Wiliot API Authentication

Usage of Wiliot API requires a valid JWT token.

Today, the Token is obtained using a call to Endpoint: https://api.wiliot.com/v1/auth/token endpoint by providing username and password for authentication.

Starting **October 24th, 2022** , to increase platform security, **New Users** in the Wiliot platform will be required to login with a Two Factor Authentication.

The meaning of this change is that requesting a token by users with 2FA enabled, can be done using an **API Security key** rather than with a username and a password.

The use of Two Factor Authentication will be expanded for **Existing Users** by **November 24th, 2022 by this date all users required to update their existing scripts o work with API Security keys**

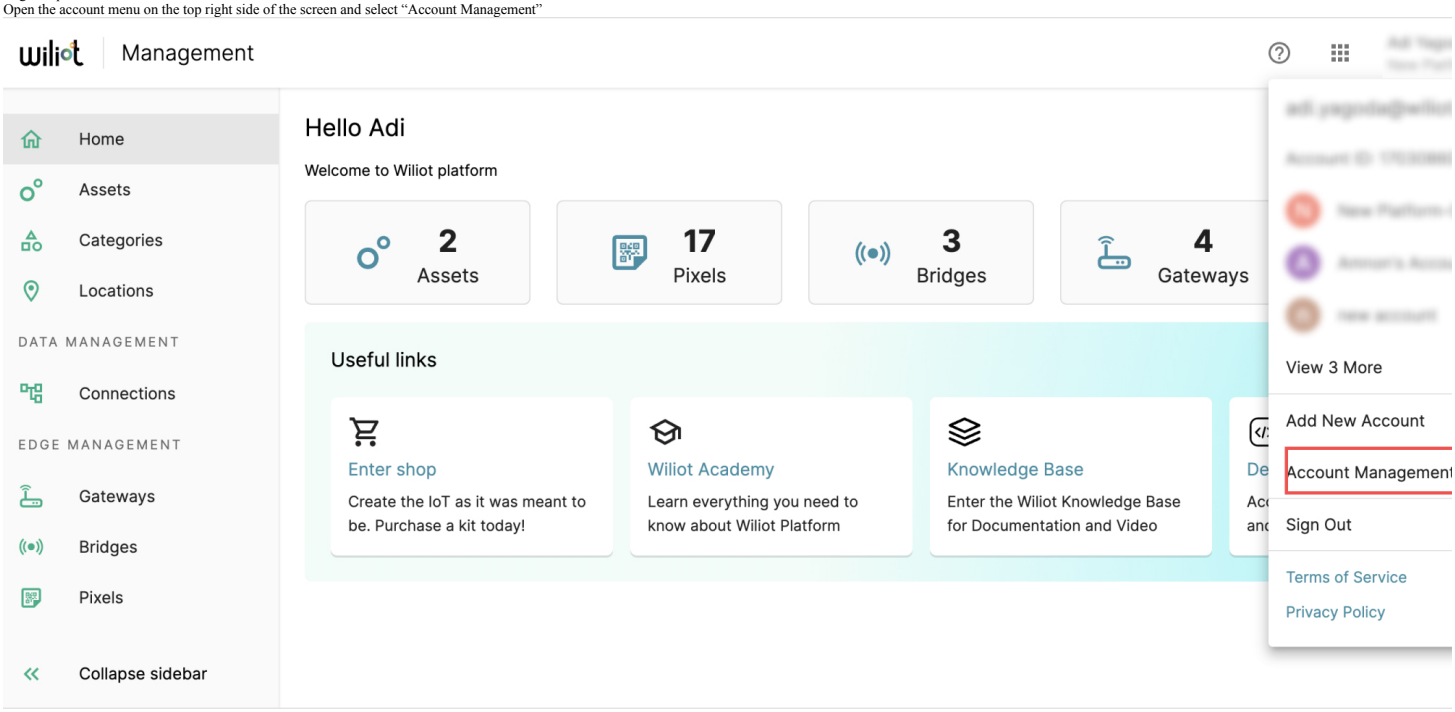
When migrating to use security keys the endpoint above will be replaced by https://api.wiliot.com/v1/auth/token/api endpoint, providing API Security Key for authentication.

