:0 (sent:0)
Enable  653:RetrieverCompletionStatus, Count:3 (sent:3) , TotSize:4776, Seconds
from assessment start First:156 Last:757
Enable  654:ProbeResultMsg, Count:0 (sent:0)
Disable 655:EventSubscriberStatusMsg, Count:3 (sent:0) , TotSize:726, Seconds fr
om assessment start First:156 Last:757
Enable  656:OpenPortsMsg, Count:1 (sent:1) , TotSize:1061, Seconds from assessme
nt start First:6 Last:6
Disable 657:ProbeInfoMsg, Count:1 (sent:0) , TotSize:241, Seconds from assessmen
t start First:0 Last:0
------------------------
Dur Since last config load sec: 591724
All Messages count: 7632
All Messages size:  4645385
Messages successfully sent:5316
Health Message: Count:5045, Seconds from agent start: First:0 Last:591591
 {"t":1556772754895,"proxy":142,"o":"\"Ubuntu 16.04.6 LTS\"","k":"4.4.0-1074-aws
","s":5316,"d":0,"l":21,"m":1}

ubuntu@ip-10-0-0-7:~$
```

Figure 2. Messages exchanged between agent and inspector

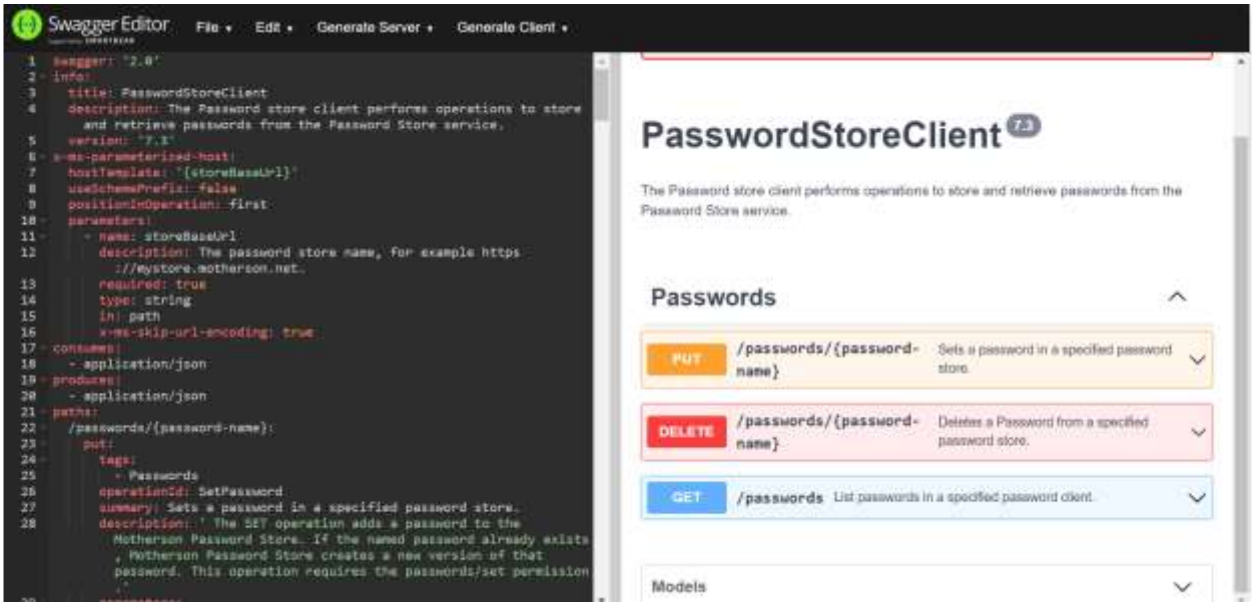
This command returns the status of the currently running agent, on checking the status it is observed in the screenshot that messages are being exchanged between the agent installed on ec2 machine and amazon inspector.

AWS Systems Manager Agent (SSM Agent) is Amazon software that can be installed and configured on an Amazon EC2 instance, an on-premises server, or a virtual machine (VM). SSM Agent makes it possible for Systems Manager to update, manage, and configure ec2 instances. SSM Agent is installed, by default in some but in some like the machine tested on it had to be manually installed.

motivated to pool the resource. This participation credit is also used by helping server to further lower its bid price, hence increasing its wining probability in next auction round.

