AVANAN - R&D DOCUMENTATION

SmartAPI Documentation

Document V1.30 Beta
(2021/8)

API Overview

1. API Concepts
2. Authentication and Authorization
3. Response Codes
4. Restrictions
5. URLs and URL Base
6. Scopes

API Authentication & Authorization

1. Overview
   - **AVANAN API Security**
2. /auth - Generate the AVANAN API Access token
   - **Request**
   - **Calculating “x-av-sig” for token generation**
   - **Response**
3. Calculating API request signature for all SmartAPI requests
   - **Calculating header signature “x-av-sig”**
4. /scopes - List of scopes supported by the App Client
   - **Request**
   - **Response**
   - **Response Sample**

EVENT API

1. GET /event/{eventId} - Retrieve a specific AVANAN security event
   - **Request**
   - **Response**
   - **Response Sample**
2. POST /event/query - Query for AVANAN security events
   - **Request**
   - **Response**
   - **Response Sample**

Search API

1. GET /search/entity/{entityId} - Search for a specific AVANAN SaaS entity
   - **Request**
   - **Response**
   - **Response Sample**
2. POST /search/query - Search query for SaaS entities
   - **Request**
   - **Response**
   - **Response Sample**

Action API

1. /action/event - Perform an action on AVANAN security events

- **Request**
- **Response**
- **Response Sample**

2. /action/entity - Perform Action on AVANAN SaaS entities (by AVANAN entity ID)
    - **Request**
    - **Response**
    - **Response Sample**
3. (not available yet) - Perform Action on AVANAN SaaS entities (by filter/condition)
    - **Request**
    - **Response**
    - **Response Sample**

Task API

1. GET /task/{taskId} - Search for a specific AVANAN Task entity
    - **Request**
    - **Response**
    - **Response Sample**

API Overview

1. API Concepts

The AVANAN SmartAPI uses a customized variant of the REST model of state transfer.
it is aimed toward uniformity in all API calls, embracing REST standards wherever possible for ease of use and standardization.

2. Authentication and Authorization

Authentication and authorization sequence is done by using an application id and secret key – provided by AVANAN within the signup process. These are used in order to obtain access token and sign each and every request sent to the API.
This entire process will be detailed on the "API Authentication & Authorization" on this document.

3. Response Codes

The following table include all http/s standard response codes returned by the API

Code	Message	Description
200	Success	Request was processed successfully
400	Bad Request	Server cannot process the request
401	Unauthorized	Must provide token in header, token expired or token invalid/malformed
403	Forbidden	Data not available for customer
404	Not found	Server cannot find requested resource
429	Restrictions	Too many requests
500	Server Error	Server encountered an unexpected condition

4. Restrictions

The SmartAPI uses various restrictions for enhanced API protection, such as limitation on the number of API call rate (call per second) or API call validity check for re-play control.

5. URLs and URL Base

All API calls to the AVANAN SmartAPI should be directed to the following URI base, by region.

- US: **smart-api-production-1-us.avanan.net**
- EU: **smart-api-production-1-eu.avanan.net**
- CA: **smart-api-production-1-ca.avanan.net**

To comply with regional data protection laws, all regions operate independently, so you cannot access data from one region by calling the other region endpoint.
Also, app clients (client_id and client_secret pairs) are regional.

6. Scopes

Starting in version 1.30 it is possible to associate one app client to multiple Avanan tenants.
This was created to allow easy querying multiple portals in the same region for customers that have them, but mainly MSP (Managed Service Providers) partners.
Particularly for MSP, the list of associated portals is updated automatically by our MSP system.

To verify the available scopes for your app client, call the “**GET /scopes**” endpoint, it will return a list of the scopes available at that moment for your app client.

Scopes follow this format: “**{farm}:{tenant}**”. **Farm** is the internal Avanan identifier of a complete regional compute unit, and **tenant** is your unique identifier. Avanan portal URLs always follow this schema “**{tenant}.avanan.net**”

Query endpoints (**POST /event/query**, and **POST /search/query**) have “**scopes**” as an optional argument. If you have a multi scope app client, you can pass a list of scopes to narrow down the query to just a set of tenants. By default queries will be performed on all available scopes.

Action related endpoints (**POST /action/event**, **POST /action/entity** and **GET /task/{task_id}**) are **single scope only**. If you have a multi-scope app, the optional “**scope**” argument of the payload is mandatory, and the API will return a 400 if none is passed.

API Authentication & Authorization

1. Overview

- **AVANAN API Security**

  AVANAN's API authentication utilizes JWT token based access. Token must be requested and transferred alongside other parameters for all API calls in the request header.

  Upon registering to AVANAN's API service the customer is issued the following:

  1. **Application ID** – a unique identifier for API client
  2. **Secret Key** – a shared secret used for initial token request authorization, and message signature (protecting the entire API message call from malicious tampering)

  All access tokens generated by AVANAN have automatic expiration of 24 hours, so when a token expires, a new token must be created in order to keep sending API calls.

  This section will detail which calls should be performed in order to obtain a valid access token and how to sign a message with the "Secret Key" issued by AVANAN for API users.

2. /auth - Generate the AVANAN API Access token

- **URI - GET**

  To use this endpoint send a GET request to retrieve a specific security event by its AVANAN id:

```
/auth
```

- **Request**

  The request includes HTTP headers obtained when registering to AVANAN API service and calculated by the API consumer

- **Request Headers**

Header	TYPE	Required	Format	Description/Sample
x-av-req-id	String	Y	UUID – generated and supplied on the request	d290f1ee-6c54-4b01-90e6
x-av-token	String	Y	**Should be sent empty on this request only**	
x-av-app-id	String	Y	AVANAN Application ID	US:myapp29
x-av-date	String	Y	Date-time in GMT	'2021-04-10T00:00:00.000Z'
x-av-sig	String	Y	Calculated signature	Please see signature calculation explanation below

- **Calculating “x-av-sig” for token generation**

  The request includes HTTP headers obtained when registering to AVANAN API service and calculated by the API consumer when issuing an API request.

  In order to calculate the signature for the request the following parameters should be concatenated, in a specific order, then a base 64 should be invoked and then sha-256 calculated on the resulting value to produce the signature value. The following describes the order of concatenation:

```
x-av-req-id
x-av-app-id
x-av-date
Secret Key
```

So in the following example, assuming our secret key is the string “**my_avanan_secret**”, calculating the **x-av-sig** will be as such:

```
for the following values:

x-av-req-id: “d290f1ee-6c54-4b01-90e6”
x-av-app-id: “US:myapp29”
x-av-date: “2021-04-10T00:00:00.000Z”
The Secret Key is: “my_avanan_secret”

the following calculation should be performed to calculate x-av-sig:

Sha256(
      base64(
            d290f1ee-6c54-4b01-90e6US:myapp292021-04-10T00:00:00.000Zmy_avanan_secret
       )
)

Which will result in the value:
sha256(
ZDI5MGYxZWUtNmM1NC00YjAxLTkwZTZVUzpteWFwcDI5MjAyMS0wNC0xMFQwMDowMDowMC4wM
DBabXlfYXZhbmFuX3NlY3JldA==
)

Which is:
2462b23346ab0642b65d7d094aca5fb4c29fd96d0468deceae2704d258e81497

So, sending the token generation request must include this header:
x-av-sig: “2462b23346ab0642b65d7d094aca5fb4c29fd96d0468deceae2704d258e81497”
```

- **Request String Parameters**

  None

- **Request Body**

  Not applicable on GET

- **Request sample (CURL) format**

```
curl -X GET -H “Accept: application/json” \
    -H “x-av-req-id: d290f1ee-6c54-4b01-90e6” \
    -H “x-av-token: “ ” \
    -H “x-av-app-id: myapp29” \
    -H “x-av-date: 2021-04-10T00:00:00.000Z” \
    -H “x-av-sig: 2462b23346ab0642b65d7d094aca5fb4c29fd96d0468deceae2704d258e81497” \
    https://smartapi-prod-us-1.avanan.net/v1.0/auth
```

- **Response**

  The response obtained from the service includes HTTP response code and a single string (which is the JWT token valid for 24 hours in case authentication was successful),

  This token should be sent with all API consecutive calls as the **x-av-token** header value

3. Calculating API request signature for all SmartAPI requests

- **Calculating header signature “x-av-sig”**

  When issuing other API calls (all calls other than “/auth” token generation requests), the client application must provide request HTTP headers.

  the **x-av-token** obtained on the auth sequence is one of these headers, but **x-av-sig** signature should be calculated for each request.

  In order to calculate the signature for the request the following parameters should be concatenated, in this specific order, then a base 64 should be invoked and then sha-256 on the resulting value. The following describe the order of concatenation:

  x-av-req-id
  x-av-app-id
  x-av-date
  Request Text
  Secret Key

  The value of “**Request Text**” is the endpoint string, for example: “/v1.0/event/<event_id>” (with the actual id replaced) or “/v1.0/search/query”.

