Security Awareness Training API

https://campus.barracuda.com/doc/79463896/

The Security Awareness Training REST API provides remote administration and configuration of Security Awareness Training. This article gives a brief description of REST API and the API methods you can use to access your Security Awareness Training.

Representational State Transfer (REST) is a stateless architecture that runs over HTTP. REST API is a simple web service API you can use to interact with Security Awareness Training. For more information on REST API, visit http://en.wikipedia.org/wiki/Representational_state_transfer.

Security Awareness Training API

API Endpoint	Functions	Permission Required
Authentication	• Create an access token	None. Uses API key, username, and password.
Campaign	• Read data of a campaign • Get all basic campaign data for all campaigns	Email Campaign – Can Edit All
CampaignResult	• Get all outbound campaign results	Email Campaign – Can Edit All
Web Activity	• Get all activity from a user's interactions with a campaign.	One of the following: • Email Campaign – Can Edit All • Email Campaign Results – Can View All

For an example of writing Security Awareness Training API in PHP, refer to Example - API in PHP.

Getting Started

User Account Setup

To set up a new user with API access:

> **Note:** An API User account cannot be used except for API access. Do not try to use a normal user account. The API users do not use SSO / OAuth2, but all normal user accounts do use SSO / OAuth2.

1. Navigate to **System > User Manager**. Click **New**.
2. Choose a name and create the new user. Example: `APIUser1@example.com.` A real email address should be used because the email address may be used for contacting in case of error.

3. These are the only settings that need to be filled out:
    - Authentication: Active
    - Authentication: Password
    - Group membership: Add "Email Campaign – Can Edit All". This will give access to the 3 currently available endpoints - /campaign, /campaignresult, /webactivity.
    - Group membership: Add "Everyone – All Users Must Be In This Group". This is selected by default.
4. Click **Save**. Note: this will automatically check the **Force Password Expire** checkbox. You must uncheck this box and click **Save** a second time.

REQUIRED: API KEY SETUP

1. Go to System -> API Keys and generate a new API key.
2. OPTIONAL: Assign the API key to only be used by a specific user. I am creating and assigning this new API key to the user I created, `ApiUser1@example.com`.
3. OPTIONAL: CHANGE API KEY AND USER PASSWORD EXPIRATION SETTINGS

Go to System -> Global Settings -> Default Security Settings and modify the expiration time for API keys and/or passwords.

Getting API Access

Security Awareness Training user accounts are used to access the API. In addition, you will need to acquire an API key. API keys can be generated by administrators from the Security Awareness Training interface, under "**System** > **API Keys**". Note that API keys expire after 1 year.

Base API URL

The base API URL is: `https://api.phishline.com/<phishline_example>/rest`. Substitute your instance name for `<phishline_example>`.

Endpoints add to the URL. For example, the '/authenticate' endpoint will be `https://api.phishline.com/<phishline_example>/rest/authenticate`. Again, substitute your instance name for `<phishline_example>`.

Using the API key

The API key, username, and password are used to make a call to the authentication endpoint per the /authenticate endpoint section.

Using the Access Token

After retrieving an access token from /authenticate, include it with all subsequent requests.

The token can be passed in the query string OR as an `Authorization: Bearer` header.

Query string example:

```
https://api.phishline.com/<phishline_example>/rest/campaign/1?access_token=28
3efd73abd654cf92fd8g7a23742
```

Header example

If this header was sent, and the token was valid:

```
Authorization: Bearer 283efd73abd654cf92fd8g7a23742
```

Then this would be a valid GET request:

```
 https://api.phishline.com/<phishline_example>/rest/campaign/1
```

If you receive an authorization error (HTTP code 401), retrieve a new access token from the /authenticate endpoint.

Access tokens are guaranteed to expire after 24 hours, and may expire much more quickly based on the last time it was used. Access tokens that have not been used for a period of time may expire before 24 hours.

API Envelope

The envelope for your request will have the following attributes.

- **jobid** - If a job cannot be completed in a timely manner, you may receive a jobid instead. This is provided for future enhancement.
- **status**: This will be the same as the HTTP status returned.
- **statusMessage**: This is the short human readable name of the result of the request. In case of error, please reference this error in this API documentation.
- **statusDetails**: If the status requires more in-depth details, they will be enumerated here as an array of objects. This will often include the number of total results.
- **entity**: The name of the returned object(s) (if any). For example, "campaign". In case of error, the type may be "unknown".
- **notifications**: You will receive notifications including, but not necessarily limited to:
  - The number of API calls allowed.
  - The number of API calls completed.
  - The expiration date for your API key.
- **totalRowCount**: The total number of rows the request returned or could return. The maximum number of rows a request can return is 5,000.
- **pageRowCount**: The number of rows returned in this request.
- **remainingRowCount**: The remaining number of rows available to request.
- **MaxIdReturned**: The maximum record id returned in the current request.
- **data**: If data is returned, it is returned as an array of objects, even if there is only one item

returned. Even if there are 0 returned results, the data array will be present on requests that are expected to return data.

A note about data types

All data returned in the "data" section of the envelope will be string data. You will need to convert data to other variable types as required. The endpoint documentation will show you the variable types you can expect to be able to convert the data to.

HTTP Requirements

When sending requests, note the following:

- Unless otherwise noted, when posting data, only `Content-Type: application/json` is accepted.
- Any endpoint that is not available via public API will return a 405 NOT ALLOWED error.

Authorization Requirements

- All endpoints except /authentication will require an access_key. Access keys are generated from the /authentication endpoint.
- Be aware that a user account being used for API access must have the appropriate access levels assigned in the User Manager. For example, if a user cannot browse to "Results -> Outbound Analysis", they will also not be able to use the /campaignresults/ endpoint.