Algorithm 1: Broker Module

```
Input: Incoming traffic $X_{in}$ havingpackets Pk
      V[t]: Traffic volume at current instant,
      $V_{max}$: Maximum capacity of channel
Start
Fetch (Pk header, V[t])
If(Source_address[$Pk_i$]$\epsilon$blacklist_log
&&payload[$Pk_i$]==payload[$Pk_j$])
{                 Alert();            //malicious behavior
                  Drop();
                  Update_log();}
Else Fwd_module(){      If (V[t] <$V_{max}$)        //normal flow
                  {Fwd_server()
                        {Send[$X_{in}$] -> server;}}
                  Else Fwd_ORA();                 //overflow
Stop
```



```yaml
swagger: '2.0'
info:
  title: PasswordStoreClient
  description: The Password store client performs operations to store
    and retrieve passwords from the Password Store service.
  version: '7.3'
x-ms-parameterized-host:
  hostTemplate: '{storeBaseUrl}'
  useSchemePrefix: false
  positionInOperation: first
  parameters:
    - name: storeBaseUrl
      description: The password store name, for example https
        ://mystore.motherson.net.
      required: true
      type: string
      in: path
      x-ms-skip-url-encoding: true
consumes:
  - application/json
produces:
  - application/json
paths:
  /passwords/{password-name}:
    put:
      tags:
        - Passwords
      operationId: SetPassword
      summary: Sets a password in a specified password store.
      description: ' The SET operation adds a password to the
        Motherson Password Store. If the named password already exists
        , Motherson Password Store creates a new version of that
        password. This operation requires the passwords/set permission
        .'
      parameters:
```

PasswordStoreClient 7.3

The Password store client performs operations to store and retrieve passwords from the Password Store service.

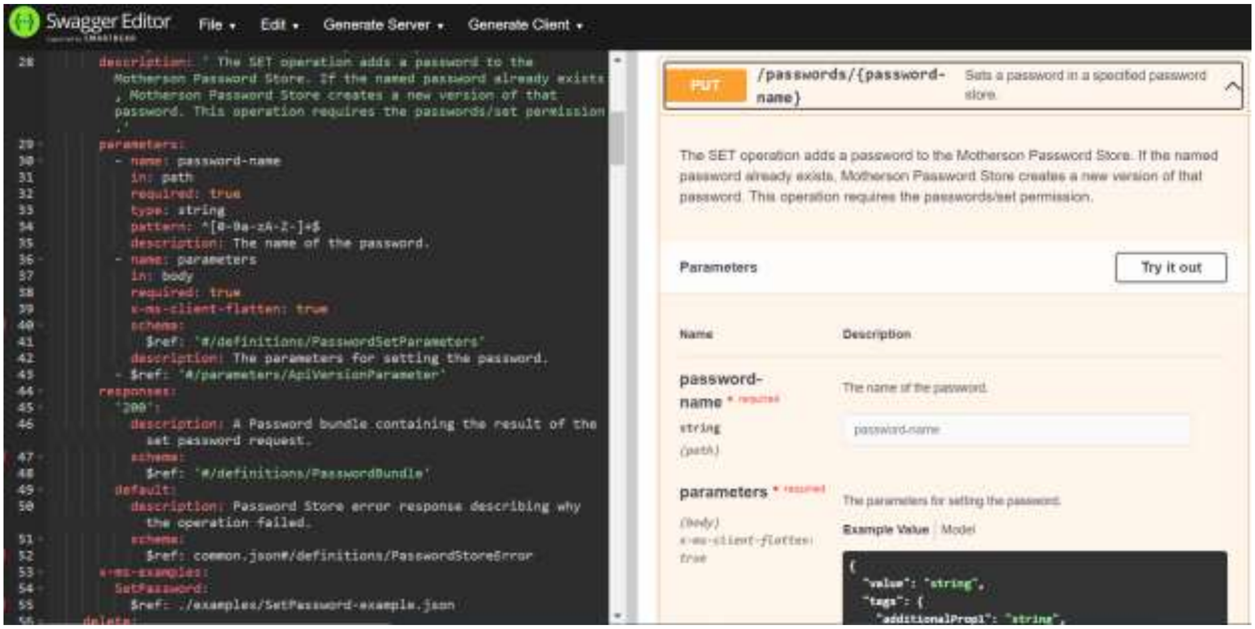
Passwords

PUT `/passwords/{password-name}` Sets a password in a specified password store.

DELETE `/passwords/{password-name}` Deletes a Password from a specified password store.

GET `/passwords` List passwords in a specified password client.