  The “**Secret Key**” value is issued by AVANAN to customers on API registration, and it is the same key used to sign a request for token generation explained in the previous section.

4. /scopes - List of scopes supported by the App Client

- **URI - GET**

  To use this endpoint send a GET request to retrieve a list of scopes supported by the App Client:

```
/scopes
```

- **Request**

  The request includes HTTP headers obtained when registering to AVANAN API service and calculated by the API consumer

- **Request Headers**

Header	TYPE	Required	Format	Description/Sample
x-av-req-id	String	Y	UUID – generated and supplied on the request	d290f1ee-6c54-4b01-90e6
x-av-token	String	Y	Token obtained on the authentication sequence	tkn8546ffffggd9d8934593
x-av-app-id	String	Y	AVANAN Application ID	US:myapp29
x-av-date	String	Y	Date-time in GMT	'2021-04-10T00:00:00.000Z'
x-av-sig	String	Y	Calculated signature	Please see signature calculation explanation below

- **Request String Parameters**

  None

- **Request Body**

  Not applicable on GET

- **Request sample (CURL) format**

```
curl -X GET -H “Accept: application/json” \
      -H “x-av-req-id: d290f1ee-6c54-4b01-90e6” \
      -H “x-av-token: tkn8546ffffggd9d8934593” \
      -H “x-av-app-id: myapp29” \
      -H “x-av-date: 2021-04-10T00:00:00.000Z” \
      -H “x-av-sig: 2462b23346ab0642b65d7d094aca5fb4c29fd96d0468deceae2704d258e81497” \
      https://smartapi-prod-us-1.avanan.net/v1.0/scopes
```

- **Response**

  The response obtained from the service includes HTTP response code and JSON formatted structure.

  The structure includes a **responseEnvelope** structure which is common to all API calls, and a **responseData** object that holds an array of scopes supported by the App Client.

- **Response Structure**

  The following is a valid response obtained from the service (JSON format):

```
{
 "responseEnvelope": {
  "requestId": "string",
  "responseCode": 200,
  "responseText": "string",
  "additionalText": "string",
  "recordsNumber": 1,
  "scrollId": "string"
 },
 "responseData": [
  “us:customername”
 ]
}
```

EVENT API

1. /event/{eventId} - Retrieve a specific AVANAN security event

- **URI - GET**

  To use this endpoint send a GET request to retrieve a specific security event by its AVANAN id:

```
/event/{eventId}
```

- **Request**

  The request includes HTTP headers (obtained on the authentication/authorization process and used to sign the request) alongside with request string parameters.

- **Request Headers**

Header	TYPE	Required	Format	Description/Sample
x-av-req-id	String	Y	UUID – generated and supplied on the request	d290f1ee-6c54-4b01-90e6-d701748f0851
x-av-token	String	Y	Token obtained on the authentication sequence	tkn8546ffffggd9d8934593
x-av-app-id	String	Y	Application ID provided by AVANAN	myapp29
x-av-date	String	Y	Date-time in GMT	'2016-08-29T09:12:33.001Z'
x-av-sig	String	Y	Calculated signature	tkn8jmveolrrtertr9d8934593

- **Request String Parameters**

Parameter	TYPE	Required	Format	Description/Sample
eventId	String	Y		AVANAN internal request Id, such as: “ebb3e4bc8a9b14d7a529bb54ea6991b6”

- **Request Body**

  Not applicable on GET

- **Request sample (CURL) format**

```
curl -X GET -H “Accept: application/json” \
      -H “x-av-req-id: d290f1ee-6c54-4b01-90e6-d701748f0851” \
      -H “x-av-token: tkn8546ffffggd9d8934593” \
      -H “x-av-app-id: myapp29” \
      -H “x-av-date: 2016-08-29T09:12:33.001Z” \
      -H “x-av-sig: tkn8jmveolrrtertr9d8934593” \
      https://smartapi-prod-us-1.avanan.net/v1.0/event/ebb3e4bc8a9b14d7a529bb54ea6991b6
```

- **Response**

  The response obtained from the service includes HTTP response code and JSON formatted structure.

  the structure includes a **responseEnvelope** structure which is common to all API calls, and a **responseData** object that holds an array of security events.

  within each events one can find event details, and array of actions taken on the event entity (under the **actions** array) . An array of available actions to take on the event and their corresponding parameters (**availableEventActions** array) also appear on the response.

- **Response Structure**

  The following is a valid response obtained from the service (JSON format):

```
{
 "responseEnvelope": {
  "requestId": "string",
  "responseCode": 0,
  "responseText": "string",
  "additionalText": "string",
  "recordsNumber": 1,
  "totalRecordsNumber": 1,
  "scrollId": "string"
 },
 "responseData": [
  {
   "eventId": "string",
   "cusomerId": "string",
   "saas": "string",
   "entityId": "string",
   "state": "string",
   "type": "string",
   "confidenceIndicator": "string",
   "eventCreated": "string",
   "severity": "string",
   "description": "string",
   "data": "string",
   "additionalData": {},
   "availableEventActions": [
    {
     "actionName": "string",
     "actionParameter": "string"
    }
   ],
   "actions": [
    {
     "actionType": "string",
     "createTime": "string",
     "relatedEntityId": "string"
    }
   ]
  }
 ]
}
```

- **Response Parameters**

  The following are the response parameters:

Parameter		Type	Description
responseEnvelope		Object	A container of metadata properties
	requestId	String	Request Id (from the request header **x-av-req-id** value)
	responseCode	Integer	0 is success, other value failure
	responseTest	String	Text value of response
	additionalText	String	Extra information
	recordsNumber	Integer	Number of record is response
	totalRecordsNumber	Integer	Total number of records
	scrollId	String	Unique ID used for scrolling
responseData		Object	Array of event entities
	eventId	String	Unique ID of the security event
	customerId	String	AVANAN customer Id
	saas	String	A name of the relevant SaaS
	entityId	String	Unique ID of the relevant SaaS entity
	state	String	Current state of the security event
	type	String	Security event type
	confidenceIndicator	String	Confidence indicator
	eventCreated	String	Security event creation time
	severity	String	Lowest, Low, Medium, High, Critical
	description	String	Short explanation of the event
	data	String	Description in not resolved form

	additionalData	Object	Raw data of description field
availableEventActions		Array	List of available actions
	actionName	String	A name of available action
	actionParameter	String	A name of parameter of the action
actions		Array	A list of actions that were done on this event
	actionType	String	A name of performed action
	createTime	String	A date when the action was performed
	relatedEntityId	String	Unique ID of the relevant SaaS entity

- **Response Sample**

  The following is a valid response from the service:

```
{
 "responseEnvelope": {
  "responseCode": 0,
  "responseTest": "Success",
  "additionalText": "",
  "recordsNumber": 1,
  "totalRecordsNumber": 1,
  "scrollId": "34234345454353343"
 },
 "responseData": {
   "eventId": "7ded0371a3e1475c9a877e452f23a049",
   "customerId": "us:customername",
   "saas": "office365_emails",
   "entityId": "639c16e1aaa3affd5d3fa4fda5e75765",
   "state": "dismissed",
   "type": "dlp",
   "confidenceIndicator": "malicious",
   "eventCreated": "2020-07-24T20:58:27.073355+00:00",
   "severity": "Low",
   "data": "",
   "description": "SmartDLP has detected a leak in ‘please see my credit data’ from user@customer.com",
   "additionalData": "some links here and additional parameters",
   "availableEventActions": [
     {
       "actionName": "dismiss",
       "actionParameter": {"eventId":"7ded0371a3e1475c9a877e452f23a049"}
     },
     {
       "actionName": "severityChange",
       "actionParameter": {"newSeverity":"Low"}
     },
     {
       "actionName": "severityChange",
       "actionParameter": {"newSeverity":"Medium"}
     },
     {
       "actionName": "severityChange",
       "actionParameter": {"newSeverity":"High"}
     },
     {
       "actionName": "severityChange",
       "actionParameter": {"newSeverity":"Highest"}
     },
   ]
}
```

2. /event/query - Query for AVANAN security events

- **URI - POST**

  To use this endpoint you send a POST request to retrieve a specific security event or multiple events by a flexible query criteria:

```
/event/query
```

- **Request**

  The request includes HTTP headers (obtained on the authentication/authorization process and used to sign the request) alongside with request parameters posted on the request body.

