

IBM Integration Bus

Integration with IBM API Management

Featuring:

- Deploying REST API within IIB
- Pushing REST API to IBM API Management
- Adding REST API to API Management plan
- Publishing REST API for use within application
- Workload rate limiting using APIM/DataPower
- Workload rate limiting using IIB workload policies

January 2016

Hands-on lab built at product
Version 10.0.0.3

Contents

1. ACKNOWLEDGEMENTS.....	3
2. INTRODUCTION.....	3
2.1 TASKS.....	4
3. PREPARE IIB AND APIM ENVIRONMENTS	5
3.1 CONFIGURE TESTNODE_IIBUSER FOR REST APPLICATIONS.....	5
3.2 OPEN IIB LOG MONITOR.....	5
3.3 CONFIGURE TESTNODE_IIBUSER TO WORK WITH DB2	6
3.4 START IBM API MANAGEMENT ENVIRONMENT.....	7
3.5 CHECK IBM API MANAGEMENT ENVIRONMENT (OPTIONAL)	8
4. PREPARE THE IIB REST APPLICATION	9
4.1 IMPORT AND DEPLOY PRE-REQUISITE IIB PROJECTS.....	9
4.2 PUSH DEPLOYED REST API TO IBM API MANAGEMENT	11
5. CONFIGURE REST API IN IBM API MANAGEMENT.....	13
5.1 LOCATE REST API.....	13
5.2 ENABLE ENFORCEMENT BY IBM API MANAGEMENT GATEWAY	14
5.3 ADD SECURITY SETTINGS.....	15
5.4 ADD PROXY URL	18
6. CREATE AND PUBLISH USE PLAN FOR REST API	19
6.1 ADD REST API TO NEW API MANAGEMENT PLAN.....	19
6.2 TEST REST API (AS API MANAGER).....	23
6.3 STAGE AND PUBLISH PLAN	26
7. PUBLISH REST API.....	28
7.1 DOCUMENT APPLICATION TO USE REST API	28
7.2 DISCOVER URL FOR PUBLISHED REST API	32
7.3 TEST PUBLISHED REST API.....	34
8. INVOKE THE PUBLISHED REST API.....	36
8.1 INVOKE FROM BROWSER.....	36
8.2 REQUEST FROM SOAPUI.....	38
8.3 VIEW THROUGHPUT FOR PUBLISHED REST API IN IIB WEB UI	40
9. LOAD TEST PUBLISHED REST API.....	42
9.1 CHANGE USE PLAN RATE LIMIT	42
9.1.1 <i>Stage and republish the plan.....</i>	45
9.1.2 <i>Publish the REST API again from Developer Portal</i>	47
9.1.3 <i>Test the published URL.....</i>	48
9.2 CREATE AND RUN LOAD TEST.....	49
10. LOAD TEST DEPLOYED API USING IIB WLM.....	53
11. APPENDIX – INSTALLATION AND CONFIGURATION OF API MANAGEMENT ENVIRONMENT.....	55
11.1 PREPARATION.....	55
11.2 START DATAPOWER GATEWAY.....	55
11.3 START API MANAGEMENT APPLIANCE.....	56
11.4 CONFIGURE GATEWAY APPLIANCE – CLI SECTION.....	56
11.5 CONFIGURE GATEWAY APPLIANCE - ACCEPT GATEWAY LICENCE	57
11.6 CONFIGURE GATEWAY APPLIANCE - NTP & TIME ZONE.....	57
11.7 CONFIGURE GATEWAY APPLIANCE - ENABLE XML MANAGEMENT INTERFACE PORT	58
11.8 CONFIGURE GATEWAY APPLIANCE - ENABLE STATISTICS.....	58
11.9 CONFIGURE API MANAGEMENT APPLIANCE.....	59
11.10 CONFIGURE API MANAGEMENT CLOUD	59
END OF LAB GUIDE	61