How to Obtain the API Security Key

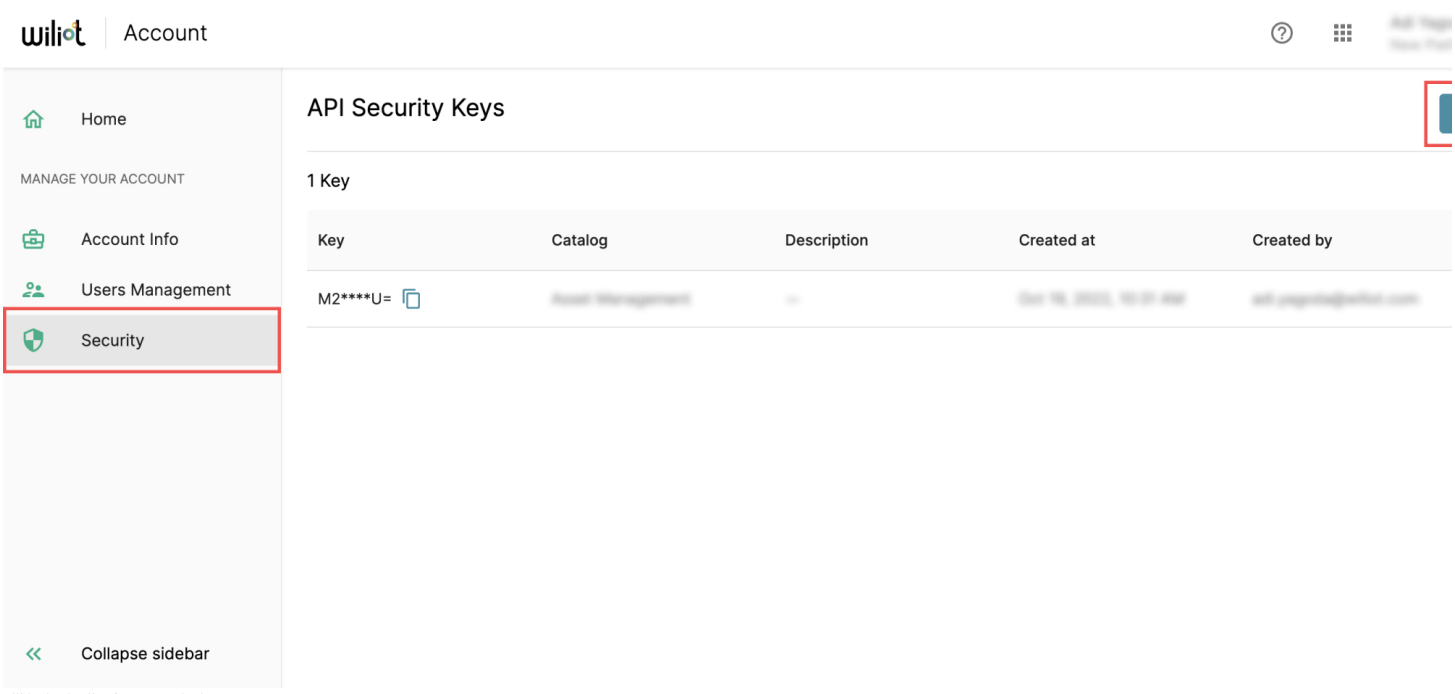
Security Keys are generated and managed in the Wiliot Platform and can be generated by Admin users only.

For accounts on the New Wiliot Platform:

- Login to platform.wiliot.com
- Open the account menu on the top right side of the screen and select “Account Management”



- From the menu on the left select “Security”
- Click on “Add New”



