REST API Version 3 (v3)

https://campus.barracuda.com/doc/73698479/

In this article:

The Barracuda Web Application Firewall supports a comprehensive REST API module for management and configuration. Version 3.2 is the latest version of the REST API and previous versions of API are v3 and v3.1. Documentation for the API v3.2 and earlier versions is available at:
https://campus.barracuda.com/product/webapplicationfirewall/api

Accessing the API in Version 3

This section describes how to invoke a REST API call on the Barracuda Web Application Firewall and the expected response.

The REST API supports both HTTP and HTTPS URI requests. HTTP and HTTPS requests should include the respective port number (i.e., port 8000 for HTTP and 8443 for HTTPS).

API Endpoint

The Barracuda Web Application Firewall REST API endpoint for making calls with the access token is “/restapi”, for example, http://<IP address of BWAF>: 8000/restapi
Combine the endpoint with the API version number and appropriate resource URL to make a call.

Example: To create a service group under a specific Vsite, the REST API call is http://{IP address of WAF}:8000/restapi/{api version}/vsites/{vsite_id}/service_groups/{service_group_id} .

REST API Request Format

- http://{IP address of BWAF}:8000/restapi/v3.2/{object_id}

- https://{IP address of BWAF}:8443/restapi/v3.2/{object_id}

Where:

- **http/https** – Protocol used to invoke a REST API call.
- **IP address of BWAF** – IP address of the Barracuda Web Application Firewall to access.
- **8000/8443** – Port number.
- **restapi** – Name of the API.
- **v3.2** – REST API version on the Barracuda Web Application Firewall.
- **object_id** – Name of the object to be created/retrieved/modified/deleted. An object may be a service, security policy, certificate, etc.

In order to use the Barracuda WAF REST API, a login access token is required for authentication. Login credentials with admin privileges or a role-based administrator with restricted permissions can be used.

Content-Type Header

All POST and PUT requests should include the Content-Type header with the value as “application/json”.

Getting the Login Access Token

The login request must include the username and password to generate the token. HTTP and HTTPS request examples are provided below for reference:

HTTP Login Request

Example:

Request:

```
curl -X POST http://10.36.73.160:8000/restapi/v3.2/login -H "Content-Type: application/json" -d
'{"username": "admin", "password": "admin"}'
```

Response:

```
{"token":"eyJldCI6IjEIiwidXNlciI6ImFkbWluIn0=\n"}
```

HTTPS Login Request

For HTTPS requests, the Barracuda Web Application Firewall uses the certificate that is configured for the management access, specified in the **ADVANCED > Secure Administration > SSL Certificate Configuration** section. The example below shows the login request for HTTPS with the following details:

Example:

Request:

```
curl -k -X POST https://10.36.73.160:8443/restapi/v3.2/login -H "Content-Type: application/json"
-d '{"username": "admin", "password": "admin"}'
```

Response:

```
{"token":"eyJldCI6IjyIiwidXNlciI6ImFkbWluIn0=\n"}
```

In the example above, -k flag is used with the curl command to ignore the SSL certificate error. This is required if the default self-signed certificate of the Barracuda WAF's management interface is used. If a certificate issued by a public CA is used, -k flag is not required.

Logout Request

HTTP Logout Request

Example:

Request:

```
curl -X DELETE http://10.36.73.160:8000/restapi/v3.2/logout -u
'eyJ1cRiIiwiZXQiOiIxNjI2MDcyMDM2In0=\n:'
```

Response:

```
{"msg":"Token deleted successfully."}
```

HTTPS Logout Request

Example:

Request:

```
curl -k -X DELETE https://10.36.73.160:8443/restapi/v3.2/logout -u
'eyJ1c2VyIjZXQiOiIxNjI2MDcyMjIyIn0=\n:'
```

Response:

```
{"msg":"Token deleted successfully."}
```

All examples provided here use the HTTP protocol. You can modify it to use HTTPS by making the required protocol and port changes.

Using the Token

The generated token is embedded with the username, password, and timestamp. For this reason, every request made by the user should include the generated token followed by a colon (:).
See the example below.

Example 1: Using the login token to fetch all the services from the WAF

Request:

```
curl -X GET http://10.36.73.160:8000/restapi/v3.2/services -u
'eyJwYXNzd29yZCNjI2MDcyODkxIn0=\n:'
```

Response:

```
{
"data": {
"auth0": {
"Mask Sensitive Data": {
"sensitive-parameter-names": ""
},
"Slow Client Attack Prevention": {
"incremental-request-timeout": "30",
"exception-clients": "",
"status": "Off",
"max-request-timeout": "600",
"data-transfer-rate": "10",
"incremental-response-timeout": "30",
"max-response-timeout": "600"
},
"URL Encryption": {
"status": "Off"
},
"name": "auth0",
<.........>,
"object": "Service",
"token": "eyJldCDZlNzJhM2JkOGU4ZDUzY2NlMzhhIn0=\n"
}
```

The above response data has been snipped in the middle (shown as <.........>).

Next Step:

Continue with REST API Request and Response Types.

Related Article:

- How to Generate API Calls