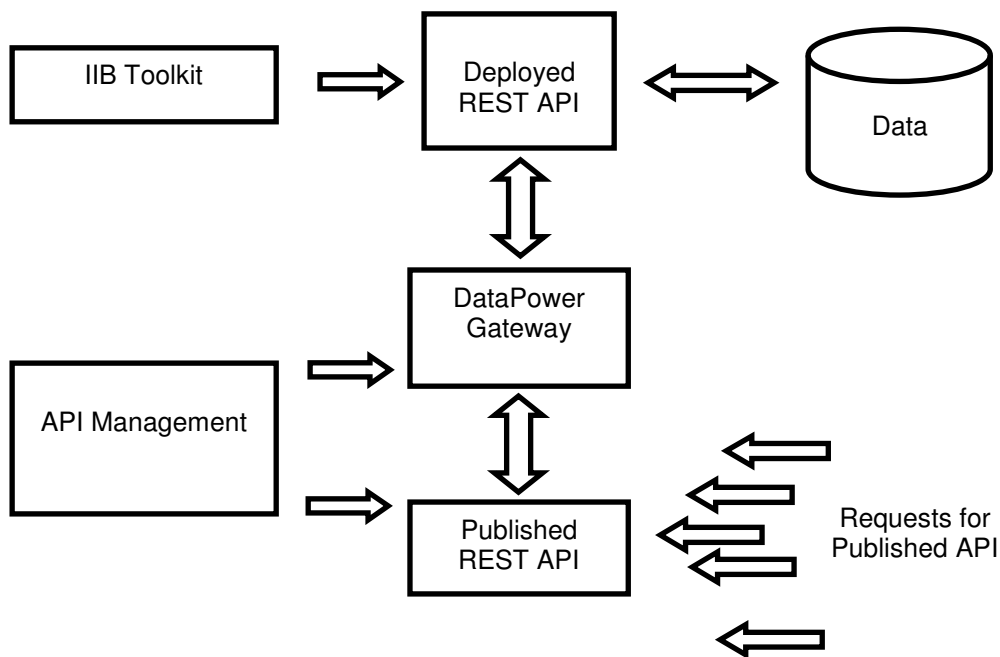
1. Acknowledgements

This lab guide is based in part on the **IBM Integration Bus and IBM API Management Lab** written for the **2015 IBM WebSphere Technical University** by IIB Developer Simon Stone.

The appendix, which describes how to create the API Management environment used here, is based on an IBM internal document written by Mike Alley from the IBM WW Technical Pre Sales team

2. Introduction

This lab guide provides instructions on how control and use the REST API created in the lab *Developing a REST API Service* from within IBM API Management.



2.1 Tasks

In this lab, you will perform the following tasks, with the associated roles:

Within IIB

- 1) You will use the IIB node TESTNODE_iibuser, that is automatically created by the IIB Toolkit.
- 2) Import and deploy the REST API Service solution from the *Developing a REST API Service* lab to TESTNODE_iibuser
- 3) Test the service using Swagger UI (optional)
- 4) Push the deployed REST API to IBM API Management

Within API Management as the API Manager

- 1) Complete configuration of the REST API, including using applications' credentials* to access REST API.
- 2) Add the REST API to an API Management use plan, including specification of a rate limit to applications' use of the REST API.
- 3) Test the REST API
- 4) Publish the plan

Within API Management as an API Developer

- 1) Subscribe to the plan to use and publish the REST API within an application
- 2) Test the published REST API through the IBM DataPower Gateway, including
 - requesting REST API with invalid application credentials
 - exceeding rate limit for application

As an API user

- 1) Submit requests to the published REST API

In addition, you will run the load tests using SOAP UI for the following:

- 1) Published REST API with (new) rate limit in the API Management use plan, to demonstrate limits enforced by the DataPower Gateway at the application level
- 2) Deployed REST API with rate limit enforced by WLM

*Applications' Credentials

- Client ID: identifies applications that are making API calls so that application-specific quotas and statistics can be monitored, displayed, and enforced.
- Client Secret: used, like a password, in conjunction with Client ID.

3. Prepare IIB and APIM environments

3.1 Configure TESTNODE_iibuser for REST applications

The IIB support for the REST API requires some special configuration for the IIB node and server. If you have already done the REST API lab in this series of labs, you can proceed straight to section 3.2, below.

Login to Windows as the user "iibuser", password = "passw0rd".

Start the IIB Toolkit from the Start menu.

1. Ensure that TESTNODE_iibuser is started.
2. Enable Cross-Origin Resource Scripting for REST. This is required when testing with the SwaggerUI test tool. See http://en.wikipedia.org/wiki/Cross-origin_resource_sharing for further information.

(Helpful hint - the VM keyboard is set to UK English. if you cannot find the "\" with your keyboard, use "cd .." to move to a higher-level folder in a DOS window).