Models



```
    description: ' The SET operation adds a password to the
      Motherson Password Store. If the named password already exists
      , Motherson Password Store creates a new version of that
      password. This operation requires the passwords/set permission
      .'
    parameters:
      - name: password-name
        in: path
        required: true
        type: string
        pattern: ^[0-9a-zA-Z-]+$
        description: The name of the password.
      - name: parameters
        in: body
        required: true
        x-ms-client-flatten: true
        schema:
          $ref: '#/definitions/PasswordSetParameters'
        description: The parameters for setting the password.
      - $ref: '#/parameters/ApiVersionParameter'
    responses:
      '200':
        description: A Password bundle containing the result of the
          set password request.
        schema:
          $ref: '#/definitions/PasswordBundle'
      default:
        description: Password Store error response describing why
          the operation failed.
        schema:
          $ref: common.json#/definitions/PasswordStoreError
    x-ms-examples:
      SetPassword:
        $ref: ./examples/SetPassword-example.json
  delete:
```

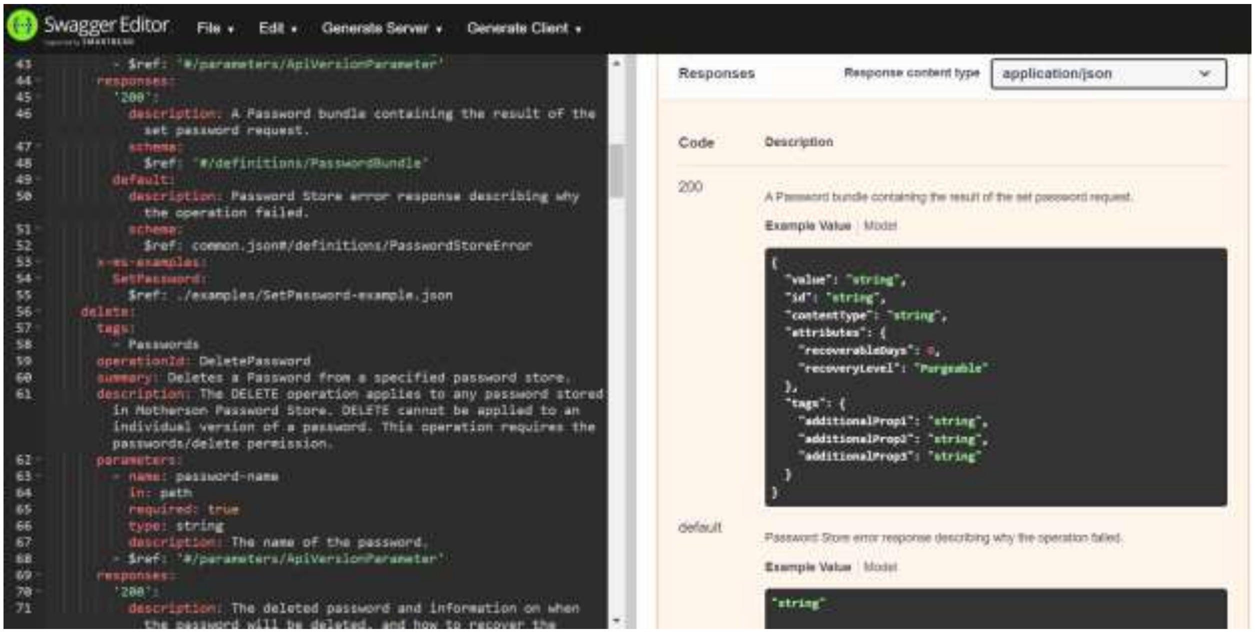
/passwords/{password-name} Sets a password in a specified password store.

The SET operation adds a password to the Motherson Password Store. If the named password already exists, Motherson Password Store creates a new version of that password. This operation requires the passwords/set permission.

Parameters

Name	Description
password-name * required string *(path)*	The name of the password. password-name
parameters * required *(body)* *x-ms-client-flatten: true*	The parameters for setting the password. Example Value | Model

```
{
  "value": "string",
  "tags": {
    "additionalProp1": "string",
```



```yaml
        - $ref: '#/parameters/ApiVersionParameter'
      responses:
        '200':
          description: A Password bundle containing the result of the
            set password request.
          schema:
            $ref: '#/definitions/PasswordBundle'
        default:
          description: Password Store error response describing why
            the operation failed.
          schema:
            $ref: common.json#/definitions/PasswordStoreError
      x-ms-examples:
        SetPassword:
          $ref: ./examples/SetPassword-example.json
    delete:
      tags:
        - Passwords
      operationId: DeletePassword
      summary: Deletes a Password from a specified password store.
      description: The DELETE operation applies to any password stored
        in Motherson Password Store. DELETE cannot be applied to an
        individual version of a password. This operation requires the
        passwords/delete permission.
      parameters:
        - name: password-name
          in: path
          required: true
          type: string
          description: The name of the password.
