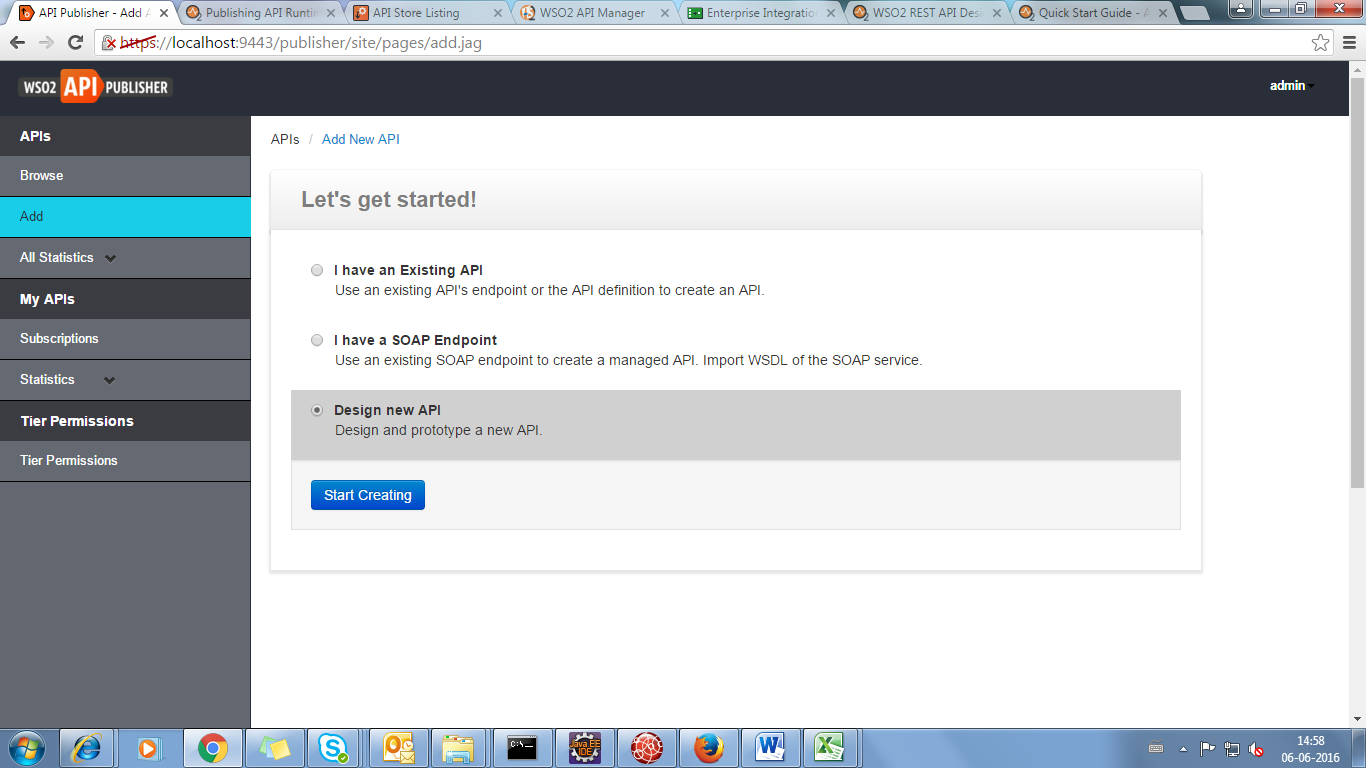
**API\_PUBLISHER**

Adding new API



Design New API

General Details

Name

Display name to be shown in the API Store.

Context

URI context path of the API (case sensitive).  
The supported formats are..   
1. /foo   
2. /foo/bar   
3. /foo/{version}/bar (case sensitive) - allows the version to be within the context

Version

Display version number

Visibility

**Public :** The API is accessible to everyone and can be advertised in multiple stores - a central store and/or non-WSO2 stores.  
**Visible to my domain :** The API is visible to all users who are registered in the API's tenant domain.  
**Restricted by roles :** The API is visible only to specific user roles in the tenant store that you specify.

Description

Can Describe about the Service

Tags

Can used to search API

**ENDPOINTS**

An **endpoint** defines an external destination for an outgoing message through WSO2 ESB