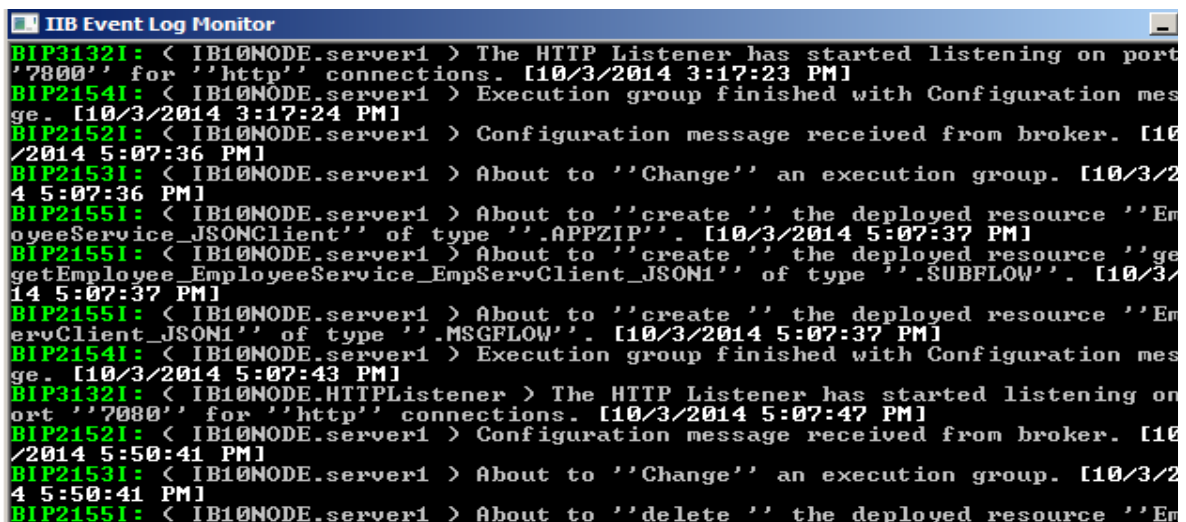
In an IIB Command Console (shortcut on the Start menu), run the command:

```
mqsichangeproperties TESTNODE_iibuser -e default
-o HTTPConnector
-n corsEnabled -v true
```

3.2 Open IIB Log Monitor

A useful tool for IIB development on Windows is the IIB Log Monitor. This tool continuously monitors the Windows Event Log, and all messages from the IIB and WMB log are displayed immediately.

From the Start menu, click IIB Event Log Monitor. The Monitor will open; it is useful to have this always open in the background.



```
IIB Event Log Monitor
BIP3132I: < IB10NODE.server1 > The HTTP Listener has started listening on port
'7080' for 'http' connections. [10/3/2014 3:17:23 PM]
BIP2154I: < IB10NODE.server1 > Execution group finished with Configuration mes
ge. [10/3/2014 3:17:24 PM]
BIP2152I: < IB10NODE.server1 > Configuration message received from broker. [10
/2014 5:07:36 PM]
BIP2153I: < IB10NODE.server1 > About to 'Change' an execution group. [10/3/2
4 5:07:36 PM]
BIP2155I: < IB10NODE.server1 > About to 'create' the deployed resource 'Em
ployeeService_JSONClient' of type '.APPZIP'. [10/3/2014 5:07:37 PM]
BIP2155I: < IB10NODE.server1 > About to 'create' the deployed resource 'ge
getEmployee_EmployeeService_EmpServClient_JSON1' of type '.SUBFLOW'. [10/3/
14 5:07:37 PM]
BIP2155I: < IB10NODE.server1 > About to 'create' the deployed resource 'Em
ployClient_JSON1' of type '.MSGFLOW'. [10/3/2014 5:07:37 PM]
BIP2154I: < IB10NODE.server1 > Execution group finished with Configuration mes
ge. [10/3/2014 5:07:43 PM]
BIP3132I: < IB10NODE.HTTPListener > The HTTP Listener has started listening on
port '7080' for 'http' connections. [10/3/2014 5:07:47 PM]
BIP2152I: < IB10NODE.server1 > Configuration message received from broker. [10
/2014 5:50:41 PM]
BIP2153I: < IB10NODE.server1 > About to 'Change' an execution group. [10/3/2
4 5:50:41 PM]
BIP2155I: < IB10NODE.server1 > About to 'delete' the deployed resource 'Em
```

This tool is not shipped as part of the IIB product; please contact us directly if you would like a copy.

3.3 Configure TESTNODE_iibuser to work with DB2

If you have already done Lab 1 in this series (create an Integration Service), you can skip straight to Start IBM API Management on the next page.

To run this lab, the Integration Bus node must be enabled to allow a JDBC connection to the HRDB database.

1. Open an IIB Command Console (from the Start menu), and navigate to

```
c:\student10\Create_HR_database
```

2. Run the command

```
3_Create_JDBC_for_HRDB
```

Accept the defaults presented in the script. This will create the required JDBC configurable service for the HRDB database.