        - $ref: '#/parameters/ApiVersionParameter'
      responses:
        '200':
          description: The deleted password and information on when
            the password will be deleted, and how to recover the
```

Responses

Response content type: application/json

Code | Description

200

A Password bundle containing the result of the set password request.

Example Value | Model

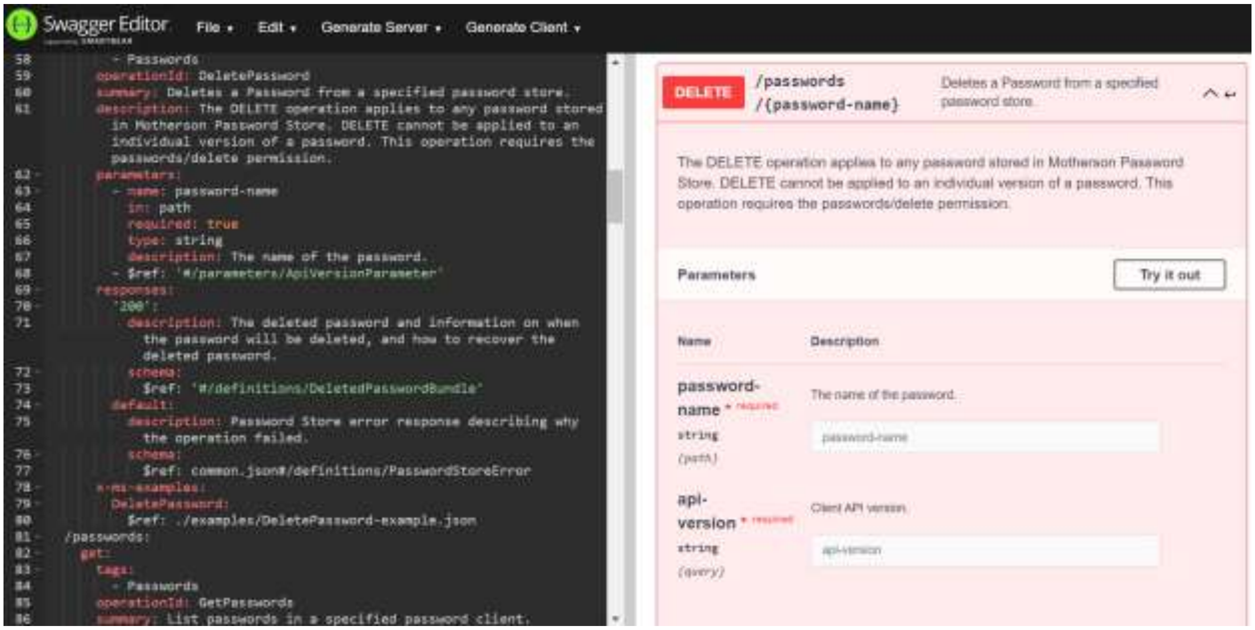
```json
{
  "value": "string",
  "id": "string",
  "contentType": "string",
  "attributes": {
    "recoverableDays": 0,
    "recoveryLevel": "Purgeable"
  },
  "tags": {
    "additionalProp1": "string",
    "additionalProp2": "string",
    "additionalProp3": "string"
  }
}
```

default

Password Store error response describing why the operation failed.

Example Value | Model

```json
"string"
```



```yaml
        - Passwords
      operationId: DeletePassword
      summary: Deletes a Password from a specified password store.
      description: The DELETE operation applies to any password stored
        in Motherson Password Store. DELETE cannot be applied to an
        individual version of a password. This operation requires the
        passwords/delete permission.
      parameters:
        - name: password-name
          in: path
          required: true
          type: string
          description: The name of the password.