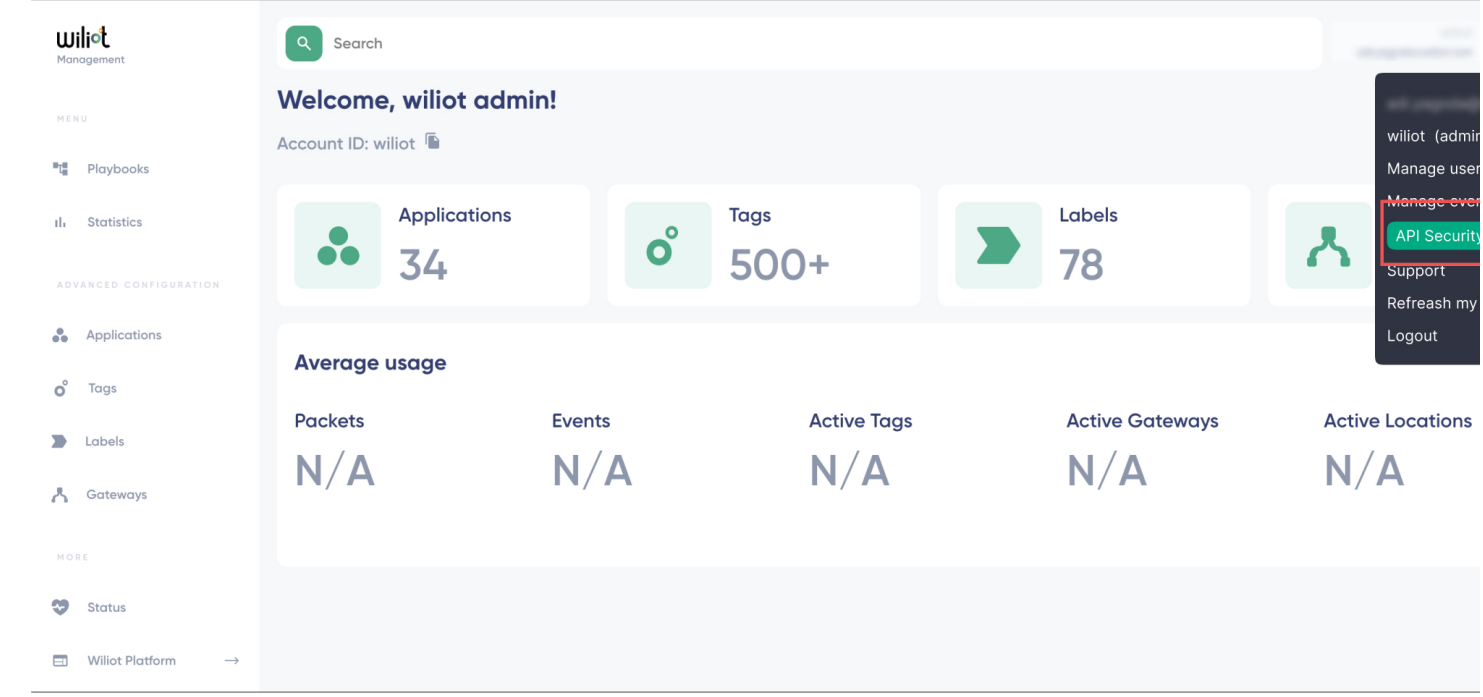
- Fill in the details of your security key.

Note: A key grants access to one API catalog. select the catalog of API’s that you would like to use.
*Select the API key from **Asset Management** in case you are going to use any API from New Platform APIs catalog .*
*Select the API key from **Edge Management** in case you are going to use any API from Edge API catalog .*

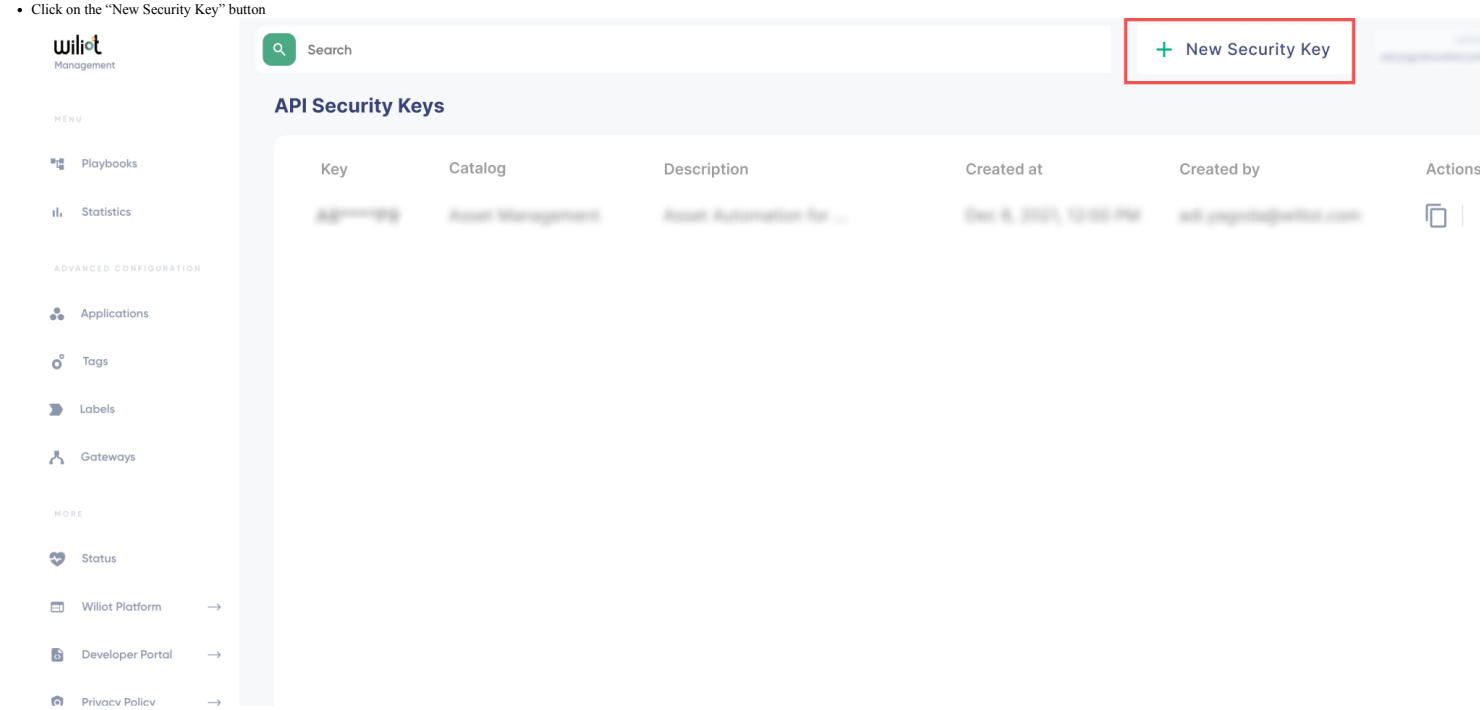
- Your key is now created and can be copied to be used

