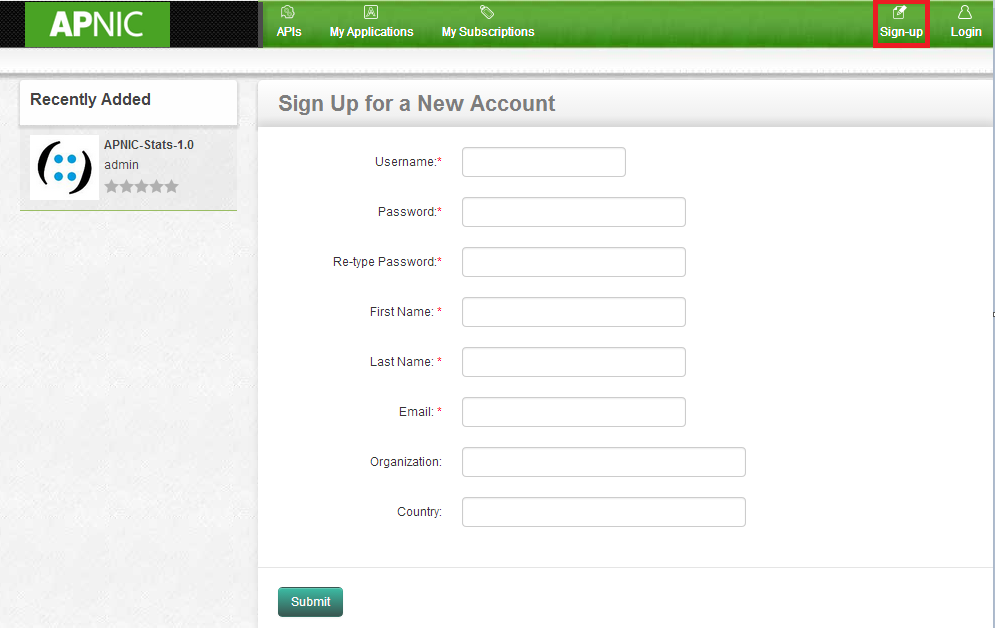
Getting started with APNIC Stats REST API

# Signing Up

Go to https://api.apnic.net:9443/store, click on the Sign-Up link on the top right hand corner.

Complete the form with the required details making sure to supply a valid email address.

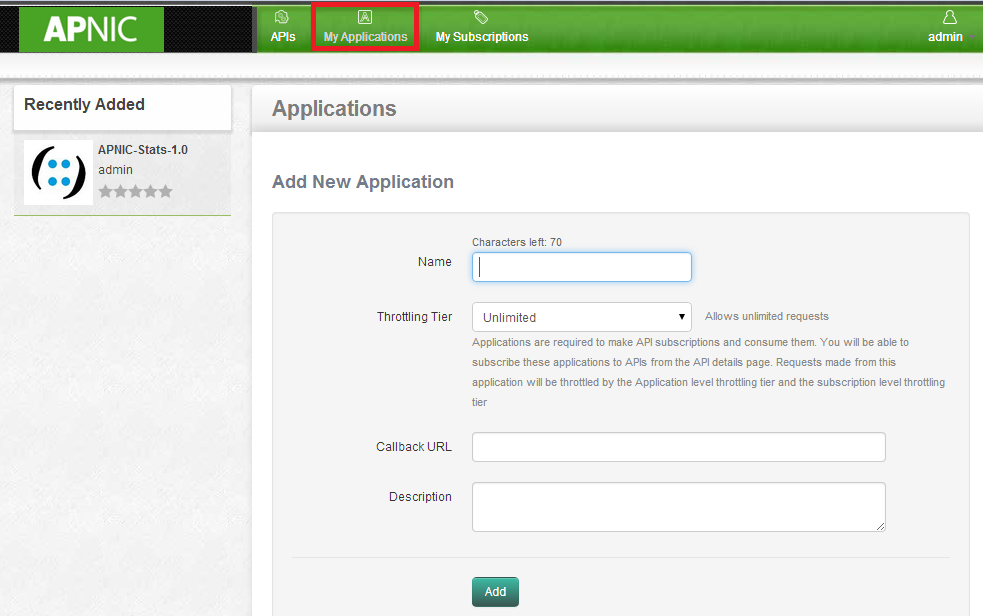


Click on the Submit button.

# Setting up an Application

Login to https://api.apnic.net:9443/store using the Login button on the top right hand corner.

Click on the My Applications tab at the top of the page.



Give your Application a name.