        - $ref: '#/parameters/ApiVersionParameter'
      responses:
        '200':
          description: The deleted password and information on when
            the password will be deleted, and how to recover the
            deleted password.
          schema:
            $ref: '#/definitions/DeletedPasswordBundle'
        default:
          description: Password Store error response describing why
            the operation failed.
          schema:
            $ref: common.json#/definitions/PasswordStoreError
      x-ms-examples:
        DeletePassword:
          $ref: ./examples/DeletePassword-example.json
  /passwords:
    get:
      tags:
        - Passwords
      operationId: GetPasswords
      summary: List passwords in a specified password client.
```

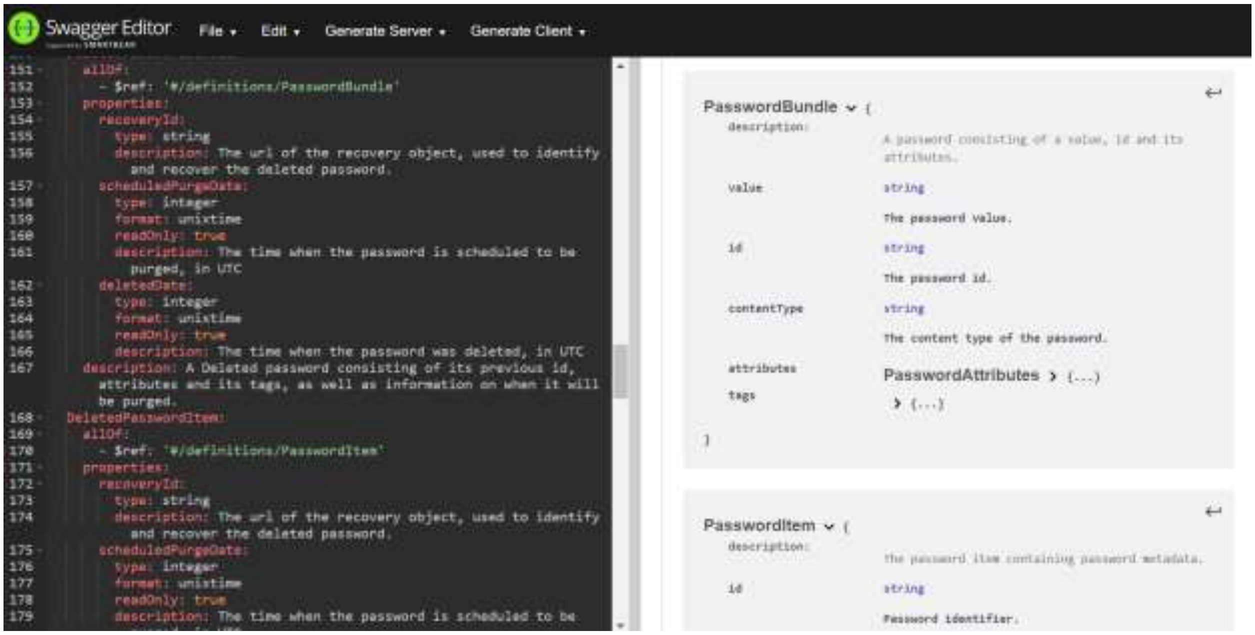
/passwords/{password-name}

Deletes a Password from a specified password store.

The DELETE operation applies to any password stored in Motherson Password Store. DELETE cannot be applied to an individual version of a password. This operation requires the passwords/delete permission.

