

Swagger UI with Tek NS US:

1. Enter the following command from Linux machine to get JWT token. Make sure the Linux machine has necessary curl packages installed.

Linux Command:

The **username** and **password** fields highlighted below should be your login username and password used to login to the Tektelic Network Server <https://lorawan-ns-na.tektelic.com>.

```
curl -X POST --header 'Content-Type: application/json' --header 'Accept: application/json' -d
'{"username":"your_username ", "password":"your_password"}' "https://lorawan-ns-
na.tektelic.com/api/auth/login" | grep -o ""token": "[^"]*" | grep -o '[^"]*$/
```

After entering the above curl command, it would give you the token like this.

```
eyJhbGciOiJIUzUxMiJ9eyJzdWliOiJkbWFyY2hhcmxhQHRIa3RlbGljLmNvbSIsInNjb3Blcyl6WyJDVVNU
T01FUI9BR
E1JTIjdLCJ1c2VySWQiOiI1NzU3MTdmMC0zYjJmLTEzWMMtYWMxYy0zMzg5NGFiYjQxYWliLCJmaXJzdE5hbWUi
OjEaGFudXNoaWsiLCJsYXN0TmFtZSI6Ik1hY2hhcmxhliwiZW5hYmxlZCI6dHJ1ZSwicHJvdmIkZXJJZCI6ljYxNjNiYzE
wLThjYTgtMTF1Ny1iYjjLThkZDlzNDg2MTQzMlsImN1c3RvbWVysWQioiI4NjU0MzY2MC00NGViLTExZTktODBh
MC1hMzZIM2ZiZWM0NzciLCJpc3MiOj0ZWt0ZWxpYy5jb20iLCJpYXQiOjE2NTY5NzA2NzcsImV4cCI6MTY1Njk3N
zg3N30.ENIXMJjeMSetkZ2tBUbs3y73pfYLALZOUgCtMU_cQqF6I-kujRnQ5ZpAzB0x9sH1R-
PRsU1jVNhGXzDzobJ1w
```

Windows Command:

```
C:\curl>curl -X POST --header "Content-Type: application/json" --header "Accept: application/json" -d
'{"username":"your_username","password":"your_password"}' "https://lorawan-ns-
na.tektelic.com/api/auth/login"
```

In this example I used US Instance. For EU instance please use '<https://lorawan-ns-eu.tektelic.com/api/auth/login>'

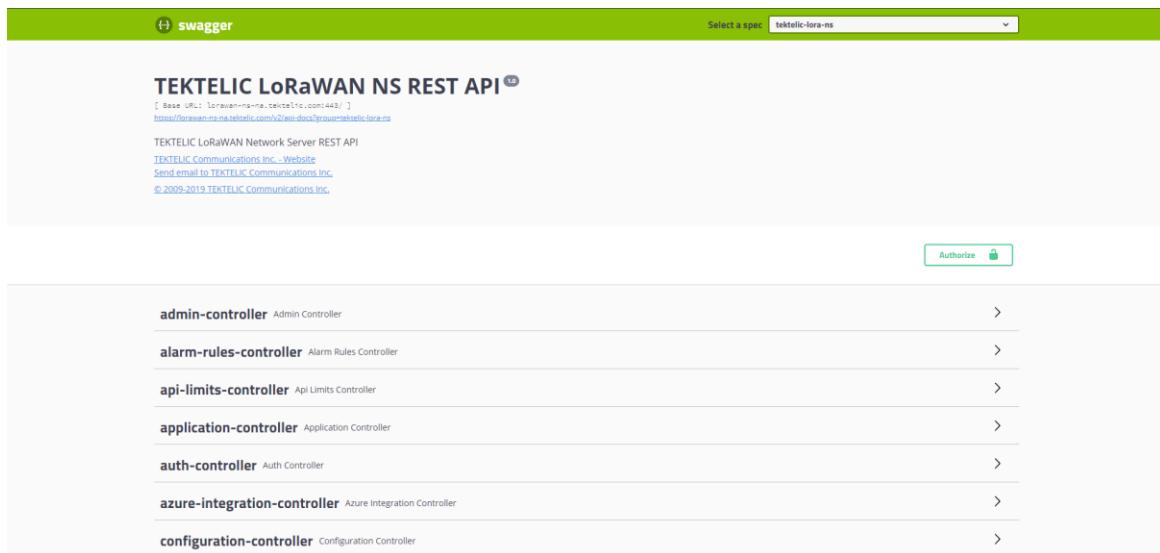
User name and Password – Login credentials to NS.