* **Address Endpoint**

The direct URL of the service

* **Failover Group**

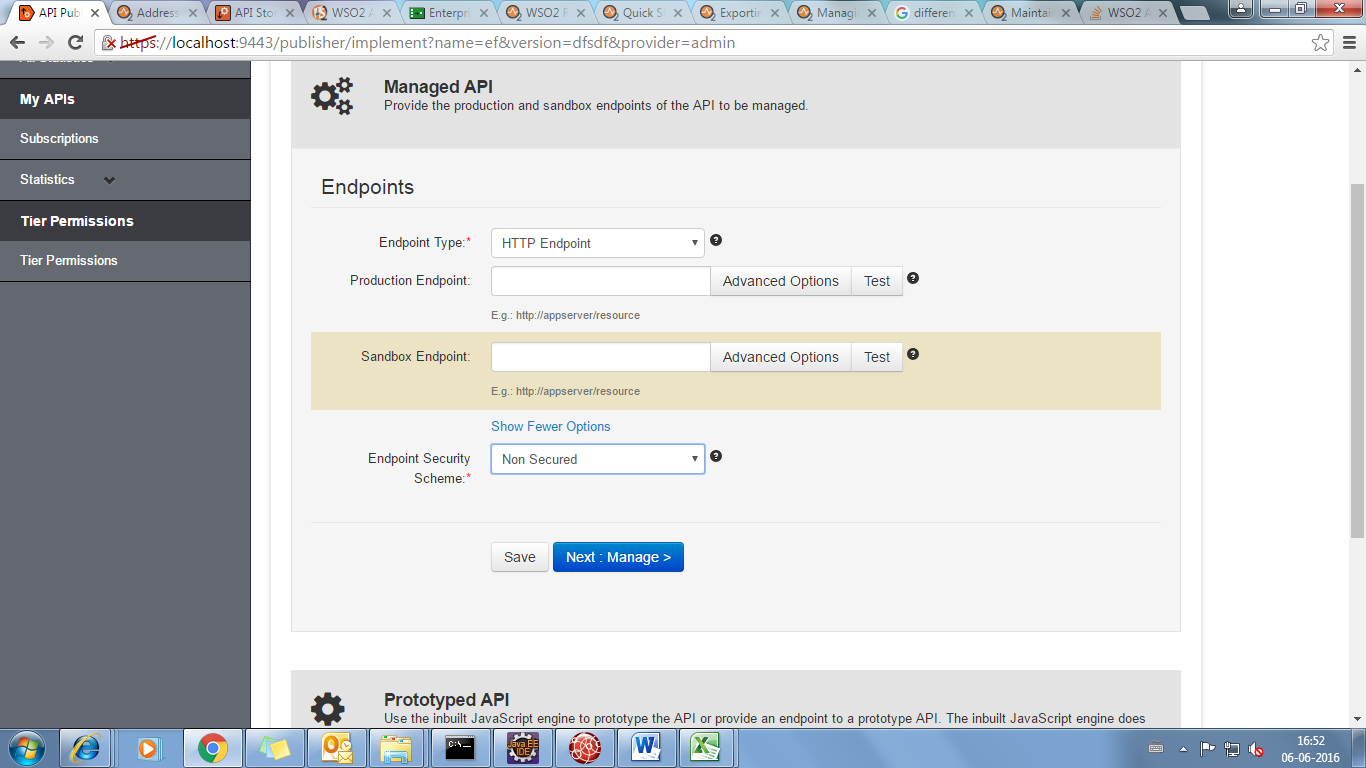
The endpoints that the service tries to connect to in case of a failure. This happens in a round robin manner.

* **Load Balance**

The endpoints where the incoming requests are directed to in a round robin manner. They automatically handle fail-over as well.

* **HTTP Endpoint**

A REST service endpoint based on a URI template



The **production endpoint** is the actual location of the API,

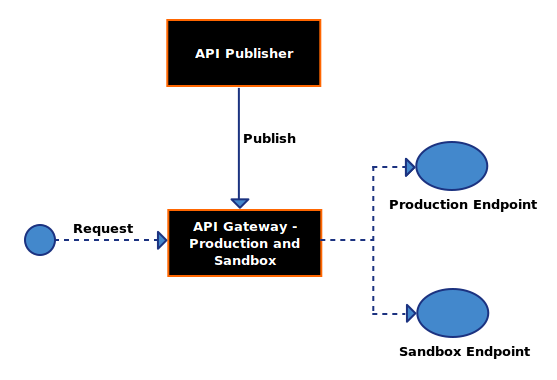
WSO2 API Manager uses HTTP Head to check the validity of the endpoint.

The **sandbox endpoint** points to its testing/pre-production environment.

WSO2 API Manager uses HTTP Head to check the validity of the endpoint.

#### Single Gateway to handle both production and sandbox requests

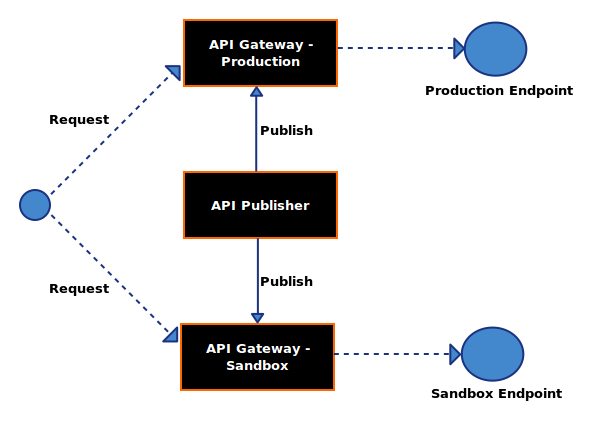
This is the default scenario. Because this Gateway instance handles both production and sandbox token traffic, it is called a hybrid API Gateway. When an API request comes to the API Gateway, it checks whether the requesting token is of type PRODUCTION or SANDBOX and forwards the request to the appropriate endpoint.