Parameters

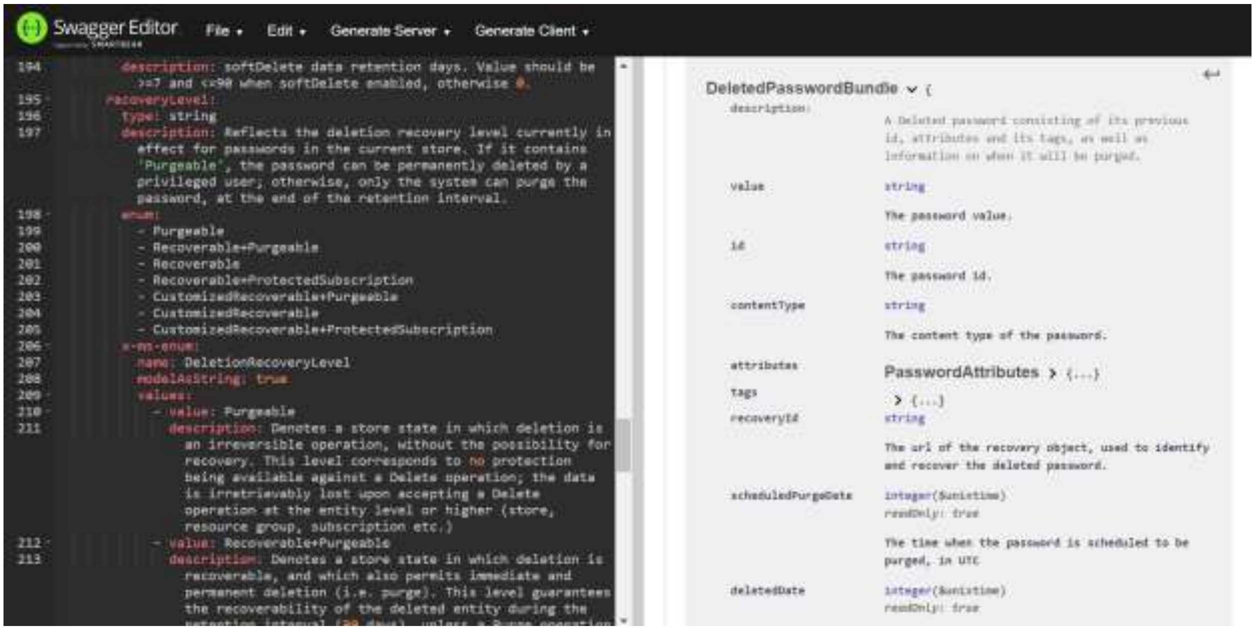
Name	Description
password-name * required string (path)	The name of the password. password-name
api-version * required string (query)	Client API version. api-version



```
    allOf:
      - $ref: '#/definitions/PasswordBundle'
    properties:
      recoveryId:
        type: string
        description: The url of the recovery object, used to identify
          and recover the deleted password.
      scheduledPurgeDate:
        type: integer
        format: unixtime
        readOnly: true
        description: The time when the password is scheduled to be
          purged, in UTC
      deletedDate:
        type: integer
        format: unixtime
        readOnly: true
        description: The time when the password was deleted, in UTC
    description: A Deleted password consisting of its previous id,
      attributes and its tags, as well as information on when it will
      be purged.
  DeletedPasswordItem:
    allOf:
      - $ref: '#/definitions/PasswordItem'
    properties:
      recoveryId:
        type: string
        description: The url of the recovery object, used to identify
          and recover the deleted password.
      scheduledPurgeDate:
        type: integer
        format: unixtime
        readOnly: true
        description: The time when the password is scheduled to be
```

```
PasswordBundle ⌄ {
    description:       A password consisting of a value, id and its
                       attributes.
    value              string
                       The password value.
    id                 string
                       The password id.
    contentType        string
                       The content type of the password.
    attributes         PasswordAttributes › {...}
    tags               › {...}
}
```

```
PasswordItem ⌄ {
    description:       The password item containing password metadata.
    id                 string
                       Password identifier.
```



```
          description: softDelete data retention days. Value should be
            >=7 and <=90 when softDelete enabled, otherwise 0.
        recoveryLevel:
          type: string
          description: Reflects the deletion recovery level currently in
            effect for passwords in the current store. If it contains
            'Purgeable', the password can be permanently deleted by a
            privileged user; otherwise, only the system can purge the
            password, at the end of the retention interval.
          enum:
            - Purgeable
            - Recoverable+Purgeable
            - Recoverable
            - Recoverable+ProtectedSubscription
            - CustomizedRecoverable+Purgeable
            - CustomizedRecoverable
            - CustomizedRecoverable+ProtectedSubscription
          x-ms-enum:
            name: DeletionRecoveryLevel
            modelAsString: true
            values:
              - value: Purgeable
                description: Denotes a store state in which deletion is
                  an irreversible operation, without the possibility for
                  recovery. This level corresponds to no protection
                  being available against a Delete operation; the data
                  is irretrievably lost upon accepting a Delete
                  operation at the entity level or higher (store,
                  resource group, subscription etc.)