3. Run the command

```
4_Create_HRDB_SecurityID
```

4. Stop and restart the node to enable the above definitions to be activated

```
mqsistop TESTNODE_iibuser
```

```
mqsistart TESTNODE_iibuser
```

This will create the necessary security credentials enabling TESTNODE_iibuser to connect to the database.

3.4 Start IBM API Management environment

VMWare Virtual Networking

Note that all virtual machines in this lab, including the IIB Windows system, run on the IP subnet 192.168.126.xxx. If you are not running this lab in the prepared IIB workshop environment, you must make sure that the VMNet8 adapter is specified to use NAT, and that it has a subnet IP of 192.168.126.0, and that the subnet mask is 255.255.255.0.

This is done by using the VMWare Virtual Network Editor.

If you are doing this lab in a BetaWorks workshop, then the IBM API Management environment will have been set up for you, comprising the following systems:

IBM DataPower Gateway Virtual Machine

VM: DPGW

IP address: 192.168.126.52 (hard-coded address)

Admin account:

UserID = admin

Password = passw0rd!

Note: you will not need to directly access this VM during this lab.

IBM API Management Appliance Virtual Machine

VM: APIM-Appliance

IP address: 192.168.126.100 (hard-coded address)

Admin account:

UserID = admin

Password = !n0r1t5@C

Cloud owner account:

Userid = admin

Password = passw0rd! (note the '!' at the end)

API Manager user organization: My Organization

Developer organization: My Lab

Developer organization URL Path Segment: mylab

1. If you need to create the environment, follow the instructions in the Appendix before proceeding.
2. Ensure the IBM DataPower Gateway and IBM API Management Appliance Virtual Machines are powered on.
3. From the IIB Virtual Machine, ping the DataPower Gateway and API Management appliance to check they are available.

3.5 Check IBM API Management environment (optional)

If you are doing this lab in a BetaWorks workshop, the environment will have been set up for you and these steps should not be necessary. However, doing these steps may give you a better understanding of the configuration that has been done.

1. Log on to the API Management Appliance with the Admin account.
 - UserID = admin
 - Password = !n0r1t5@C (note, the ! and @ characters may be on a different key on your keyboard - check this first by typing into the userid field, so that you can see the typed character).

Run the command `net show all` and note the IP address for eth0. For a BetaWorks workshop, it should be as shown here:

```
ci-192-168-126-100/APIManagement> net show all
Hostname (DHCP from eth0): ci-192-168-126-100
Domain (DHCP from eth0): localdomain
Domain Search (Static): [None]
Nameservers (Static): 192.168.126.2
Gateway (Static on eth0): 192.168.126.2
NTP (Static): 185.53.93.157

Carrier timeout: 30 seconds

Eth0 (00:0c:29:bb:0d:15): Static
Address: 192.168.126.100, Netmask: 255.255.255.0, Broadcast: 192.168.126.255
MTU: 1500
Link Status is not available

Routes: [None]
```

Again, note that the first three parts of the IP address (`192.168.126`) match the corresponding parts of the IP address of the VMnet8 ethernet adapter.

2. Login to the Windows IIB VM:
 - User = iibuser
 - Password = passw0rd

From the Windows command prompt, run the `ipconfig` command. It is essential that the IPv4 Address and Subnet Mask entries for the VMnet8 ethernet adapter match those on which the environment was originally prepared. For a BetaWorks workshop, they should be as shown here:

```
Ethernet adapter VMware Network Adapter VMnet8:
Connection-specific DNS Suffix . . . : 
Link-local IPv6 Address . . . . . : fe80::f0d8:a24c:405f:af1b%21
IPv4 Address. . . . . : 192.168.126.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
```