- **Request Headers**

Header	TYPE	Required	Format	Description/Sample
x-av-req-id	String	Y	UUID – generated and supplied on the request	d290f1ee-6c54-4b01-90e6-d701748f0851
x-av-token	String	Y	Token obtained within the authentication sequence	tkn8546ffffggd9d8934593
x-av-app-id	String	Y	Application ID provided by AVANAN	myapp29
x-av-date	String	Y	Date-time in GMT	'2016-08-29T09:12:33.001Z'
x-av-sig	String	Y	Calculated signature	tkn8jmveolrrtertr9d8934593

- **Request String Parameters**

  None

- **Request Body**

  All applicable request parameters are posted on the request body JSON :

```
{
  "requestData": {
   “scopes”: [“string”],
   "eventTypes": ["string"],
   "eventStates": ["string"],
   "severities": ["string"],
   "saas": ["string"],
   "eventIds": ["string"],
   "confidenceIndicator": "string",
   "startDate": "string",
   "endDate": "string",
   "description": "string",
   "scrollId": "string"
   }
}
```

- **Request Body Parameters**

  The JSON parameters are as follows:

Parameter	**TYPE**	**Required**	**Format**	**Description/Sample**
scopes	Array of String			List of scopes
eventTypes	Array of String			List of required event types. Possible values are: 1. phishing 2. malware 3. suspicious malware 4. dlp 5. anomaly 6. shadow_it 7. malicious_url_click 8. malicious_url

eventStates	Array of String			List of required event states. Possible values are: 1. new 2. detected 3. pending 4. remediated 5. dismissed 6. exception
severities	Array of String			List of required event severity. Possible values are: 1. lowest 2. low 3. medium 4. high 5. critical
startDate	String	Y	Date-time	Start of required time frame. Sample: ‘2016-08-29T09:12:33.001Z'
endDate	String		Date-time	End of required time frame. Sample: '2016-08-29T09:12:33.001Z'
saas	Array of String			Name of required SaaS. Possible values: 1. office365_emails 2. office365_onedrive 3. office365_sharepoint 4. sharefile 5. slack 6. ms_teams 7. google_mail

description	String			Substring of event description. This provides an ability for free text search in event description field. For example if the value of this parameter is “inbox@email.com” then this condition will be True if a string “inbox@email.com” is included in event description field.
eventIds	Array of String			This parameter is used to retrieve a list of events by event id which only requires
confidenceIndicator	String			Confidence indicator. Sample: 'malicious'
scrollId	String	Y (paging)		This parameter is used to retrieve large sets of results. First response will include this parameter and partial result. Use this parameter to retrieve the rest of results.

- **Request sample (CURL) format**

```
curl -X POST -H “Accept: application/json” \
      -H “x-av-req-id: d290f1ee-6c54-4b01-90e6-d701748f0851” \
      -H “x-av-token: tkn8546ffffggd9d8934593” \
      -H “x-av-app-id: myapp29” \
      -H “x-av-date: 2016-08-29T09:12:33.001Z” \
      -H “x-av-sig: tkn8jmveolrrtertr9d8934593” \
      -d “{“startDate”:” “2020-01-01T00:00:00.000Z”}” \
      https://smartapi-prod-us-1.avanan.net/v1.0/event/query
```

The above will query every security event starting Jan 1st 2020.

- **Response**

  The response obtained from the service includes HTTP response code and JSON formatted structure. It is similar to the GET request per a single entity (which return a single security event in an array – but return possibly an array of security events).

  if the number of returned events is smaller than the entire number of possible responses, a consecutive call should be sent with the returned value of scrollId in order to keep paging)

- **Response Structure**

  The following is a valid response obtained from the service (JSON format):

```
{
 "responseEnvelope": {
  "requestId": "string",
  "responseCode": 0,
  "responseText": "string",
  "additionalText": "string",
  "recordsNumber": 0,
  "totalRecordsNumber": 0,
  "scrollId": "string"
 },
 "responseData": [
  {
   "eventId": "string",
   "customerId": "string",
   "saas": "string",
   "state": "string",
   "entityId": "string",
   "type": "string",
   "confidenceIndicator": "string",
   "eventCreated": "string",
   "severity": "string",
   "description": "string",
   "data": "string",
   "additionalData": {},
   "availableEventActions": [
    {
     "actionName": "string",
     "actionParameter": "string"
    }
   ],
   "actions": [
    {
     "actionType": "string",
     "createTime": "string",
     "relatedEntityId": "string"
    }
   ]
  }
 ]
}
```

- **Response Parameters**

  The following are the response parameters:

Parameter		Type	Description
responseEnvelope		Object	A container of metadata properties
	requestId	String	Request Id (from the request header **x-av-req-id** value)
	responseCode	Integer	0 is success, other value failure
	responseTest	String	Text value of response
	additionalText	String	Extra information
	recordsNumber	Integer	Number of record is response
	totalRecordsNumber	Integer	Total number of records
	scrollId	String	Unique ID used for scrolling
responseData		Object	Array of event entities
	eventId	String	Unique ID of the security event
	customerId	String	AVANAN customer id
	saas	String	A name of the relevant SaaS
	entityId	String	Unique ID of the relevant SaaS entity
	state	String	Current state of the security event
	type	String	Security event type
	confidenceIndicator	String	Confidence indicator
	eventCreated	String	Security event creation time
	severity	String	Lowest, Low, Medium, High, Critical
	description	String	Short explanation of the event
	data	String	Description in not resolved form

	additionalData	Object	Raw data of description field
availableEventActions		Array	List of available actions
	actionName	String	A name of available action
	actionParameter	String	A name of parameter of the action
	actions	Array	A list of actions that were done on this event
	actionType	String	A name of performed action
	createTime	String	A date when the action was performed
	relatedEntityId	String	Unique ID of the relevant SaaS entity

- **Response Sample**

The following is a valid response from the service:

```
{
 "responseEnvelope": {
  "responseCode": 0,
  "responseTest": "Success",
  "additionalText": "",
  "recordsNumber": 1,
  "totalRecordsNumber": 1,
  "scrollId": "34234345454353343"
 },
 "responseData": {
   "eventId": "7ded0371a3e1475c9a877e452f23a049",
   "customerId": "us:customername",
   "saas": "office365_emails",
   "entityId": "639c16e1aaa3affd5d3fa4fda5e75765",
   "state": "dismissed",
   "type": "dlp",
   "confidenceIndicator": "malicious",
   "eventCreated": "2020-07-24T20:58:27.073355+00:00",
   "severity": "Low",
   "data": "",
   "description": "SmartDLP has detected a leak in ‘please see my credit data’ from user@customer.com",
   "additionalData": "some links here and additional parameters",
   "availableEventActions": [
    {
     "actionName": "dismiss",
     "actionParameter": }"eventId":"7ded0371a3e1475c9a877e452f23a049"{
    },
    {
     "actionName": "severityChange",
     "actionParameter": {"newSeverity":"Low"}
    },
    {
     "actionName": "severityChange",
     "actionParameter": {"newSeverity":"Medium"}
    },
    {
     "actionName": "severityChange",
     "actionParameter": {"newSeverity":"High"}
    },
    {
     "actionName": "severityChange",
     "actionParameter": {"newSeverity":"Highest"}
    },
   ]
}
```

Search API

1. /search/entity/{entityId} - Search for a specific AVANAN SaaS entity

- **URI - GET**

  This endpoint is used to retrieve AVANAN SaaS entity details, given the AVANAN entity id. AVANAN keeps a unique global entity identifier for every entity in the system and given a single entity id, all entity details and related EXTENDED details can be extracted in a single API call

```
/search/entity/{entityId}
```

- **Request**

  The request includes HTTP headers (obtained on the authentication/authorization process and used to sign the request) alongside with request string parameters.

- **Request Headers**

Header	TYPE	Required	Format	Description/Sample
x-av-req-id	String	Y	UUID – generated and supplied on the request	d290f1ee-6c54-4b01-90e6-d701748f0851
x-av-token	String	Y	Token obtained on the authentication sequence	tkn8546ffffggd9d8934593
x-av-app-id	String	Y	Application ID provided by AVANAN	myapp29
x-av-date	String	Y	Date-time in GMT	'2020-08-29T09:12:33.001Z'
x-av-sig	String	Y	Calculated signature	tkn8jmveolrrtertr9d8934593

- **Request String Parameters**

Parameter	TYPE	Required	Format	Description/Sample
entityId	String	Y		AVANAN internal entity Id, such as: “f05b74da3ee859eea41aeac40aaad3c2”

- **Request Body**

  Not applicable on GET

- **Request sample (CURL) format**

```
curl -X GET -H “Accept: application/json” \
     -H “x-av-req-id: d290f1ee-6c54-4b01-90e6-jjshduhuh” \
     -H “x-av-token: tkn8546ffffggd9d8934593” \
     -H “x-av-app-id: myapp29” \
     -H “x-av-date: 2021-02-28T09:12:33.001Z” \
     -H “x-av-sig: tkn8jmveolrrtertr9d8934593” \
     https://smartapi-prod-us-1.avanan.net/v1.0/search/entity/f05b74da3ee859eea41aeac40aaad3c2
```

- **Response**

  The response obtained from the service include HTTP response code and JSON formatted structure.

  the structure include a **responseEnvelope** structure which is common to all API calls, and a **responseData** object that holds an array of returned SAAS entities (a single entity in this case). A SAAS entity structure include the following:

  1. A common generic area with general SAAS entity details (common to all SAAS entities) **entityInfo**

  2. Specific SAAS related payload details **entityPayload** – this section is SAAS specific and holds all related entity data. The document will include details for email search related data