#### Multiple Gateways to handle production and sandbox requests separately

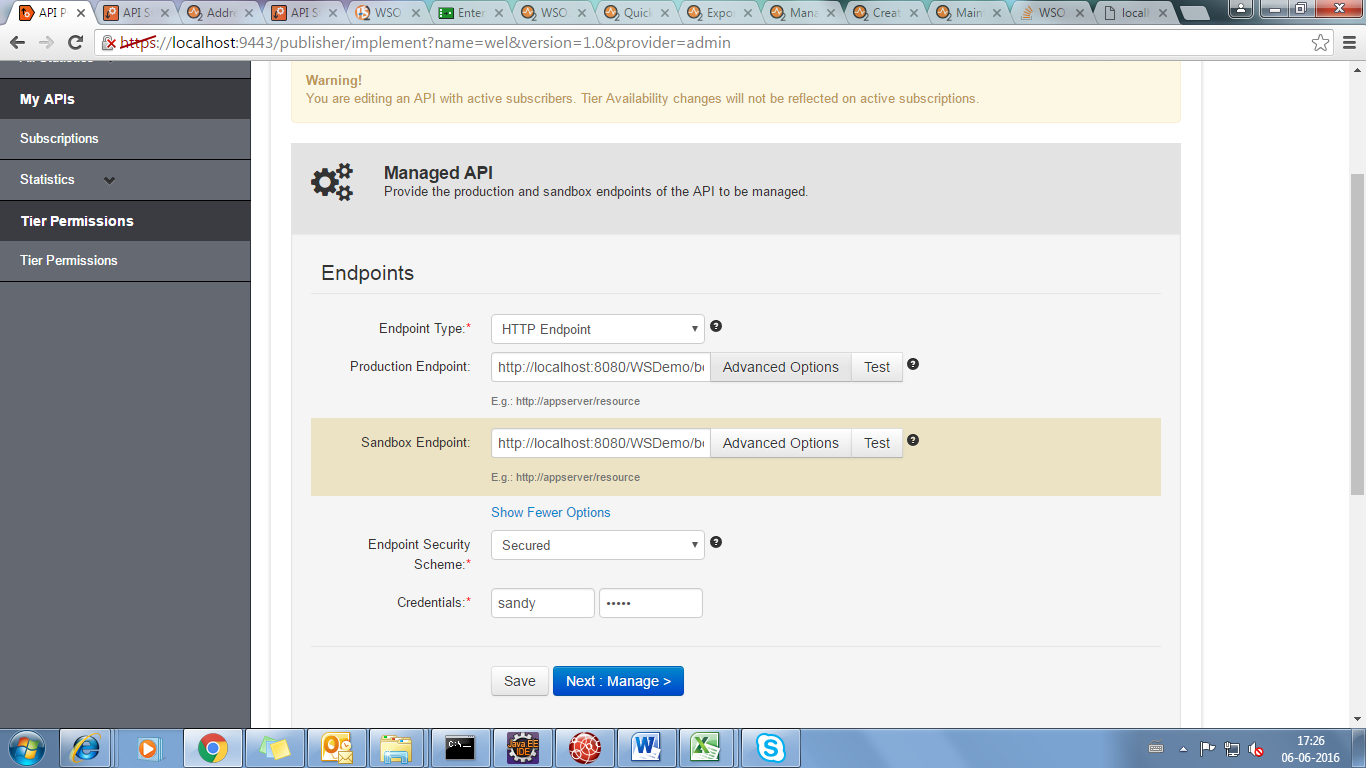
Having a single gateway instance to pass through both types of requests can negatively impact the performance of the production server. To avoid this, you can set up separate API Gateways. The production API Gateway handles requests that are made using PRODUCTION type tokens and the sandbox API Gateway handles requests that are made using SANDBOX type tokens.

The diagram below depicts this using two Gateways:



Endpoint Security Scheme

If secured endpoint is selected, user is asked for credentials of the backend service.



**CONFIGURATION:**

* Make this the Default Version



Marks one API version in a group as the default, so that it can be invoked without specifying the version number in the URL.

For example, if you mark http://host:port/youtube/2.0 as the default API, requests made to http://host:port/youtube/ are automatically routed to version 2.0.

* Tier Availability

Tiers limit the number of requests a subscriber can make to an API. An API can be exposed over one or more tiers.