After entering the above curl command, it would give you the token like this.

```
{"token":"eyJhbGciOiJIUzUxMiJ9eyJzdWliOiJkbWFyY2hhcmxhQHRIa3RlbGljLmNvbSIsInNjb3Blcyl6WyJDVVNU
T01FUI9BR
E1JTIjdLCJ1c2VySWQiOiI1NzU3MTdmMC0zYjJmLTEzWMMtYWMxYy0zMzg5NGFiYjQxYWliLCJmaXJzdE5hbWUi
OjEaGFudXNoaWsiLCJsYXN0TmFtZSI6Ik1hY2hhcmxhliwiZW5hYmxlZCI6dHJ1ZSwicHJvdmIkZXJJZCI6ljYxNjNiYzE
wLThjYTgtMTF1Ny1iYjjLThkZDlzNDg2MTQzMlsImN1c3RvbWVysWQioiI4NjU0MzY2MC00NGViLTExZTktODBh
MC1hMzZIM2ZiZWM0NzciLCJpc3MiOj0ZWt0ZWxpYy5jb20iLCJpYXQiOjE2NTY5NzI5OTcsImV4cCI6MTY1Njk4MDE5N30.Gj10K6-
NYIqLEJWSJszRKn8YiZagAMxTLG_yP651upIsWNYj0eayAT9FmlFSOsvtRV0ykOr5tHVFK67HjpaOQ","refreshTok
en":"eyJhbGciOiJIUzUxMiJ9eyJzdWliOiJkbWFyY2hhcmxhQHRIa3RlbGljLmNvbSIsInNjb3Blcyl6WyJSRUZSRVNIX
1RPSOV0I0slnVzZJJZCI6ljU3NTcxN2YwLTNiMmYtMTFIYy1hYzFjLTmzODk0YWJiNDfhYilsImlcyl6InRla3RlbGlj
mNvbSIsImP0aSI6ljM1M2ZiNThhLWFkOTUtNGQ5Yy1hNDdjLWRINWYxZDAyNzY5ZilsImlhdcI6MTY1Njk3Mjk5N
ywiZXhwIjoxNjU3MDU5Mzk3fQ.EYWRi5EPM84TtDmyxExHI-
8R0GNWch0645DOFFwExwzg0XYHBCJ15coljjKpgS-YZQMHqAJXBQ_mT0CJJROnQ"}
```

