Authentication

Contents on this Page

POST /auth

Endpoint

/auth

Method

POST

Request parameters

Name	Required
username	Y
password	Y

Response


```
{
    "response": {
        "status": "OK",
        "logged_in": true,
        "token": "t1nrm15okcel715d2c0oilgev2"
    },
    "audit": {
        "user": false,
        "user_id": false
    },
    "debug": {
        "parsetime": "2,314.006090",
        "now": "2014-03-28 14:35:11"
    },
 "csrf":"ac8cf752c04a2fabcc1d66db5f662b28"
 }
```

Subsequent requests will allow you to see the logged in user:

```
{
 "response":{
  "status":"OK",
  "logged_in":true
 },
 "audit":{
  "user":"Demo Summit",
  "user_id":"380"
 },
 "debug":{
  "parsetime":"50.677061",
  "now":"2014-03-28 14:28:40"
 },
 "csrf":"ac8cf752c04a2fabcc1d66db5f662b28"
}
```

Example

```
curl -b cookies.txt -c cookies.txt --data
"username=[username]&password=[password]"
"https://platform.flxone.com/api/auth"
```

Use the ‘token’ received to perform future calls. This token should be placed as string value into the ‘X-Auth’ header.

The token expires after 30 minutes of inactivity. Instead of a token you can also use session cookies.

If sending any other POST request you will need to read the CSRF parameter and add it to the POST request using the X-CSRF header. The CSRF token stays the same for the duration of the session. The CSRF parameter is also included on all subsequent requests. The CSRF parameter is used to prevent CSRF requests, see http://en.wikipedia.org/wiki/Cross-site_request_forgery

http://en.wikipedia.org/wiki/Cross-site_request_forgery