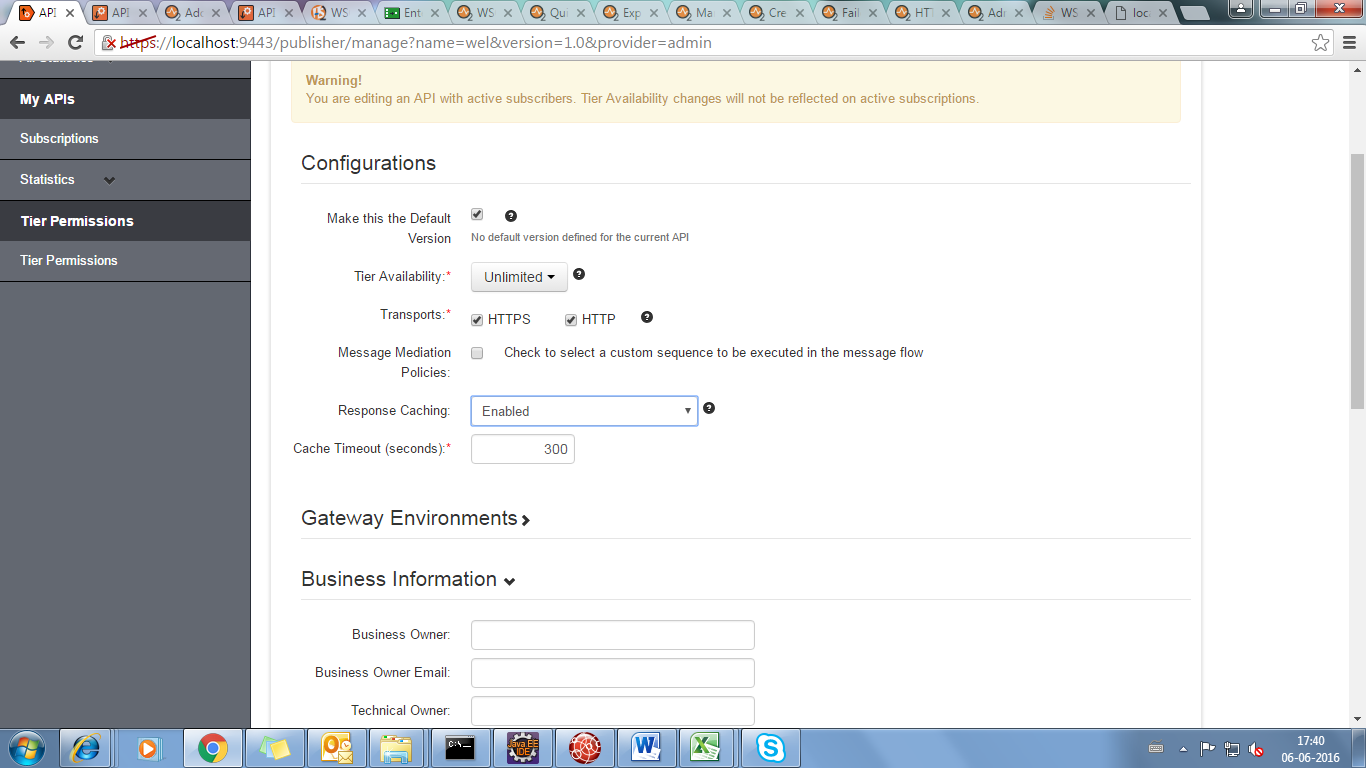
**The Gold, Silver and Bronze tiers allow 20, 5 and 1 request/s respectively per minute.**

* Transports

HTTP is less secure than HTTPS and makes your API vulnerable to security threats.

* Response Caching

This option determines whether to cache the response messages of the API. Caching improves performance, because the backend server does not have to process the same data for a request multiple times. To offset the risk of stale data in the cache, set an appropriate timeout period when prompted.