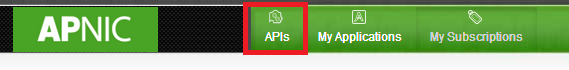
Set the throttling tier:

* Bronze - Allows 1 request per minute
* Silver - Allows 5 requests per minute
* Gold - Allows 20 requests per minute
* Unlimited – No limit to requests per minute

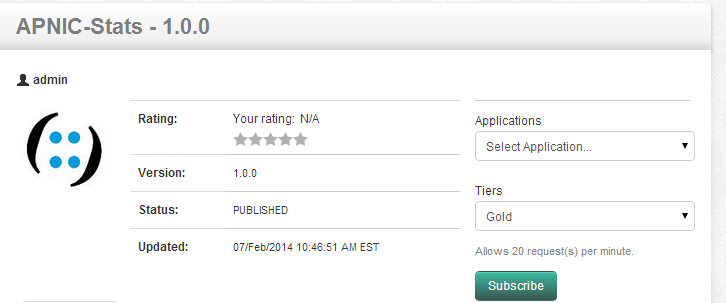
If you wish to define a call-back URL, you can do so here however it is not required. It can be used for [Generating authorization code](http://docs.wso2.org/display/AM160/Token+API#TokenAPI-Generatingauthorizationcode)s.

# Subscribing to an API

Go to the APIs tab at the top of the window.



Click on an API that you wish to subscribe to from the list.



In the Applications dropdown, select your newly created Application.

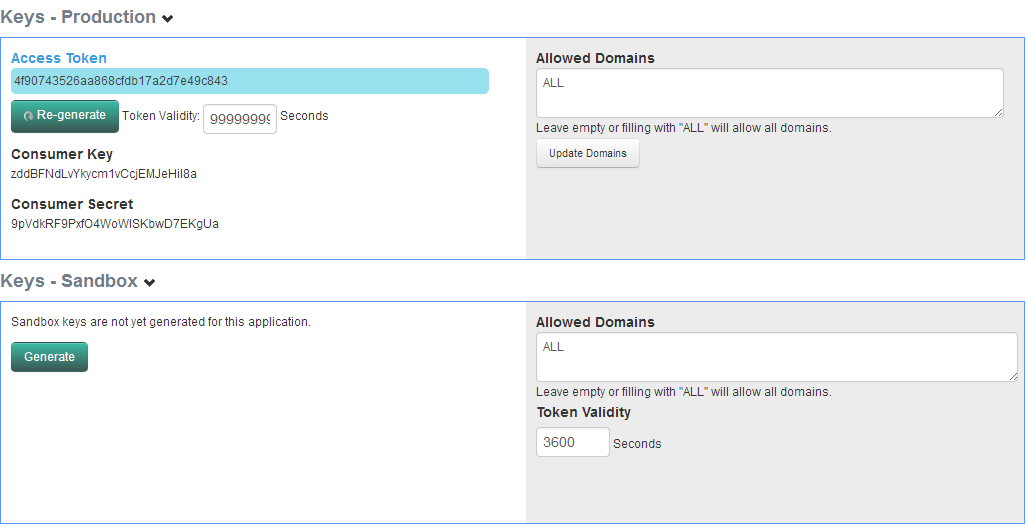
Select one of the Tiers from the dropdown list; this will determine the number of requests you can make per minute.

Click on the Subscribe button.

# Generating an Access Token

Click on the “My Subscriptions” tab at the top.

The page will automatically load with your selected Application. If you have multiple Applications set up, you might need to select the desired application from the “Applications With Subscriptions” dropdown list.



Go to the appropriate Keys section and go to “Production”.

Set a Token Validity time (it’s recommended you use a high number 99999999), in which the token will expire after generation.

# Using the API

Please see the examples guide for more information. Refer to the API Console to see the latest definition of accepted parameters and a description of each of the fields.

You can use a REST client (there are a number available as extensions to most browsers), use cURL, or programmatically call the REST API through your Application using your desired programming language.

When calling the API, send the values as the OAuth 2.0 access token with authentication type set as Bearer.