              - value: Recoverable+Purgeable
                description: Denotes a store state in which deletion is
                  recoverable, and which also permits immediate and
                  permanent deletion (i.e. purge). This level guarantees
                  the recoverability of the deleted entity during the
                  retention interval (90 days), unless a Purge operation
```

DeletedPasswordBundle ∨ {

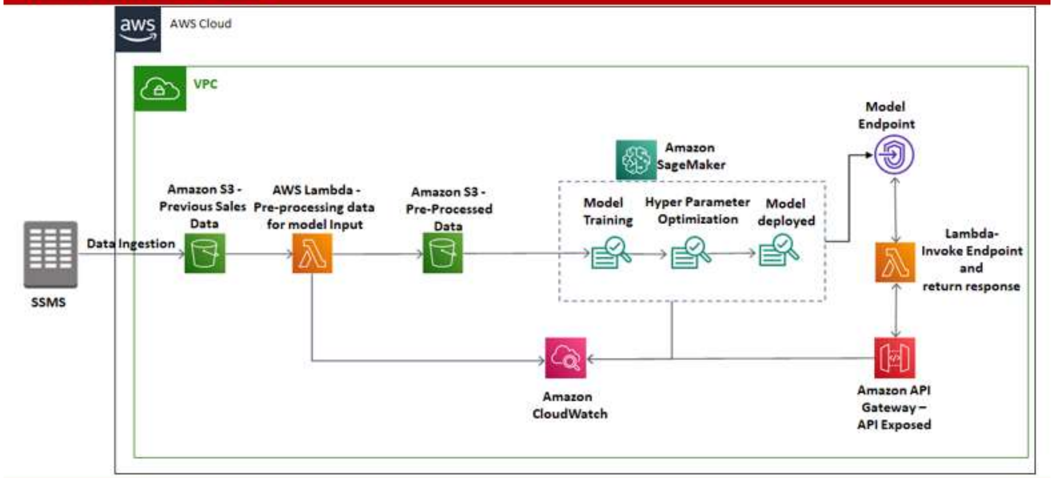
description:	A Deleted password consisting of its previous id, attributes and its tags, as well as information on when it will be purged.
value	string The password value.
id	string The password id.
contentType	string The content type of the password.
attributes	PasswordAttributes > {...}
tags	> {...}
recoveryId	string The url of the recovery object, used to identify and recover the deleted password.
scheduledPurgeDate	integer($unixtime) readOnly: true The time when the password is scheduled to be purged, in UTC
deletedDate	integer($unixtime) readOnly: true

5 KNOWN ISSUES

This section provides information about the known issues and workarounds.

PAR Number	Description
RMTS-5292	**Error indication:** Upload button is unavailable in Asset Catalog. **Description:** After publishing the assets, the Upload button is unavailable to upload the next version of assets. **Workaround:**Delete the existing version of assets to upload a new version.
RMTS-4707	**Error indication:** IFS Client application closes on Windows Mixed Reality Headset, when kept idle for 15 minutes. **Description:**During a session in IFS Client application if the application is kept idle for 15 minutes, IFS Client application on Windows Mixed Reality Headset gets closed and you can not resume the session. **Workaround:**Increase the Idle time on Mixed Reality Headset.
RMTS-6957	**Error Indication:** The user enters the plant without any PPEs even though it is selected from the VR room. **Description:** In the multi-user session, the user enters the plant without any PPEs even though it is selected from the VR room.

Architecture Diagram


aws
AWS Cloud
VPC
SSMS
Data Ingestion
Amazon S3 - Previous Sales Data
AWS Lambda - Pre-processing data for model Input
Amazon S3 - Pre-Processed Data
Amazon SageMaker
Model Training
Hyper Parameter Optimization
Model deployed
Model Endpoint
Lambda- Invoke Endpoint and return response
Amazon API Gateway – API Exposed
Amazon CloudWatch

How AWS services helped in building the model for sales Forecasting

AWS Lambda to handle the backend API calls

It helped to initialize and validate the input and acted as the backend of the whole task. AWS Lambda lets us run code without provisioning or managing servers. Also, it helped to connect with various AWS API's to acquire various insights from the inputs.

Amazon API Gateway

Amazon API Gateway is an AWS service for creating, publishing, maintaining, monitoring, and securing REST, HTTP, and WebSocket APIs at any scale.