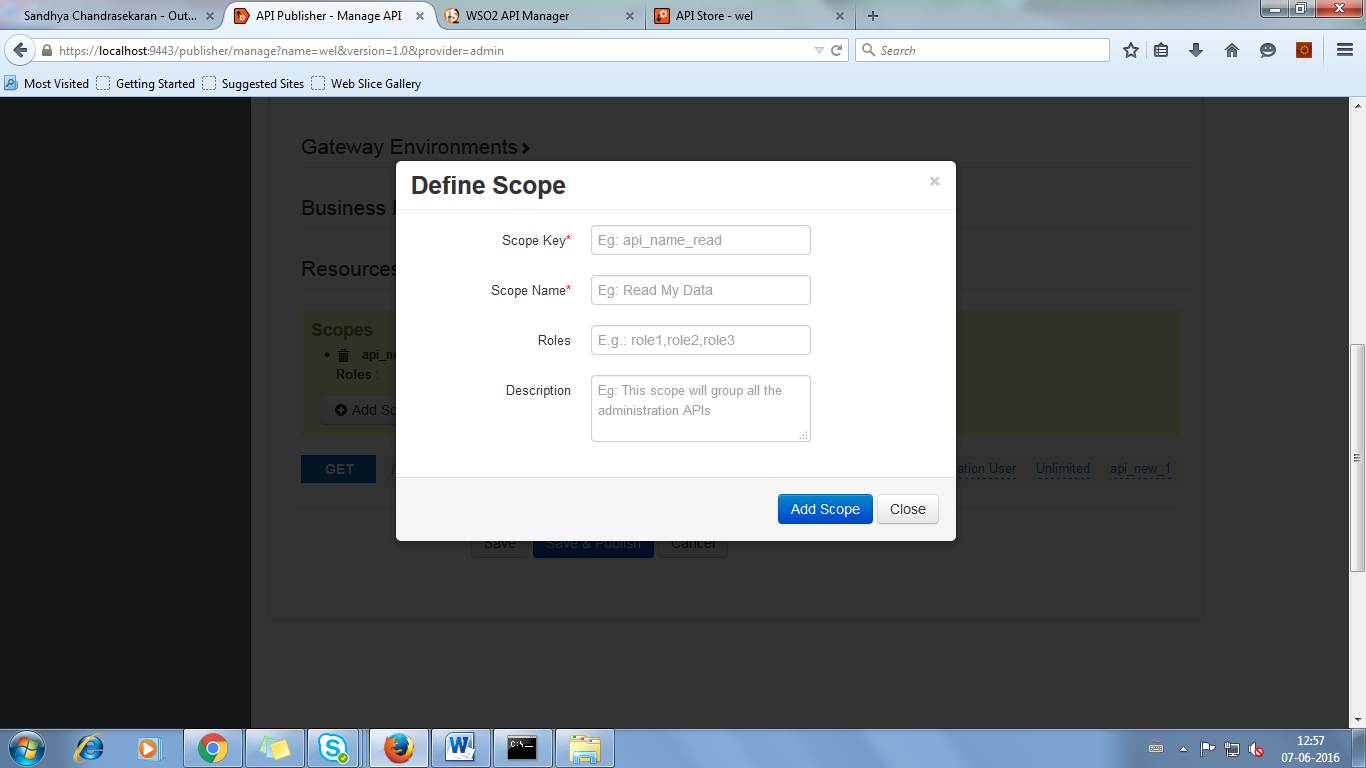


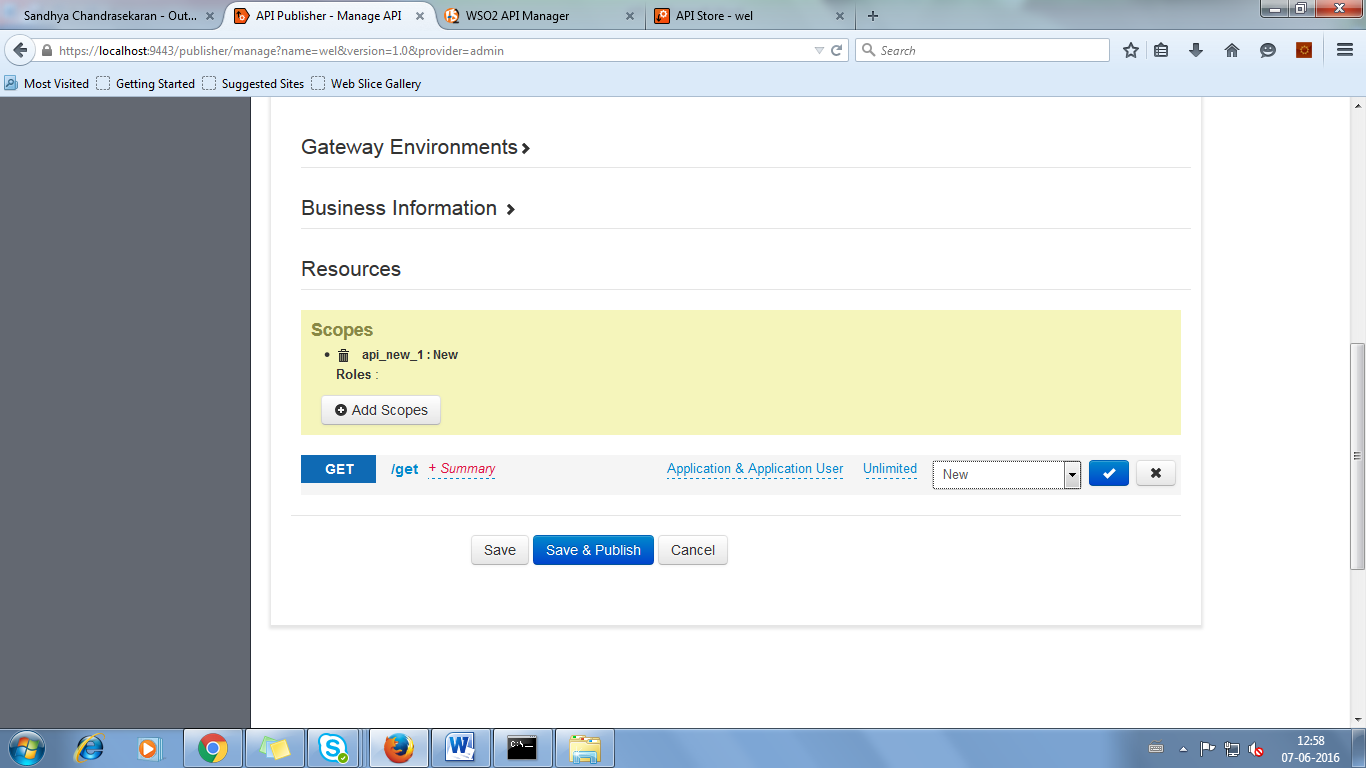
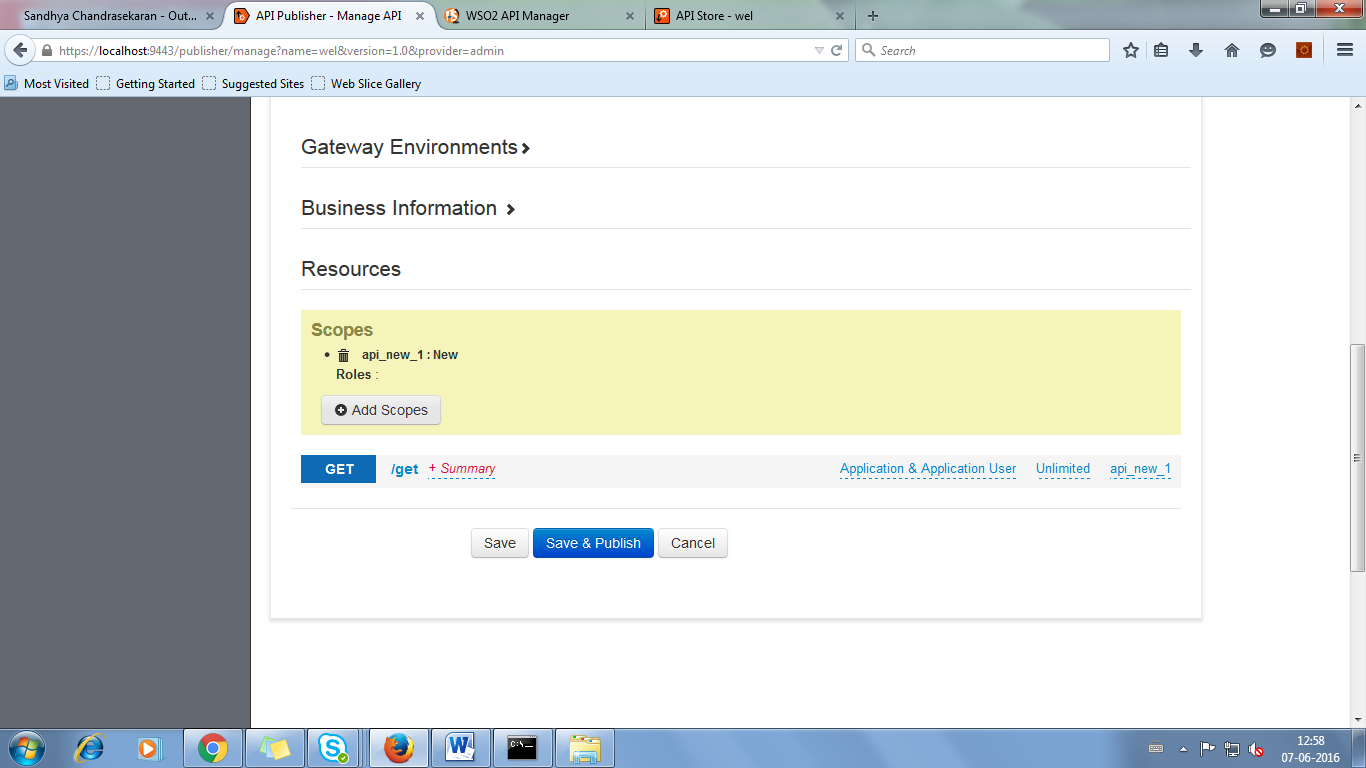
If it is enabled it will automatically set the cache timeout(300 sec) ,we can made changes in that

