Authentication

https://campus.barracuda.com/doc/79463957/

Permission Required to use this API Endpoint

Requires API key, username, and password. No additional permission is required.

Create an access token

Post your username, password, and API key to receive an access token for all other actions. All other actions will require a valid access token created from this endpoint. If the token becomes invalid, retrieve another one with this endpoint. The token expires every 24 hours (maximum), but might expire before then. If it expires, call the authenticate endpoint again.

Make your API requests from the same IP address you used when retrieving your access token. If you use a different IP address, your API calls will be unsuccessful, returning a `401 – Not Authorized` response.

POST /authenticate

Parameters

Name	Type	Description
bof_ticket_user	String	Your assigned username.
bof_ticket_pw	String	Your assigned password.
api_key	String	Your assigned key.
sso	String	Optional; only required if you are using RestAPI OAUTH2/ODIC authentication. The only valid value is **oauth2** .
bof_sso_config_id	Integer	Optional; only required if you set the **sso** parameter. This is the BSAT SSO Configuration Id for the SSO Configuration you created in BSAT, specifically for the RestAPI OAUTH2/ODIC authentication. See Single Sign-On with OAUTH2/ODIC for instruction on how to setup an RestAPI OAUTH2/ODIC identity provider.

Examples and usage

```
curl -X POST -H "Content-Type: application/json" -H "Cache-Control: no-cache"
-d '{
"bof_ticket_user": "USERNAME",
"bof_ticket_pw": "PASSWORD",
"api_key": "AAAAAAAA-BBBB-CCCC-YYYY-XXXXXXXXXX"
}' "https://api.phishline.com/phishline_example/rest/authenticate"
```

Success Response and example

```
HTTP/1.1 200 OK
{
 "status": 200,
 "statusMessage": "OK",
 "statusDetails": {
 "Reason": "Authentication created."
 },
 "entity": "accesstoken",
 "jobid": 0,
 "notifications": {
 "API Token Expiration Date": "N\/A",
 "Maximum API calls per hour": 1000,
 "Your API calls in the last hour": 7
 },
 "data": {
 "access_token": "ab34ef56gbdgbb139215nda72751111e64e"
 }
}
```

Success 200

Name	Type	Description
access_token	String	The access token. You will use this access token either in the query string, or as an Authorization header, named 'access_token' on all subsequent API calls.

Error 4xx

Name	Type	Description
NotAuthenticated		Your attempt to authenticate failed. Please check your credentials and try again.
NotAuthorized		Authentication failure: Bad API Key.

Error Response

Response (example):

```
HTTP/1.1 401 Not Authorized
{
 "status": 401,
 "statusMessage": "NotAuthorized",
 "statusDetails": {
 "Reason": "Authentication failure: Bad API Key."
 },
 "entity": "unknown",
 "jobid": 0,
 "notifications": [],
 "data": []
}
```