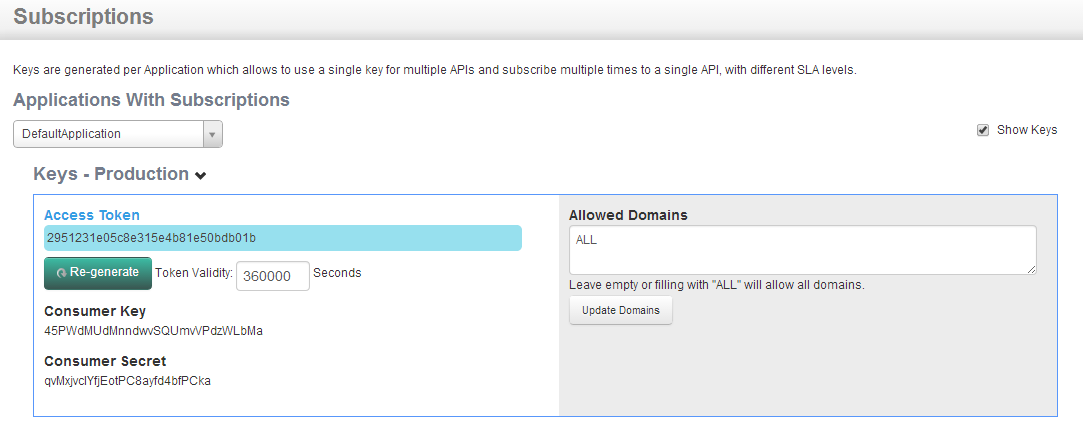
Example: Authorization: Bearer {accessToken}

# User Tokens

Assuming you have already followed the above steps in this Getting Started guide, you should have everything you need to generate or renew the access tokens for your API calls. There are two ways to generate a user token:

* Using the API Manager console – (recommended – already covered in this document above)
* Using the API Manager login API (below)

Instructions to generate a user token and invoke APIs through the management console can be found in the section Subscribing to an API.



# Using the API Manager Login API

You will need to use the consumer key and consumer secret obtained from the subscriptions page in the management console. These must be generated initially through the management console. Refer to Subscribing to an API for instructions.

Combine the consumer key and consumer secret keys in the format '{consumer-key}:{consumer-secret}' and encode the combined string using base64. Encoding to base64 can be done using the <URL:http://base64encode.org>.

1. An example consumer key and secret combination is as follows: wU62DjlyDBnq87GlBwplfqvmAbAa:ksdSdoefDDP7wpaElfqvmjDue.
2. Access the Login API by using a [REST client](https://chrome.google.com/webstore/detail/rest-console/cokgbflfommojglbmbpenpphppikmonn?hl=en) or cURL, with the following parameters.

* Request URL endpoint: <https://api.apnic.net:8243/login>
* Payload:
  + "grant\_type=password&username={username}&password={password}&scope=PRODUCTION".

1. Replace the {username} and {password} values as appropriate.

* Headers:
  + Authorization: Basic {base64 encoded string}
  + Content-Type: application/x-www-form-urlencoded

1. Replace the {base64 encoded string} as appropriate.
2. For example, the following cURL command can be used to access the Login API. It generates two tokens for the user as an access token and a refresh token. The refresh token can be used at the time a token is renewed as explained in the next section.

curl -k -d "grant\_type=password&username={username}&password={password}&scope=PRODUCTION” \

-H "Authorization: Basic SVpzSWk2SERiQjVlOFZLZFpBblVpX2ZaM2Y4YTpHbTBiSjZvV1Y4ZkM1T1FMTGxDNmpzbEFDVzhh” \

-H “Content-Type: application/x-www-form-urlencoded" <https://api.apnic.net:8243/login>

# Renew User Tokens

After an access token is generated, users sometimes may have to refresh or renew the old token due to expiration or security concerns. This can be done by issuing a REST call to Login API through a REST or Curl, with the following parameters.

* Request URL endpoint: <https://api.apnic.net:8243/login>
* Payload:
  + "grant\_type=refresh\_token&refresh\_token=<retoken>&scope=PRODUCTION".

1. Replace the {username} and {password} values as appropriate.

* Headers:
  + Authorization: Basic {base64 encoded string}
  + Content-Type: application/x-www-form-urlencoded

1. Replace the {base64 encoded string} as appropriate.
2. For example, the following cURL command can be used to access the Login API.

|  |
| --- |
| curl -k -d "grant\_type=refresh\_token&refresh\_token={retoken}&scope=PRODUCTION” \  -H "Authorization: Basic SVpzSWk2SERiQjVlOFZLZFpBblVpX2ZaM2Y4YTpHbTBiSjZvV1Y4ZkM1T1FMTGxDNmpzbEFDVzhh” \  -H “Content-Type: application/x-www-form-urlencoded" <https://api.apnic.net:8243/login> |

The REST message will grant the user a renewed user token.