**Resources**

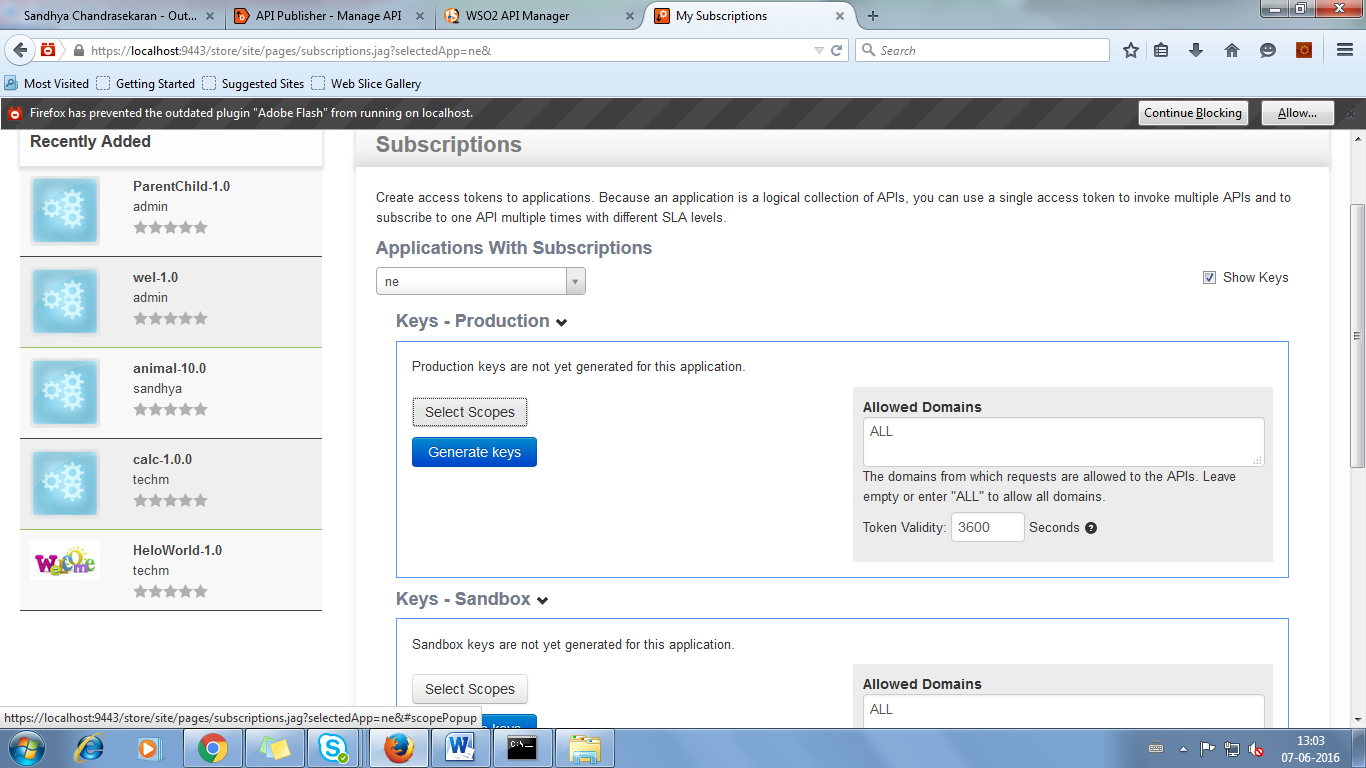
Add Scope:

We can scope so that it is visible in the API Store.