  3. An array of security tools scan results **entitySecurityResults**

  4. An array of actions taken on the entity under the **entityActions**

  5. An array of possible actions that can be taken on the entity with and their corresponding parameters (**entityAvailableActions** array)

- **Response Structure**

  The following is the response structure obtained from the service (JSON format):

```
{
 "responseEnvelope": {
  "requestId": "string",
  "responseCode": 0,
  "responseText": "string",
  "additionalText": "string",
  "recordsNumber": 1,
  "totalRecordsNumber": 1,
  "scrollId": "string"
 },
 "responseData": [
  {
   "entityInfo": {
    "entityId": "string",
    "customerId": "string",
    "saas": "string",
    "saasEntityType": "string",
    "entityCreated": "dateTime",
    "entityUpdated": "dateTime",
    "entityActionState": "string"
   },
   "entityPayload": {},
   "entitySecurityResults": {
    "combinedVerdict": {
     "ap": "string",
     "dlp": "string",
     "clicktimeProtection": "string",
     "shadowIt": "string",
     "av": "string"
    },
    "ap": {
     "entityId": "string",
     "entityType": "string",
     "payload": {},
     "score": "string",
     "securityResultEntityId": "string",
     "securityResultEntityType": "string",
     "statusCode": "string",
     "statusDescription": "string",
     "verdict": "string"
    },
    "dlp": {
     "entityId": "string",
     "entityType": "string",
     "payload": {},
     "score": "string",
     "securityResultEntityId": "string",
     "securityResultEntityType": "string",
     "statusCode": "string",
     "statusDescription": "string",
     "verdict": "string"
    },
    "clicktimeProtection": [{
     "entityId": "string",
      "entityType": "string",
      "payload": {},
      "score": "string",
      "securityResultEntityId": "string",
      "securityResultEntityType": "string",
      "statusCode": "string",
      "statusDescription": "string",
      "verdict": "string"
    }],
    "shadowIt": [{
      "entityId": "string",
      "entityType": "string",
      "payload": {},
      "score": "string",
      "securityResultEntityId": "string",
      "securityResultEntityType": "string",
      "statusCode": "string",
      "statusDescription": "string",
      "verdict": "string"
    }],
    "av": [{
      "entityId": "string",
      "entityType": "string",
      "payload": {},
      "score": "string",
      "securityResultEntityId": "string",
      "securityResultEntityType": "string",
      "statusCode": "string",
      "statusDescription": "string",
      "verdict": "string"
    }]
   },
   "entityActions": [
    {
      "entityActionName": "string",
      "entityActionDate": "dateTime",
      "entityActionResponseCode": "integer",
      "entityActionResponseText": "string",
      "entityActionState": "string"
    }
   ],
   "entityAvailableActions": [
    {
      "entityActionName": "string",
      "entityActionParam": "string"
    }
   ]
  }
 ]
}
```

- **Response Parameters**

The following are the response parameters:

Parameter		Type	Description
responseEnvelope		Object	A container of metadata properties
	requestId	String	Request Id (from the request header **x-av-req-id** value)
	responseCode	Integer	0 is success, other value failure
	responseTest	String	Text value of response
	additionalText	String	Extra information
	recordsNumber	Integer	Number of record is response
	totalRecordsNumber	Integer	Total number of records (always 1 here)
	scrollId	String	Unique ID used for scrolling
responseData		Array	Array of entities
responseData/ **entityInfo**		Object	Generic SAAS entity details
	entityId	String	Unique ID of the AVANAN entity
	customerId	String	AVANAN customer id
	saas	String	AVANAN supported saas name
	saasEntityType	String	AVANAN supported saas entity type name: message, user, file etc’
	entityCreated	DateTime	Entity creation time (AVANAN platform)
	entityUpdated	DateTime	Entity update time (AVANAN platform)
	entityActionState	String	If an action was taken on the entity, then here we will see the entity SAAS state

responseData/ **entityPayload**		Object	This object hold SAAS specific data for the AVANAN entity. (email entity data, Drive entity data etc') – this document will detail email SAAS entityPayload attributes
responseData/ **entitySecurityResults**		Array	This array of objects holds security tools scan data
	entityId	String	Unique ID of the relevant SaaS entity
	entityType	String	AVANAN supported saas entity type name: message, user, file etc'
	payload	Object	An entire payload of a security tool scan
	score	String	Security tool result score
	securityResultEntityId	String	Unique ID of the relevant security result entity
	securityResultEntityType	String	Security result entity type
	statusCode	String	Security tool scan status code
	statusDescription	String	Security tool scan status description
entityActions		Array	List of available actions
	entityActionName	String	Action Name
	entityActionDate	DateTime	action activation time
	entityActionResponseCode	integer	action response code
	entityActionResponseText	String	Action response text
	entityActionState	Integer	Indication for the action state
entityAvailableActions		Array	A list of available actions for the entity
	entityActionName	String	Action name
	entityActionParam	String	Additional action parameter

- **Extra Response Parameters for Email (responseData/entityPayload)**

  The following are the **entityPayload** object specific details which are provided for email entity SAAS search. Some of those may appear in the response under the **entityPayload** response object

Parameter		Type	Description
responseData/ entityPayload		Object	This object hold SAAS specific data for the AVANAN entity. (email entity data, Drive entity data etc') – this document will detail email SAAS entityPayload attributes
	internetMessageId	String	Original o365/gmail identifier
	subject	String	Email subject
	received	DateTime	Time of email received
	size	Integer	Email size in KB
	emailLinks	String	Included email links
	attachmentCount	Integer	Number of email attachments
	attachments	Object	An object describing the email attachment files
	mode	String	Inline|monitor
	recipients	String	Comma separated list of recipients
	fromEmail	String	From email (uesr@avanan.com)
	fromDomain	String	From domain (avanan.com)
	fromUser	Object	user object on AVANAN platform
	fromName	String	Sender name (John Smith)
	to	String	Comma separated list of recipients
	toUser	Object	user object on AVANAN platform
	cc	Object	user object on AVANAN platform

	ccUser	Object	user object on AVANAN platform
	bcc	String	Bcc email addresses
	bccUser	Object	user object on AVANAN platform
	replyToEmail	String	Email “reply to” address
	replyToNickname	String	Email “reply to” nickname if used
	isRead	String	true|false
	isDeleted	String	true|false
	isIncoming	String	true|false
	isInternal	String	true|false
	isOutgoing	String	true|false
	isQuarantined	String	true|false
	isRestored	String	true|false
	isRestoreRequested	String	true|false
	isRestoreDeclined	String	true|false
	saasSpamVerdict	String	Spam verdict value
	SpfResult	String	SPF value combined

- **Response Sample**

The following is a valid response from the service:

```
{
 "responseEnvelope": {
  "requestId": "d290f1ee-6c54-4b01-90e6-d701748f3352",
  "responseCode": 0,
  "responseText": "Success",
  "additionalText": "",
  "recordsNumber": 1,
  "totalRecordsNumber": 1,
  "scrollId": ""
 },
 "responseData": [
  {
   "entityInfo": {
    "entityId": "b05f596bc33cf53b74ea75e37cf66b98",
    "customerId": "customername",
    "saas": "office365_emails",
    "saasEntityType": "office365_emails_email",
    "entityCreated": "2020-08-29T09:12:33.001Z",
    "entityUpdated": "2020-08-29T09:12:33.001Z",
    "entityActionState": "Clean"
   },
   "entityPayload": {
    "internetMessageId": "<562714b9-aba3-719f-5286-0b030bbdff77@o365.com>",
    "subject": "this is a test email message",
    "received": "2020-08-29T09:12:33.001Z",
    "size": "35009",
    "emailLinks": "https://www.avanan.com",
    "attachmentCount": "",
    "attachments": "",
    "mode": "inline",
    "recipiants": "developer@avanan.com",
    "fromEmail": "manager@gmail.com",
    "fromDomain": "gmail.com",
    "fromUser": "12d14cf0-9698-4bde-9d6d-e45065dd432de",
    "fromName": "gmail manager",
    "to": "developer@avanan.com",
    "toUser": "
{\"mail\":\"developer@avanan.com\",\"entity_id\":\"12d14cf0-9698-4bde-9d6d-e49843598595\",\"entity_type\":\
"office365_emails_user\"}",
    "cc": "",
    "ccUser": "",
    "bcc": "",
    "bccUser": "",
    "replyToEmail": "",
    "replyToNickName": "",
    "isRead": "true",
    "isDeleted": "flase",
    "isIncoming": "true",
    "isInternal": "false",
    "isOutgoing": "false",
    "isQuarantined": "false",
    "isRestoreRequested": "false",
    "isRestoreDeclined": "false",
    "isRestored": "false",
   "saasSpamVerdict": "",
   "SpfResult": "pass"
  },
  "entitySecurityResults": {
    "combinedVerdict": {
    "ap": "phishing",
    "dlp": null,
    "clicktimeProtection": null,
    "shadowIt": "clean",
    "av": null
    },
    "ap": [{
    "entityId": "a60ca316d8c4f19a2923114380fb0070",
    "entityType": "office365_emails_email",
    "payload": {
    "reasons_by_category": {
            "sender_reputation": [{
            "short_text": "Insignificant historical reputation with sender",
            "full_text": "The sending email address hasn't established significant historical reputation with your
domain"
            },
            {
            "short_text": "Low-traffic 'From'-domain",
            "full_text": "The sender's domain has very low traffic - often indicating low-trust domains"
            }
            ],
            "links": [{
            "short_text": "Link to a low-traffic site",
            "full_text": "The email contains link to low-traffic web-sites - often indicating low-trust domains"
            }]
    }
    },
    "score": "526.670776",
    "securityResultEntityId": "a60ca316d8c4f19a2923114380fb0070",
    "securityResultEntityType": "avanan_ap_scan",
    "statusCode": "0",
    "statusDescription": null,
    "verdict": "phishing"
    }],
    "dlp": null,
    "clicktimeProtection": null,
    "shadowIt": [{
    "entityId": "a60ca316d8c4f19a2923114380fb0070",
    "entityType": "office365_emails_email",
    "payload": {
    "subject": "TEST-0429-1619902351-15",
    "from": "user@email.com"
    },
    "score": "0.0",
    "securityResultEntityId": "a60ca316d8c4f19a2923114380fb0070",
    "securityResultEntityType": "shadow_it_emails_scan",
    "statusCode": "clean",
    "statusDescription": "Clean",
    "verdict": "clean"
    }],
    "av": null
  },
   "entityActions": [
    {}
   ],
   "entityAvailableActions": [
    {
     "entityActionName": "quarantine",
     "entityActionParam": ""
    },
    {
     "entityActionName": "restore",
     "entityActionParam": ""
    }
   ]
  }
 ]
}
```