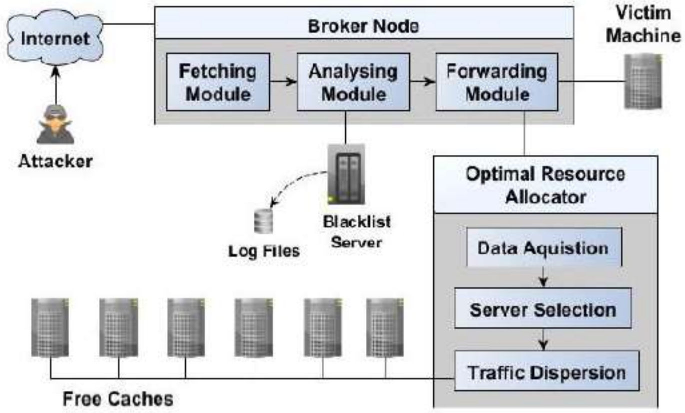


Fig. 3. Architecture of defense scheme

B. Blacklist Server: The blacklist server stores the list of IP addresses which have sent malicious packets in the past. This record is regularly updated and stored in the log files as the traffic arrives at the broker node.

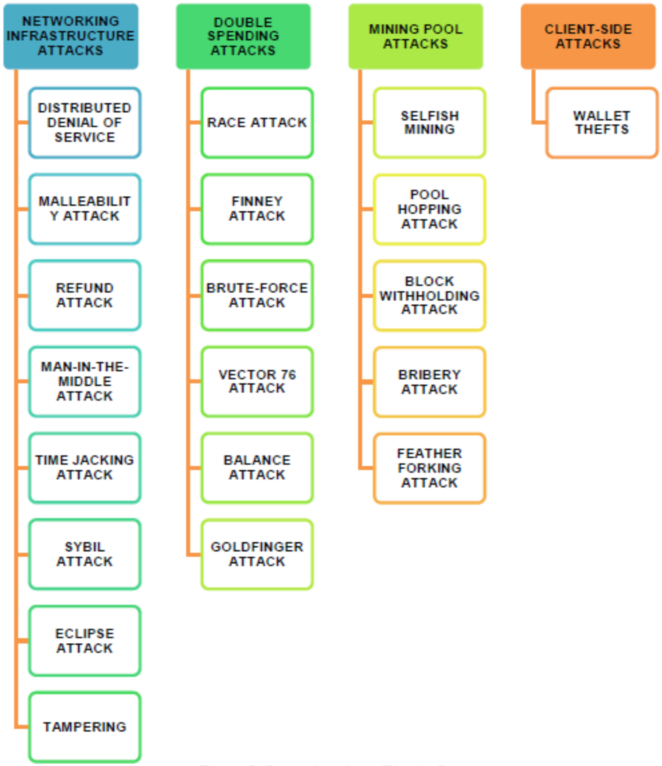


Figure 3. Cyber Attacks in Bitcoin System

are payment services which provide the exchange and wallet service providers with a platform and infrastructure to operate in a secure environment. The refund attack takes place by exploiting the authentication vulnerability present in BIP70. In this attack, the user wallet is under the

These are hacker-proof physical devices that are connected to the PC only at the time of making a transaction. To protect the private key from getting exposed, it is stored in an analog medium instead of electronic one. If the bitcoin user wants to use only hot wallet then he must ensure that

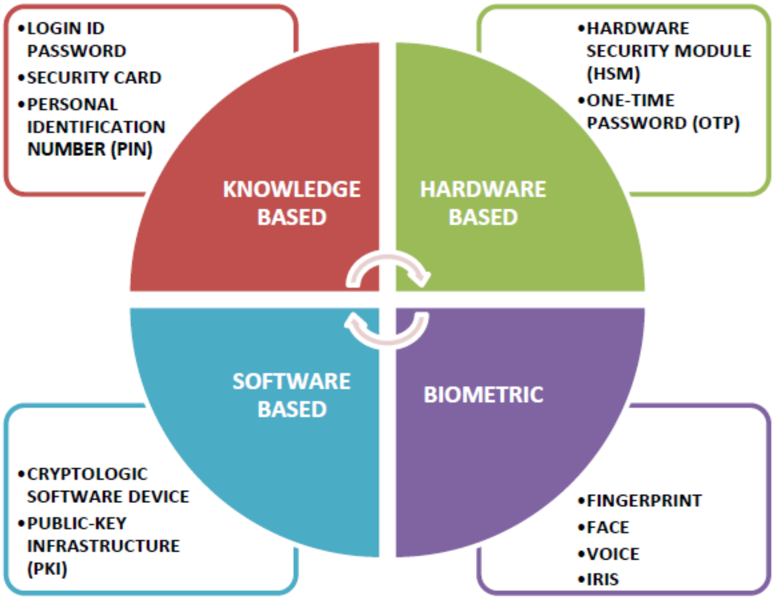


Figure 10. User authentication methods for e-financial transactions.