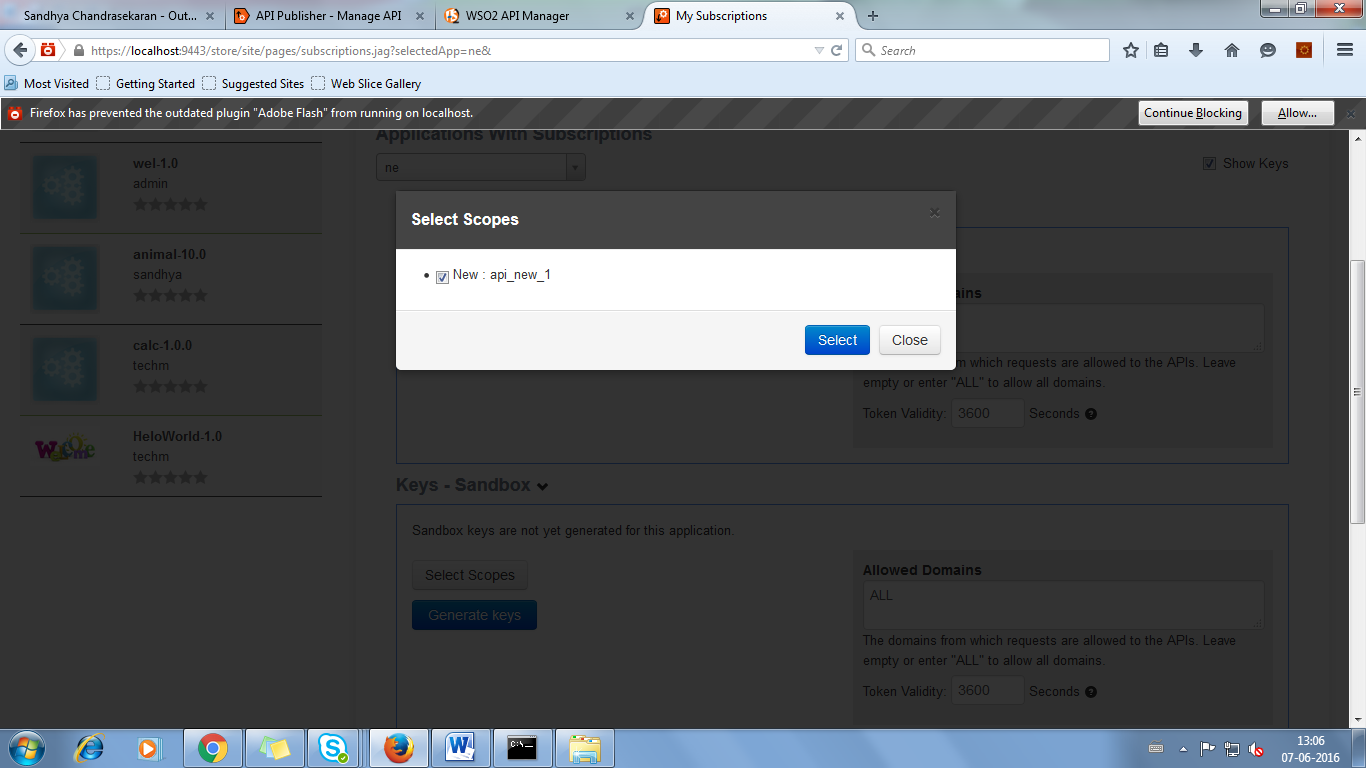


We have to select Scope which we have created and publish,it will visible in the key generation area in the store API of particular API