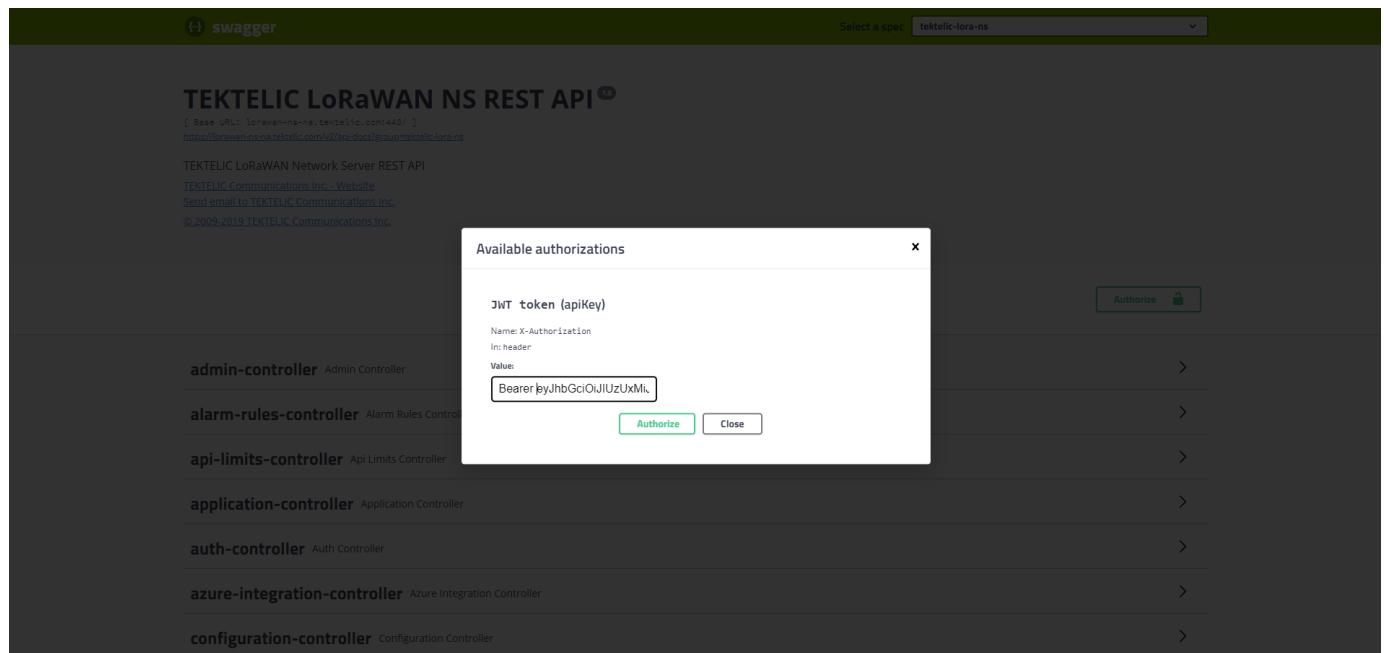
Then copy the first part of the token (as highlighted above), which is **JWT token**.

2. Go to swagger page for the Network Server: (In this example I used US Instance)
<https://lorawan-ns-na.tektelic.com/swagger-ui.html#/>



The screenshot shows the TEKTELIC LoRaWAN NS REST API homepage. At the top, there is a navigation bar with a 'swagger' icon, a dropdown menu set to 'tektelic-lora-ns', and a green 'Authorize' button. Below the header, the title 'TEKTELIC LoRaWAN NS REST API' is displayed along with its base URL: [Base URL: lorawan-ns-na.tektelic.com:443 /] <https://lorawan-ns-na.tektelic.com:443/swagger-ui.html#/>. Below the title, there is a brief description of the API and copyright information. The main content area lists several controllers: 'admin-controller' (Admin Controller), 'alarm-rules-controller' (Alarm Rules Controller), 'api-limits-controller' (Api Limits Controller), 'application-controller' (Application Controller), 'auth-controller' (Auth Controller), 'azure-integration-controller' (Azure Integration Controller), and 'configuration-controller' (Configuration Controller). Each controller entry has a right-pointing arrow icon.

Then click Authorize button. And type **Bearer** then give a space and paste the **JWT token** that you copied before. And then select Authorize button. You are logged in now.



The screenshot shows the same TEKTELIC LoRaWAN NS REST API homepage as the previous one, but with a modal dialog box titled 'Available authorizations' overlaid. The dialog contains a single item: 'JWT token (apiKey)'. It shows the 'Name: X-Authorization', 'In: header', and 'Value:' fields. The 'Value:' field contains the copied JWT token: 'Bearer eyJhbGciOiJIUzUxMi...'. At the bottom of the dialog are two buttons: 'Authorize' (highlighted in green) and 'Close'.

Then select the API that you want to get information from NS. In this example I selected Device-controller then selected “**GET /api/device/eui/{eui}**”. Then I entered the EUI for my device in the “value” field. Then select “Try it out!” button.

GET /api/device/eui/{eui} getDeviceByEui

Cancel

Parameters

Name	Description
eui <small>* required</small>	eui string (path) 647FDA00000088FF