2. /search/query - Search query for SaaS entities

- **URI - POST**

  To use this endpoint send a POST request to retrieve multiple entities using a flexible query criteria:

  ```
  /search/query
  ```

- **Request**

  The request includes HTTP headers (obtained on the authentication/authorization process and used to sign the request) alongside with request parameters posted on the request body.

- **Request Headers**

Header	TYPE	Required	Format	Description/Sample
x-av-req-id	String	Y	UUID – generated and supplied on the request	d290f1ee-6c54-4b01-90e6-d701748f0851
x-av-token	String	Y	Token obtained on the authentication sequence	tkn8546ffffggd9d8934593
x-av-app-id	String	Y	Application ID provided by AVANAN	myapp29
x-av-date	String	Y	Date-time in GMT	'2021-04-10T09:12:33.001Z'
x-av-sig	String	Y	Calculated signature	tkn8jmveolrrtertr9d8931973

- **Request String Parameters**

  None

- **Request Body**

  All applicable request parameters are posted on the request body JSON :

```
{
 "requestData": {
  "scopes": ["string"],
  "entityFilter": {
   "saas": "string",
   "saasEntity": "string",
   "startDate": "DateTime",
   "endDate": "DateTime"
  },
  "entityExtendedFilter": [
   {
    "saasAttrName": "string",
    "saasAttrOp": "string",
    "saasAttrValue": "string"
   }
  ],
  "scrollId": "string"
 }
}
```

- **Request Body Parameters**

The JSON parameters are as follows:

Parameter	TYPE	Required	Format	Description/Sample
requestData	Object			A container for action request
scopes	Array of String			List of scopes
entityFilter	Object			A container for generic query filter (apply to all entities)
entityFilter/saas	string	Y		Name of required SaaS. Possible values: sharefile slack ms_teams office365_emails office365_onedrive office365_sharepoint google_mail box dropbox
entityFilter/ saasEntity	String			Name of SaaS entity. Possible values: office365_emails_email
entityFilter/ startDate	String	Y	Date-time	Start of required time frame. Sample: ‘2019-04-10T09:12:33.001Z'
entityFilter/ endDate	String	Y	Date-time	End of required time frame. Sample: '2019-04-11T09:12:33.001Z'
entityExtendedFilter	Object			A container for SaaS specific extended query filter
entityExtendedFilter/ saasAttrName	String			saas criteria attribute name
entityExtendedFilter/ saasAttrOp	String			saas criteria attribute Operator: “is”, “contains”, “startsWith”, “isEmpty”, “isNot” , “notContains”, “isNotEmpty”, “greaterThan”,”lessThan”

entityExtendedFilter/ saasAttrValue	String			saas criteria attribute value

- **Extra Request Body Parameters for Email (specific saasAttrName used for email query)**

  The JSON parameters are as follows:

Parameter	TYPE	Required	Format	Description/Sample
entityExtendedFilter/ saasAttrName			String	Values should the address from the entity you want to match, for example: entityPayload.subject

- **Request sample (CURL) format**

```
curl -X POST -H “Accept: application/json” \
    -H “x-av-req-id: d290f1ee-6c54-4b01-90e6-d701748f0851” \
    -H “x-av-token: tkn8546ffffggd9d8934593” \
    -H “x-av-app-id: myapp29” \
    -H “x-av-date: 2021-04-10T09:12:33.001Z” \
    -H “x-av-sig: tkn8jmveolrrtertr9d8934593” \
    -d “
                    {
                     "requestData": {
                      "entityFilter": {
                       "saas": "office365_emails",
                       "saasEntity": "office365_emails_email",
                       "startDate": "2020-01-01T00:00:00.000Z",
                       "endDate": ""
                      },
                      "entityExtendedFilter": [
                       {
                              "saasAttrName": "entityPayload.fromEmail",
                              "saasAttrOp": "is",
                              "saasAttrValue": "developer@avanan.com"
                       },
                       {
                              "saasAttrName": "entityPayload.attachmentCount",
                              "saasAttrOp": "greaterThan",
                              "saasAttrValue": "0"
                       }
                      ],
                      "scrollId": ""
                     }
                    }
” \
    https://smartapi-prod-us-1.avanan.net/v1.0/search/query
```

The above will query every email message starting Jan 1st 2020 sent from developer@avanan.com with attachments

- **Response**

  The response obtained from the service includes HTTP response code and JSON formatted structure.

  The response format is the same as the single entity query, yet the returned entity array potentially includes multiple entities.

  if the number of returned SaaS entities is smaller than the entire number of possible responses, a consecutive call should be sent with the returned value of scrollId in order to keep paging)

- **Response Structure**

The following is the response structure obtained from the service (JSON format):

```
{
 "responseEnvelope": {
  "requestId": "string",
  "responseCode": 0,
  "responseText": "string",
  "additionalText": "string",
  "recordsNumber": 1,
  "totalRecordsNumber": 1,
  "scrollId": "string"
 },
 "responseData": [
  {
   "entityInfo": {
    "entityId": "string",
    "customerId": "string",
    "saas": "string",
    "saasEntityType": "string",
    "entityCreated": "dateTime",
    "entityUpdated": "dateTime",
    "entityActionState": "string"
   },
   "entityPayload": {},
   "entitySecurityResults": {
     "combinedVerdict": {
     "ap": "string",
     "dlp": "string",
     "clicktimeProtection": "string",
     "shadowIt": "string",
     "av": "string"
     },
     "ap": [{
     "entityId": "string",
     "entityType": "string",
     "payload": "object",
     "score": "string",
     "securityResultEntityId": "string",
     "securityResultEntityType": "string",
     "statusCode": "string",
     "statusDescription": "string",
     "verdict": "string"
     }],
     "dlp": "string",
     "clicktimeProtection": "string",
     "shadowIt": [{
      "entityId": "string",
      "entityType": "string",
      "payload": {
       "subject": "string",
       "from": "string"
      },
     "score": "string",
     "securityResultEntityId": "string",
     "securityResultEntityType": "string",
     "statusCode": "string",
     "statusDescription": "string",
     "verdict": "clean"
     }],
     "av": "object"
   }
   "entityActions": [
    {
     "entityActionName": "string",
     "entityActionDate": "dateTime",
     "entityActionResponseCode": "integer",
     "entityActionResponseText": "string",
     "entityActionState": "string"
    }
   ],
   "entityAvailableActions": [
    {
     "entityActionName": "string",
     "entityActionParam": "string"
    }
   ]
  }
 ]
}
```

- **Response Parameters**

The following are the response parameters:

Parameter		Type	Description
responseEnvelope		Object	A container of metadata properties
	requestId	String	Request Id (from the request header **x-av-req-id** value)
	responseCode	Integer	0 is success, other value failure
	responseTest	String	Text value of response
	additionalText	String	Extra information
	recordsNumber	Integer	Number of record is response
	totalRecordsNumber	Integer	Total number of records (always 1 here)
	scrollId	String	Unique ID used for scrolling
responseData		Array	Array of entities

responseData/ **entityInfo**		Object	Generic SAAS entity details
	entityId	String	Unique ID of the AVANAN entity
	customerId	String	AVANAN customer id
	saas	String	AVANAN supported saas name
	saasEntityType	String	AVANAN supported saas entity type name: message, user, file etc’
	entityCreated	DateTime	Entity creation time (AVANAN platform)
	entityUpdated	DateTime	Entity update time (AVANAN platform)
	entityActionState	String	If an action was taken on the entity, then here we will see the entity SAAS state
responseData/ **entityPayload**		Object	This object holds SAAS specific data for the AVANAN entity. (email entity data, Drive entity data etc’) – this document will detail email SAAS entityPayload attributes
responseData/ **entitySecurityResults**		Array	This array of objects holds security tools scan data
	entityId	String	Unique ID of the relevant SaaS entity
	entityType	String	AVANAN supported saas entity type name: message, user, file etc’
	payload	Object	An entire payload of a security tool scan
	score	String	Security tool result score
	securityResultEntityId	String	Unique ID of the relevant security result entity
	securityResultEntityType	String	Security result entity type
	statusCode	String	Security tool scan status code
	statusDescription	String	Security tool scan status description

entityActions		Array	List of available actions
	entityActionName	String	Action Name
	entityActionDate	DateTime	action activation time
	entityActionResponseCode	integer	action response code
	entityActionResponseText	String	Action response text
	entityActionState	Integer	Indication for the action state
entityAvailableActions		Array	A list of available actions for the entity
	entityActionName	String	Action name
	entityActionParam	String	Additional action parameter

- **Extra Response Parameters for Email (responseData/entityPayload)**

The following are the **entityPayload** object specific details which are provided for email entity SAAS search. Some of those may appear in the response under the **entityPayload** response object

Parameter		Type	Description
responseData/ entityPayload		Object	This object holds SAAS specific data for the AVANAN entity. (email entity data, Drive entity data etc') – this document will detail email SAAS entityPayload attributes
	internetMessageId	String	Original o365/gmail identifier
	subject	String	Email subject
	received	DateTime	Time of email received
	size	Integer	Email size in KB
	emailLinks	String	Included email links
	attachmentCount	Integer	Number of email attachments
	attachments	Object	An object describing the email attachment files
	mode	String	inline|monitor
	recipients	String	Comma separated list of recipients
	fromEmail	String	From email (user@avanan.com)
	fromDomain	String	From domain (avanan.com)
	fromUser	Object	user object on AVANAN platform
	fromName	String	Sender name (John Smith)
	to	String	Comma separated list of recipients
	toUser	Object	user object on AVANAN platform
	cc	Object	user object on AVANAN platform
	ccUser	Object	user object on AVANAN platform

	bcc	String	Bcc email addresses
	bccUser	Object	user object on AVANAN platform
	replyToEmail	String	Email “reply to” address
	replyToNickname	String	Email “reply to” nickname if used
	isRead	String	true|false
	isDeleted	String	true|false
	isIncoming	String	true|false
	isInternal	String	true|false
	isOutgoing	String	true|false
	isQuarantined	String	true|false
	isRestored	String	true|false
	isRestoreRequested	String	true|false
	isRestoreDenied	String	true|false
	saasSpamVerdict	String	Spam verdict value
	SpfResult	String	SPF value combined

- **Response Sample**

  The following is a valid response from the service:

```
{
 "responseEnvelope": {
  "requestId": "d290f1ee-6c54-4b01-90e6-d701748f3352",
  "responseCode": 0,
  "responseText": "Success",
  "additionalText": "",
  "recordsNumber": 1,
  "totalRecordsNumber": 1,
  "scrollId": ""
 },
 "responseData": [
  {
   "entityInfo": {
    "entityId": "b05f596bc33cf53b74ea75e37cf66b98",
    "customerId": "customername",
    "saas": "office365_emails",
    "saasEntityType": "office365_emails_email",
    "entityCreated": "2020-08-29T09:12:33.001Z",
    "entityUpdated": "2020-08-29T09:13:33.001Z",
    "entityActionState": "Clean"
   },
   "entityPayload": {
    "internetMessageId": "<562714b9-aba3-719f-5286-0b030bbdff77@o365.com>",
    "subject": "this is a test email message",
    "received": "2020-08-29T09:12:33.001Z",
    "size": "35009",
    "emailLinks": "https://www.avanan.com",
    "attachmentCount": "",
    "attachments": "",
    "mode": "inline",
    "recipiants": "developer@avanan.com",
    "fromEmail": "manager@gmail.com",
    "fromDomain": "gmail.com",
    "fromUser": "12d14cf0-9698-4bde-9d6d-e45065dd432de",
    "fromName": "gmail manager",
    "to": "developer@avanan.com",
    "toUser": "
{\"mail\":\"developer@avanan.com\",\"entity_id\":\"12d14cf0-9698-4bde-9d6d-e49843598595\",\"entity_type\":\
"office365_emails_user\"}",
    "cc": "",
    "ccUser": "",
    "bcc": "",
    "bccUser": "",
    "replyToEmail": "",
    "replyToNickName": "",
    "isRead": "true",
    "isDeleted": "flase",
    "isIncoming": "true",
    "isInternal": "false",
    "isOutgoing": "false",
    "isQuarantined": "false",
    "isRestoreRequested": "false",
    "isRestoreDenied": "false",
    "isRestored": "false",
     "saasSpamVerdict": "",
     "SpfResult": "pass"
    },
    "entitySecurityResults": {
      "combinedVerdict": {
      "ap": "phishing",
      "dlp": null,
      "clicktimeProtection": null,
      "shadowIt": "clean",
      "av": null
      },
      "ap": [{
      "entityId": "a60ca316d8c4f19a2923114380fb0070",
      "entityType": "office365_emails_email",
      "payload": {
      "reasons_by_category": {
                "sender_reputation": [{
                "short_text": "Insignificant historical reputation with sender",
                "full_text": "The sending email address hasn't established significant historical reputation with your
domain"
                },
                {
                "short_text": "Low-traffic 'From'-domain",
                "full_text": "The sender's domain has very low traffic - often indicating low-trust domains"
                }
                ],
                "links": [{
                "short_text": "Link to a low-traffic site",
                "full_text": "The email contains link to low-traffic web-sites - often indicating low-trust domains"
                }]
      }
      },
      "score": "526.670776",
      "securityResultEntityId": "a60ca316d8c4f19a2923114380fb0070",
      "securityResultEntityType": "avanan_ap_scan",
      "statusCode": "0",
      "statusDescription": null,
      "verdict": "phishing"
      }],
      "dlp": null,
      "clicktimeProtection": null,
      "shadowIt": [{
      "entityId": "a60ca316d8c4f19a2923114380fb0070",
      "entityType": "office365_emails_email",
      "payload": {
      "subject": "TEST-0429-1619902351-15",
      "from": "user@email.com"
      },
      "score": "0.0",
      "securityResultEntityId": "a60ca316d8c4f19a2923114380fb0070",
      "securityResultEntityType": "shadow_it_emails_scan",
      "statusCode": "clean",
      "statusDescription": "Clean",
      "verdict": "clean"
      }],
      "av": null
    },
   "entityActions": [
    {}
   ],
   "entityAvailableActions": [
    {
     "entityActionName": "quarantine",
     "entityActionParam": ""
    },
    {
     "entityActionName": "restore",
     "entityActionParam": ""
    }
   ]
  }
 ]
}
```

Action API

1. /action/event - Perform an action on AVANAN security events

- **URI - POST**

  To use this endpoint send a POST request to perform a single action on a specific security event or multiple events (a single action is supported per multiple events)

```
/action/event
```

- **Request**

  The request includes HTTP headers (obtained on the authentication/authorization process and used to sign the request) alongside with request parameters posted on the request body.