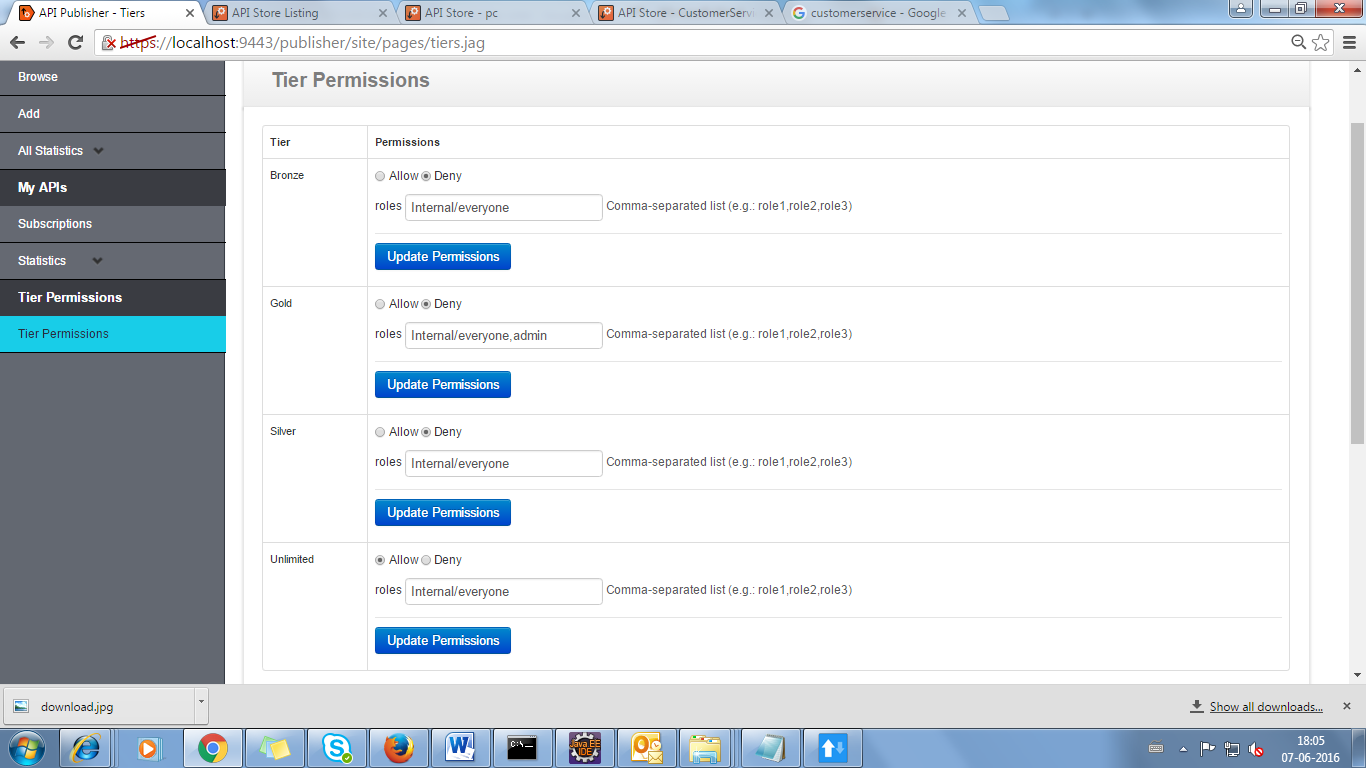


SELECT SCOPE

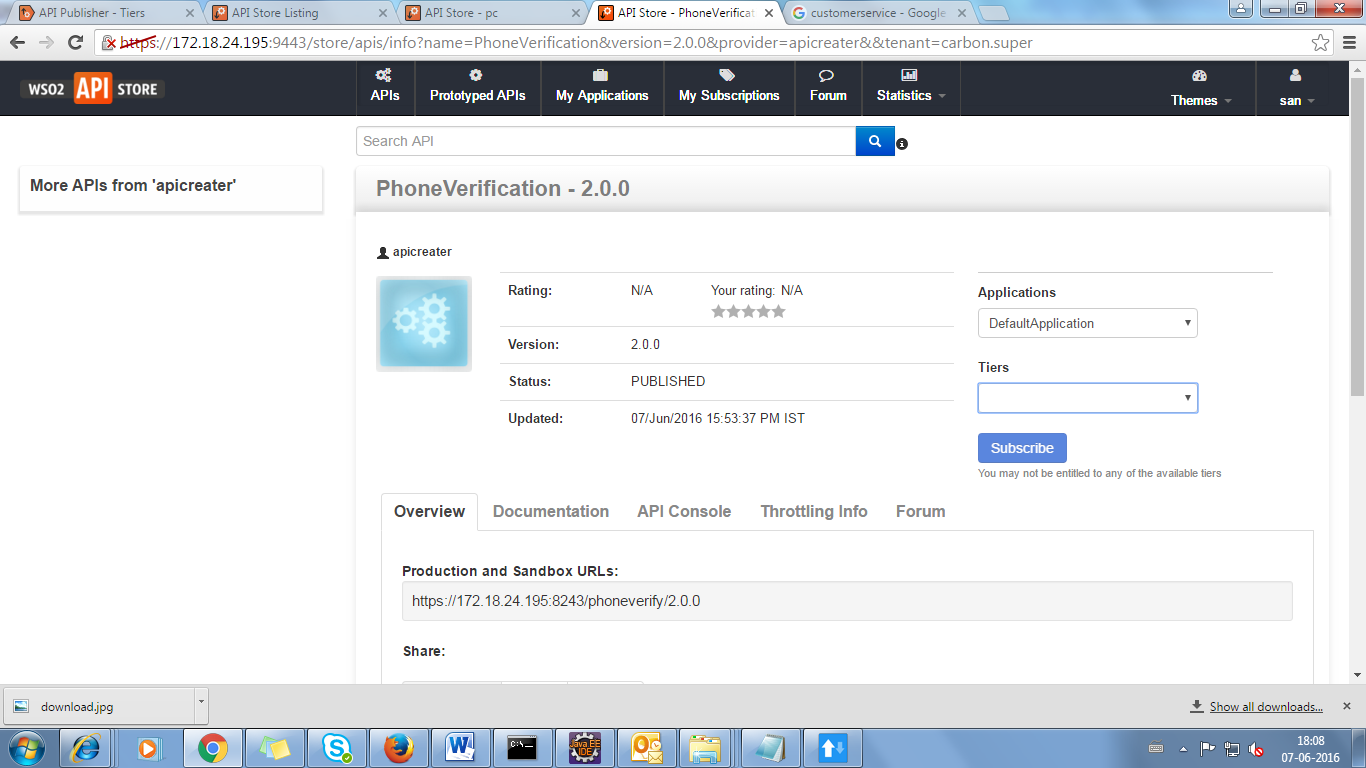
It will appear above the key generation area,we can select the particular scope which we have created



WSO2-API\_Publisher:Tier\_Permission



We can give tier permissions depending upon the role, This will be reflected in the API store.



If we give all tier permission to deny in the former screen(tier permission),we can’t able to access any API’s