Execute Clear

Responses

Response content type */*

Curl

```
curl -X GET "https://lorawan-ns-na.tektelec.com:443/api/device/eui/647FDA00000088FF" -H "accept: */*" -H "X-Authorization: Bearer eyJhbGciOiJIUzIwMiJ9.eyJzdWJtI01kbWFnY2hhcmxhQHRIa3R1bG1jLnNbSISmNb31cy16Wy.JDVNVNt01fUl9BRE1LT1dC1c2VvSwQ10i11NzU3MtdmNC68YjJmTEzWnTyWMxYy0zNzeSNGFiy1qYwM1iLCJmAxJzxE5hbMU1o1JEaFgudXHoNsWeilC3cYXN0tMftZS1G1k1hY2hhcmxhIw1Zm5hYmz1ZCT6dHJ1ZSw1chJvdmlkZXJ2C161YjxN1N1YjzEwLThjYTgtMTFlv1Yj1jLThkZD1zNdg2MTOzNS1sImN1c3RvbhVvSwQ10i14NjU0MzY2NC98NGViLTEzTktODbhMC1mMzz1M22iZWM0Nzc1lC3pc3M10iJ8t0ZwpxYy5jb28iLCjpyXQ10jE2NTyNzA2NzcsImV4c16HTy1Njk3Nzg3N30.ENIXMjjeMsckZ2tBuBs3y73pfYLALZ0UgCtMu_cQqF6I-ku)RnQ5ZpAzB89sH1lR-PRsU1jVNhGXzDzobJlw"
```

Request URL

https://lorawan-ns-na.tektelec.com:443/api/device/eui/647FDA00000088FF

You will get the response containing the information of the Device as shown below.

Request URL
<https://lorawan-ns-na.tektelec.com:443/api/device/eui/647FDA00000000FF>

Server response

Code	Details				
200	<p>Response body</p> <pre>{ "id": { "entityType": "DEVICE", "id": "3c7b0740-f401-11ec-ea28-f354b6ac8832" }, "createdTime": 1656184668852, "additionalInfo": null, "name": "dsrf", "deviceEUI": "647FDA00000000FF", "appEUI": "647FDA0000001009", "providerId": { "entityType": "PROVIDER", "id": "6163bc10-8ca8-11e7-bb2c-8dd234861431" }, "customerId": { "entityType": "CUSTOMER", "id": "86543660-44eb-11e9-80a0-a36e3fbec477" }, "deviceModelId": { "entityType": "DEVICE_MODEL", "id": "11442020-a16c-11ec-8ec4-d5a6fdc4d50c" }, "applicationId": { "entityType": "APPLICATION", "id": "a338f4a0-d868-11ec-9a5d-17d0f39d804d" }, }</pre> <p>Download</p> <p>Response headers</p> <pre>cache-control: no-cache, no-store, max-age=0, must-revalidate content-type: application/json date: Mon, 04 Jul 2022 21:48:17 GMT expires: 0 pragma: no-cache transfer-encoding: chunked vary: Origin, Access-Control-Request-Method, Access-Control-Request-Headers x-content-type-options: nosniff x-xss-protection: 1; mode=block</pre> <p>Responses</p> <table border="1"><thead><tr><th>Code</th><th>Description</th></tr></thead><tbody><tr><td>200</td><td>OK</td></tr></tbody></table>	Code	Description	200	OK
Code	Description				
200	OK				

Troubleshooting Tips:

Windows Machine:

The empty space in the JWT token will cause an issue.

In windows command prompt, when the JWT token gets displayed in multiple lines, ensure that you remove the empty space when copying to Authorize field on Swagger UI. Then, select "Authorize" button.