- **Request Headers**

Header	TYPE	Required	Format	Description/Sample
x-av-req-id	String	Y	UUID – generated and supplied on the request	d290f1ee-6c54-4b01-90e6-d701748f0851
x-av-token	String	Y	Token obtained on the authentication sequence	tkn8546ffffggd9d8934593
x-av-app-id	String	Y	Application ID provided by AVANAN	myapp29
x-av-date	String	Y	Date-time in GMT	'2016-08-29T09:12:33.001Z'
x-av-sig	String	Y	Calculated signature	tkn8jmveolrrtertr9d8934593

- **Request String Parameters**

  None

- **Request Body**

  All applicable request parameters are posted on the request body JSON :

```
{
  "requestData": {
   "scope”: "string",
   "eventIds": ["string"],
   "eventActionName": ["string"],
   "eventActionParam": ["string"]
   }
}
```

- **Request Body Parameters**

  The JSON parameters are as follows :

Parameter	TYPE	Required	Format	Description/Sample
requestData	Object			A container for action request
scope	String			Single scope string
entityIds	Array of String	Y		This is an array of event id identifiers that the single action applies to
eventActionName	String	Y		Action name to be taken
eventActionParam	String			Optional string with all action parameters

- **Request sample (CURL) format**

```
curl -X POST -H “Accept: application/json” \
       -H “x-av-req-id: d290f1ee-6c54-4b01-90e6-d701748f3351” \
       -H “x-av-token: tkn8546ffffggd9d8934593” \
       -H “x-av-app-id: myapp29” \
       -H “x-av-date: 2016-08-29T09:12:33.001Z” \
       -H “x-av-sig: tkn8jmveolrrtertr9d8934593” \
       -d “{"requestData": {"scope": "us:customername", "eventIds":
["7ded0371a3e1475c9a877e452f23a049"],"eventActionName": ["dismiss"],"eventActionParam": [""]} }” \
       https://smartapi-prod-us-1.avanan.net/v1.0/action/event
```

The above will dismiss the event with event id: “7ded0371a3e1475c9a877e452f23a049”

- **Response**

  The response obtained from the service includes HTTP response code and JSON formatted structure. The JSON structure contains response envelope and response data which include a detailed response code for the action per each **entityId** in the request

- **Response Structure**

  The following is a valid response obtained from the service (JSON format):

```
{
 "responseEnvelope": {
  "requestId": "string",
  "responseCode": integer,
  "responseText": "string",
  "additionalText": "string",
  "recordsNumber": integer,
  "totalRecordsNumber": integer,
  "scrollId": "string"
 },
 "responseData": [
   {
    "eventId": "string",
    "entityId": "string",
    "taskId": integer
   }
 ]
}
```

- **Response Parameters**

  The following are the response parameters:

Parameter		**Type**	**Description**
responseEnvelope		Object	A container of metadata properties
	requestId	Integer	Request Id (from the request header **x-av-req-id** value)
	responseCode	Integer	0 is success, other value failure
	responseTest	String	Text value of response
	additionalText	String	Extra information
	recordsNumber	Integer	Number of records is response
	totalRecordsNumber	Integer	Total number of records

	scrollId	String	Unique ID used for scrolling
responseData		Object	Array of security event identifiers and their corresponding action response codes and additional text
	eventId	String	Security event id the action applies to
	entityId	String	AVANAN event SaaS entity id the action applies to
	taskId	Integer	Unique ID of the Avanan task

- **Response Sample**

  The following is a valid response from the service:

```
{
 "responseEnvelope": {
  "requestId": "d290f1ee-6c54-4b01-90e6-d701748f3351",
  "responseCode": 0,
  "responseText": "success",
  "additionalText": "",
  "recordsNumber": 1,
  "totalRecordsNumber": 1,
  "scrollId": "9898989898"
 },
 "responseData": [
   {
    "eventId": "7ded0371a3e1475c9a877e452f23a049",
    "entityId": "a60ba316c8d4f19b2913194386fb0070",
    "taskId": "123445311234"
   }
 ]
}
```

2. /action/entity - Perform Action on AVANAN SaaS entities (by AVANAN entity ID)

- **URI - POST**

  To use this endpoint you send a POST request to perform a single action on a specific security event or multiple events (a single action is supported per multiple events)

```
/action/entity
```

- **Request**

  The request includes HTTP headers (obtained on the authentication/authorization process and used to sign the request) alongside with request parameters posted on the request body.

- **Request Headers**

Header	TYPE	Required	Format	Description/Sample
x-av-req-id	String	Y	UUID – generated and supplied on the request	d290f1ee-6c54-4b01-90e6-d701748f0851
x-av-token	String	Y	Token obtained on the authentication sequence	tkn8546ffffggd9d8934593
x-av-app-id	String	Y	Application ID provided by AVANAN	myapp29
x-av-date	String	Y	Date-time in GMT	'2016-08-29T09:12:33.001Z'
x-av-sig	String	Y	Calculated signature	tkn8jmveolrrtertr9d8934593

- **Request String Parameters**

  None

- **Request Body**

  All applicable request parameters are posted on the request body JSON :

```
{
  "requestData": {
    "scope": "string",
    "entityIds": ["string"],
    "entityActionName": ["string"],
    "entityActionParam": ["string"]
    }
}
```

- **Request Body Parameters**

  The JSON parameters are as follows :

Parameter	TYPE	Required	Format	Description/Sample
requestData	Object			A container for action request
scope	String			Single scope string
entityIds	Array of String	Y		This is an array of entity id identifiers that the single action applies to
eventActionName	String	Y		Action name to be taken
eventActionParam	String			Optional string with all action parameters

- **Request sample (CURL) format**

```
curl -X POST -H “Accept: application/json” \
        -H “x-av-req-id: d290f1ee-6c54-4b01-90e6-d701748f3351” \
        -H “x-av-token: tkn8546ffffggd9d8934593” \
        -H “x-av-app-id: myapp29” \
        -H “x-av-date: 2016-08-29T09:12:33.001Z” \
        -H “x-av-sig: tkn8jmveolrrtertr9d8934593” \
        -d “{"requestData": {"entityIds": ["6bb51619b0bb6a5a2ed3315ea1968435"],"entityActionName":
["quarantine"],"entityActionParam": [""]} }” \
        https://smartapi-prod-us-1.avanan.net/v1.0/action/entity
```

The above will quarantine the saas entity who’s AVANAN entity id is

“6bb51619b0bb6a5a2ed3315ea1968435”

- **Response**

  The response obtained from the service include HTTP response code and JSON formatted structure. The JSON structure contains response envelope and response data which include a detailed response code for the action per each **entityId** in the request

- **Response Structure**

  The following is a valid response obtained from the service (JSON format):

```
{
 "responseEnvelope": {
  "requestId": "string",
  "responseCode": integer,
  "responseText": "string",
  "additionalText": "string",
  "recordsNumber": integer,
  "totalRecordsNumber": integer,
  "scrollId": "string"
 },
 "responseData": [
   {
    "entityId": "string",
    "taskId": "integer"
   }
 ]
}
```

- **Response Parameters**

  The following are the response parameters:

Parameter		Type	Description
responseEnvelope		Object	A container of metadata properties
	requestId	Integer	Request Id (from the request header **x-av-req-id** value)
	responseCode	Integer	0 is success, other value failure
	responseTest	String	Text value of response
	additionalText	String	Extra information
	recordsNumber	Integer	Number of records is response
	totalRecordsNumber	Integer	Total number of records

	scrollId	String	Unique ID used for scrolling
responseData		Object	Array of security event identifiers and their corresponding action response codes and additional text
	entityId	String	AVANAN SaaS entity id the action applies to
	taskId	Integer	Unique ID of the Avanan task

- **Response Sample**

  The following is a valid response from the service:

```
{
 "responseEnvelope": {
  "requestId": "d290f1ee-6c54-4b01-90e6-d701748f3351",
  "responseCode": 0,
  "responseText": "success",
  "additionalText": "",
  "recordsNumber": 1,
  "totalRecordsNumber": 1,
  "scrollId": "9898989898"
 },
 "responseData": [
   {
    "entityId": "7ded0371a3e1475c9a877e452f23a049",
    "taskId": "123445311234"
   }
 ]
}
```

3. (not available yet) - /action/query - Perform Action on AVANAN SaaS entities (by filter/condition)

- **URI - POST**

  To use this endpoint you send a POST request to perform a single action on AVANAN SaaS entities. This is done by specifying a query filter (same filter as for entities query).

```
/action/query
```

- **Request**

  The request includes HTTP headers (obtained on the authentication/authorization process and used to sign the request) alongside with request parameters posted on the request body.

- **Request Headers**

Header	TYPE	Required	Format	Description/Sample
x-av-req-id	String	Y	UUID – generated and supplied on the request	d290f1ee-6c54-4b01-90e6-d701748f0851
x-av-token	String	Y	Token obtained on the authentication sequence	tkn8546ffffggd9d8934593
x-av-app-id	String	Y	Application ID provided by AVANAN	myapp29
x-av-date	String	Y	Date-time in GMT	'2016-08-29T09:12:33.001Z'
x-av-sig	String	Y	Calculated signature	tkn8jmveolrrtertr9d8934593

- **Request String Parameters**

  None

- **Request Body**

  All Applicable request parameters are posted on the request body JSON:

```
{
 "requestData": {
  "entityFilter": {
   "saas": "string",
   "saasEntity": "string",
   "startDate": "DateTime",
   "endDate": "DateTime"
  },
  "entityExtendedFilter": [
   {
    "saasAttrName": "string",
    "saasAttrOp": "string",
    "saasAttrValue": "string"
   }
  ],
  "entityActionName": "string",
  "entityActionParam": "string"
 }
}
```

- **Request Body Parameters**

  The JSON parameters are as follows:

Parameter	TYPE	Required	Format	Description/Sample
requestData	Object			A container for action request
entityFilter	Object			A container for generic query filter (apply to all entities) - see below

entityFilter object:

Parameter	TYPE	Required	Format	Description/Sample
entityFilter/saas	string	Y		Name of required SaaS. Possible values: email sharefile slack ms_teams

				office365_emails office365_onedrive office365_sharepoint google_mail box dropbox
entityFilter/ saasEntity	String			Name of SaaS entity. Possible values: Message, file user
entityFilter/ startDate	String	Y	Date-time	Start of required time frame. Sample: ‘2019-04-10T09:12:33.001Z'
entityFilter/ endDate	String	Y	Date-time	End of required time frame. Sample: '2019-04-11T09:12:33.001Z'
entityExtendedFilter	Object			A container for SaaS specific extended query filter
entityExtendedFilter/ saasAttrName	String			saas criteria attribute name
entityExtendedFilter/ saasAttrOp	String			saas criteria attribute Operator: “is”, “contains”, “startsWith”, “isEmpty”, “isNot” , “notContains”, “isNotEmpty”, “greaterThan”,”lessThan”
entityExtendedFilter/ saasAttrValue	String			saas criteria attribute value
eventActionName	String	Y		Action name to be taken
eventActionParam	String			Optional string with all action parameters

- **Request sample (CURL) format**

```
curl -X POST -H “Accept: application/json” \
      -H “x-av-req-id: d290f1ee-6c54-4b01-90e6-d701748f3351” \
      -H “x-av-token: tkn8546ffffggd9d8934593” \
      -H “x-av-app-id: myapp29” \
      -H “x-av-date: 2021-04-10T09:12:33.001Z” \
      -H “x-av-sig: ”7386a58182056205cee90e472ec3cc8518a4b8a4abcab9fc15d7b461779d664f” \
      -d “
                              {
                                "requestData": {
```

```
                           "entityFilter": {
                            "saas": "email",
                            "saasEntity": "",
                            "startDate": "2020-01-01T00:00:00.000Z",
                            "endDate": ""
                           },
                           "entityExtendedFilter": [
                            {
                                    "saasAttrName": "entityPayload.fromEmail",
                                    "saasAttrOp": "is",
                                    "saasAttrValue": "hacker@malicious.com"
                            }
                           ],

                                   "entityActionName": "quarantine",
                                   "entityActionParam": ""
                            }
                         }
” \
     https://smartapi-prod-us-1.avanan.net/v1.0/action/query
```

The above will quarantine all emails starting Jan 1st 2020 sent from hacker@malicious.com

- **Response**

  The response obtained from the service includes HTTP response code and JSON formatted structure. The JSON structure contains response envelope and response data which include a detailed response code for the action per each **entityId** in the request

- **Response Structure**

  The following is a valid response obtained from the service (JSON format):

```
{
 "responseEnvelope": {
  "requestId": "string",
  "responseCode": integer,
  "responseText": "string",
  "additionalText": "string",
  "recordsNumber": integer,
  "totalRecordsNumber": integer,
  "scrollId": "string"
 },
 "responseData": [
   {
    "entityId": "string",
    "customerId": "string",
    "entityActionResponseCode": integer,
    "entityActionResponseText": "string"
   }
 ]
}
```

- **Response Parameters**

  The following are the response parameters:

Parameter		Type	Description
responseEnvelope		Object	A container of metadata properties
	requestId	Integer	Request Id (from the request header **x-av-req-id** value)
	responseCode	Integer	0 is success, other value failure
	responseTest	String	Text value of response
	additionalText	String	Extra information
	recordsNumber	Integer	Number of records is response
	totalRecordsNumber	Integer	Total number of records
	scrollId	String	Unique ID used for scrolling
responseData		Object	Array of security event identifiers and their corresponding action response codes and additional text

	entityId	String	AVANAN SaaS entity id the action applies to
	customerId	String	AVANAN customer Id
	entityActionResponseCode	Integer	The action response code (0 for success)
	entityActionResponseText	String	Additional action response text

- **Response Sample**

  The following is a valid response from the service:

```
{
 "responseEnvelope": {
  "requestId": "d290f1ee-6c54-4b01-90e6-d701748f3351",
  "responseCode": 0,
  "responseText": "success",
  "additionalText": "",
  "recordsNumber": 2,
  "totalRecordsNumber": 2,
  "scrollId": "9898989898"
 },
 "responseData": [
   {
    "entityId": "7ded0371a3e1475c9a877e452f23a049",
    "customerId": "us:customername",
    "entityActionResponseCode": 0,
    "entityActionResponseText": "success"
   },
   {
    "entityId": "7ded037195869889t9877e452f23a049",
    "customerId": "us:customername",
    "entityActionResponseCode": 0,
    "entityActionResponseText": "success"
   }
 ]
}
```

Task API

4. /task/{taskId} - Search for a specific AVANAN Task entity

- **URI - GET**

  To use this endpoint send a GET request to get the state of action enqueued.

```
/task/{taskId}
```

- **Request**

  The request includes HTTP headers (obtained on the authentication/authorization process and used to sign the request) alongside with request string parameters.

- **Request Headers**

Header	TYPE	Required	Format	Description/Sample
x-av-req-id	String	Y	UUID – generated and supplied on the request	d290f1ee-6c54-4b01-90e6-d701748f0851
x-av-token	String	Y	Token obtained on the authentication sequence	tkn8546ffffggd9d8934593
x-av-app-id	String	Y	Application ID provided by AVANAN	myapp29
x-av-date	String	Y	Date-time in GMT	'2016-08-29T09:12:33.001Z'
x-av-sig	String	Y	Calculated signature	tkn8jmveolrrtertr9d8934593

- **Request String Parameters**

Parameter	TYPE	Required	Format	Description/Sample
taskId	String	Y		AVANAN Task Id, such as: “4b8312c5b04d4a6d884662237fa2e25d”

- **Query String**

Query	TYPE	Required	Format	Description/Sample
scope	String	N		Single scope string

- **Request Body**

  Not applicable on GET

- **Request sample (CURL) format**

```
curl -X GET -H “Accept: application/json” \
     -H “x-av-req-id: d290f1ee-6c54-4b01-90e6-d701748f0851” \
     -H “x-av-token: tkn8546ffffggd9d8934593” \
     -H “x-av-app-id: myapp29” \
     -H “x-av-date: 2016-08-29T09:12:33.001Z” \
     -H “x-av-sig: tkn8jmveolrrtertr9d8934593” \
     https://smartapi-prod-us-1.avanan.net/v1.0/task/4b8312c5b04d4a6d884662237fa2e25d
```

- **Response**

  The response obtained from the service includes HTTP response code and JSON formatted structure.

- **Response Structure**

  The following is a valid response obtained from the service (JSON format):

```
{
 "actions": [{
        "action_created": "string",
        "action_id": "string",
        "action_name": "string",
        "action_status": "string",
        "action_type": "string",
        "action_updated": "string",
        "hash_key": "string"
 }],
 "created": "string",
 "customer": "string",
 "id": "numeric",
 "name": "string",
 "owner": "string",
 "progress": "numeric",
 "sequential": "boolean",
 "status": "string",
 "total": "numeric",
 "type": "string",
 "updated": "string"
}
```

- **Response Parameters**

  The following are the response parameters:

Parameter		Type	Description
responseEnvelope		Object	A container of metadata properties
	requestId	String	Request Id (from the request header **x-av-req-id** value)
	responseCode	Integer	0 is success, other value failure
	responseTest	String	Text value of response
	additionalText	String	Extra information
	recordsNumber	Integer	Number of record is response
	totalRecordsNumber	Integer	Total number of records
	scrollId	String	Unique ID used for scrolling
responseData		Object	Array of event entities
	actions	Array of Object	Array of action data
	created	String	A date when the task was created
	customer	String	Customer name
	id	String	Unique ID of the task
	name	String	Name of the task
	owner	String	Owner’s email
	progress	Integer	Progress indicator
	sequential	Boolean	Sequential flag
	status	String	init, inprogress, completed, failed, stopped, paused
	total	Integer	Total number

	type	String	Action type
	updated	String	Date when action was updated

- **Response Sample**

The following is a valid response from the service:

```
{
 "responseEnvelope": {
        "requestId": "d290f1ee-6c54-4b01-90e6-d701748f3351",
        "responseCode": 0,
        "responseText": "success",
        "additionalText": "",
        "recordsNumber": 1,
        "scrollId": "9898989898"
 },
 "responseData": {
        "actions": [{
        "action_created": "2021-08-04 11:45:38.823008",
        "action_id": "1628077538822988",
        "action_name": "Quarantine 14cc6d3aec558cca4de1363166fa42f9",
        "action_status": "init",
        "action_type": "Quarantine_14cc6d3aec558cca4de1363166fa42f9",
        "action_updated": "2021-08-04 11:45:38.823015",
        "hash_key": "us##customername##1628077538799978"
        }],
        "created": "2021-08-04 11:45:38.799984",
        "customer": "customername",
        "id": 1628077538799978,
        "name": "Office365 Emails Manual Action",
        "owner": "service@avanan.com",
        "progress": 0,
        "sequential": true,
        "status": "inprogress",
        "total": 1,
        "type": "office365_emails_manual_action",
        "updated": "2021-08-04 11:45:38.800076"
 }
}
```