For accounts on the Legacy Management Platform:

- Login to management.wiliot.com
- Open the menu on the top right side of the screen and select “API Security”



- Click on the “New Security Key” button



- Fill in the details of your security key.

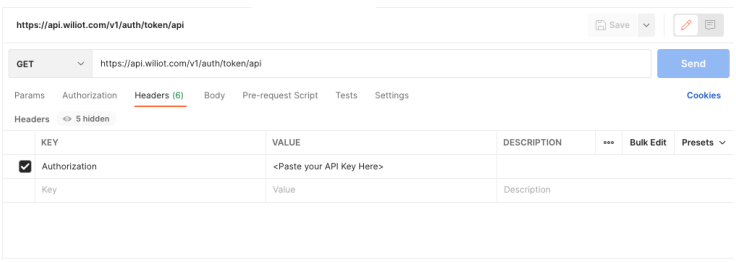
Note: A key grants access to one API catalog. select the catalog of API’s that you would like to use

- Your key is now created and can be copied to be used

How to use the API Security Key

Use the API security Key to get a JWT Token by executing the following

- Copy the key using the dedicated copy button
    - Execute POST to https://api.wiliot.com/v1/auth/token/api endpoint
  - Add Authorization header, use the key as the value



Access Token (access_token)

The access token is a JSON Web Token which can be verified at jwt.io . This token should be used in subsequent API calls by including the following header:

Authorization: Bearer <access_token>

Token Expiry (expires_in)

- Access tokens have a limited lifetime for increased security. The value provided in this field is the number of seconds the access token will be valid. Attempting to use this token past its expiry will result in a 401 (Unauthorized) error.
- When token is expired a new one should be requested. *Note: The refresh token request cannot be used anymore*

How to migrate existing scripts

- Generate the relevant Security Key
- Execute POST to https://api.wiliot.com/v1/auth/token/api endpoint and Add Authorization header, use the key as the value
- Get the token
- Remove API's that are not supported - see https://developer.wiliot.com/ for supported API's
- Remove the use of refresh token, if exist. When token is expired a new one should be requested.

Code Example (Python)

```
import requests

# this key should be obtained in Wiliot platform account management.
# ask your Wiliot account admin in case you don't have access.
# make sure you use a key with access to the correct API catalog. For this example we will use Asset Management catalog.

security_key = "yourSecurityKey"

# your account ID this can also be obtained in Wiliot platform account management.

account_id = "yourAccountId"

get_token_endpoint = "https://api.wiliot.com/v1/auth/token/api"
key_headers = {}
key_headers["Authorization"] = security_key
res = requests.post(url = get_token_endpoint, headers = key_headers)
token = res.json()["access_token"]

get_pixels_endpoint = "https://api.wiliot.com/v1/owner/" + account_id + "/tag?limit=10"
bearer_headers = {}
bearer_headers["Authorization"] = "Bearer " + token
res = requests.get(url = get_pixels_endpoint, headers = bearer_headers)
data = res.json()["data"]
print("Fetched " + str(len(data)) + " Pixels")
```