For ex: (Here is the key from my windows command prompt)

```
C:\Users\dmcharla>curl -X POST --header "Content-Type: application/json" --header "Accept: application/json" -d "{\"username\":\"dmcharla@tektelic.com\", \"password\":\"Koushik@95\"}" "https://lorawan-ns-na.tektelic.com/api/auth/login" | findstr -o "token"
% Total    % Received   % Xferd  Average Speed   Time     Time   Current
          Dload  Upload   Total   Spent  Left  Speed
100 1025  100  963  100   62  963  62  0:00:01  ---:--- 0:00:01  1930
0:eyJhbGciOiJIUzUxMiJ9.eyJzdWlIoiJkbWFyY2hhcmxhQHRIa3RlbGljLmNvbSIsInNjb3BlcyI6WyJDVVNUTO1FUI9BRE1JTiJdLCJ1c2VySWQiOiI1NzU3MTdmMC0zYjJmLTEExZWlMtyUmMxYy0zMzg5NGFiYjQxYiIiLCJmaXJzde5hbWUiOjJEaGFudXNoaWsiLCJsvXN0TmFtZSI6Ik1hY2hhcmxhIwiZWhfYmxlZCI6dHJ1ZSwicHJvdmlkZXJJZC16IjYxNjNiYzEw.ThjYTgtMTFNYi1vijjLTkhZDZtDg2TQzMSIsImN1c3RvbhWvSyQwI0iit4NjU0MzY2MC00NGViLTEzTktODBhMC1hMz1M2z1ZWlM0zciLCJpc3MlOj0ZWh0ZkxpY5jb20iLCJpXX0jje2NT5wZIMzIsIm4ccIGHTY1Njk3OTczW#0.2MdKY8EDjwtOLTciNceDN-eLjlaRlxSwF7jixn0lHTj4Coj2x4tiF0R7doKFABihd9BrPOhuikAc1ZYizYw","refreshToken":"eyJhbGciOiJIUzUxMiJ9.eyJzdWlIoiJkbWFyY2hhcmxhQHRIa3RlbGljLmNvbSIsInNjb3BlcyI6WyJSRUZSRVNIX1RPS0VOII0slnVzZXJJZC16IjU3NTcxN2YwLTNmMmYtMTFIYy1hYzFjLTMsDk0YWJiNDFhYiIsImlzcyl6InRla3RlbGljLmNvbSIsImp0aS16ljVjOGRkNmI2LWVjYmUtNDVkMi04MWViLWVjYmRhNTMxYjc4Nii1sImlhCiG6MTY1NjK3HjU2HwlZKhwiJoxldjuU3MDU40tMyFQ.RtBELPV-MEBkctFjn_70GR_NdJHQg0yRa8kSyNHeFOHZve5-Z1T80upw5AKTINWTMvT_B2HLa19T_zvhIK069Q"}
```

```
{"token":"eyJhbGciOiJIUzUxMiJ9.eyJzdWlIoiJkbWFyY2hhcmxhQHRIa3RlbGljLmNvbSIsInNjb3BlcyI6WyJDVVNUTO1FUI9BRE1JTiJdLCJ1c2VySWQiOiI1NzU3MTdmMC0zYjJmLTEExZWlMtyWMxYy0zMzg5NGFiYjQxYiIiLCJmaXJzde5hbWUiOjJEaGFudXNoaWsiLCJsvXN0TmFtZSI6Ik1hY2hhcmxhIwiZWhfYmxlZCI6dHJ1ZSwicHJvdmlkZXJJZC16IjYxNjNiYzEw.ThjYTgtMTFNYi1vijjLTkhZDZtDg2TQzMSIsImN1c3RvbhWvSyQwI0iit4NjU0MzY2MC00NGViLTEzTktODBhMC1hMz1M2z1ZWlM0zciLCJpc3MlOj0ZWh0ZkxpY5jb20iLCJpXX0jje2NT5wZIMzIsIm4ccIGHTY1Njk3OTczW#0.2MdKY8EDjwtOLTciNceDN-eLjlaRlxSwF7jixn0lHTj4Coj2x4tiF0R7doKFABihd9BrPOhuikAc1ZYizYw","refreshToken":"eyJhbGciOiJIUzUxMiJ9.eyJzdWlIoiJkbWFyY2hhcmxhQHRIa3RlbGljLmNvbSIsInNjb3BlcyI6WyJSRUZSRVNIX1RPS0VOII0slnVzZXJJZC16IjU3NTcxN2YwLTNmMmYtMTFIYy1hYzFjLTMsDk0YWJiNDFhYiIsImlzcyl6InRla3RlbGljLmNvbSIsImp0aS16ljVjOGRkNmI2LWVjYmUtNDVkMi04MWViLWVjYmRhNTMxYjc4Nii1sImlhCiG6MTY1NjK3HjU2HwlZKhwiJoxldjuU3MDU40tMyFQ.RtBELPV-MEBkctFjn_70GR_NdJHQg0yRa8kSyNHeFOHZve5-Z1T80upw5AKTINWTMvT_B2HLa19T_zvhIK069Q"}
```

So, when adding the JWT token on Swagger UI, ensure that there is no space between multiple lines. Then select "Authorize" button.

Now you should be able to make API call successfully. It should return with a 200 response code.