4. Prepare the IIB REST Application

4.1 Import and deploy pre-requisite IIB projects

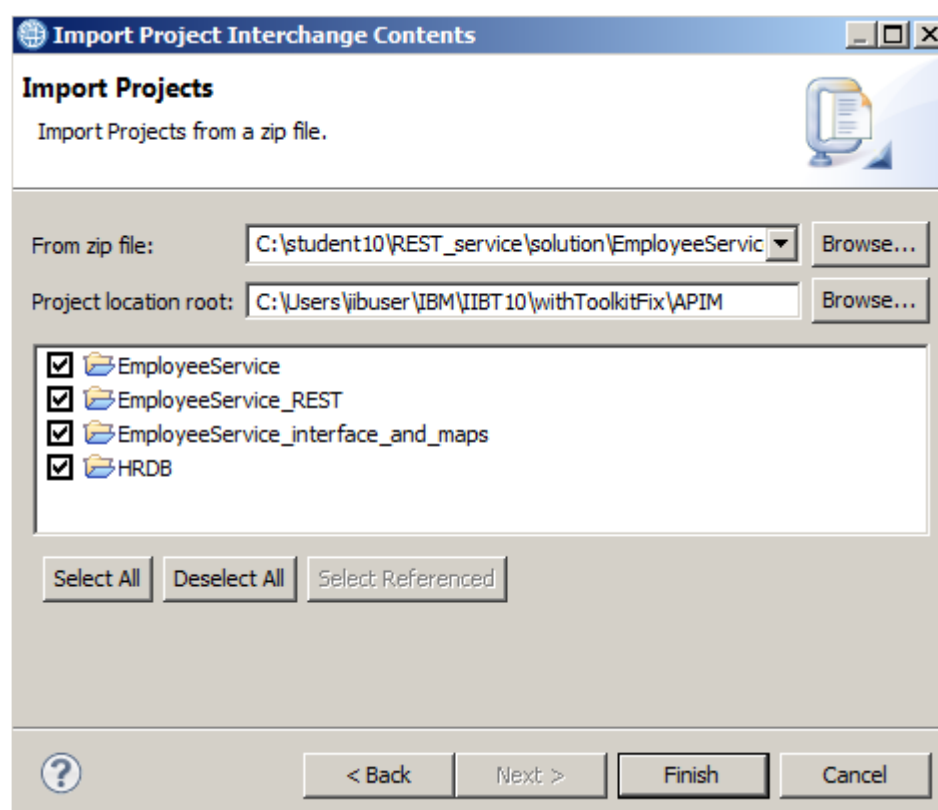
1. Login to the Windows IIB VM:
 - User = iibuser
 - Password = passw0rd
2. To ensure there are no conflicts with other components, switch to a new IIB workspace in the IIB Toolkit. For example name it

```
c:\users\iibuser\IBM\IIB 10\workspace_APIM
```

3. In the IIB Toolkit, import the Project Interchange file:

```
c:\student10\REST_service\solution\EmployeeService_REST.10.0.0.3.zip
```

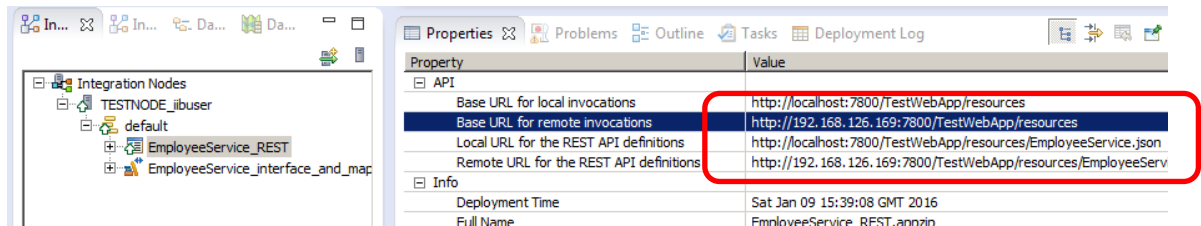
Import all the projects in the PI file.



4. Deploy **EmployeeService_interface_and_maps** to server **default** on TESTNODE_iibuser.
5. Deploy **EmployeeService_REST** to server **default** on TESTNODE_iibuser.

6. In the Integration Toolkit, navigate to the Integration Nodes view in the bottom left, click the EmployeeService_REST that has been deployed.

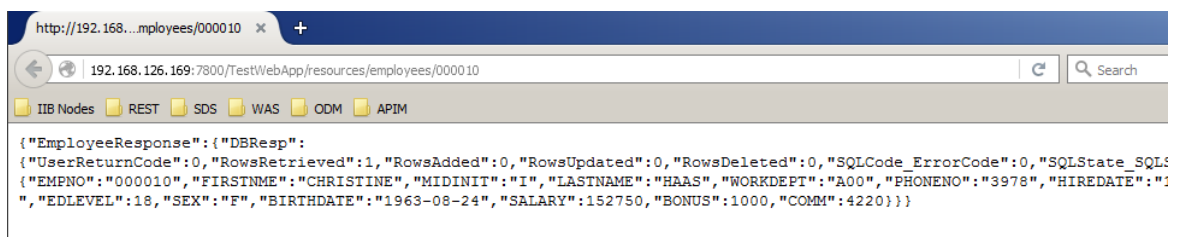
Copy the **Base URL for remote invocations** in the Properties. Copy this into a text document for future reference (use Notepad to create a temporary txt file).



7. To test the REST API, append *employees/000010* to this URL, e.g.

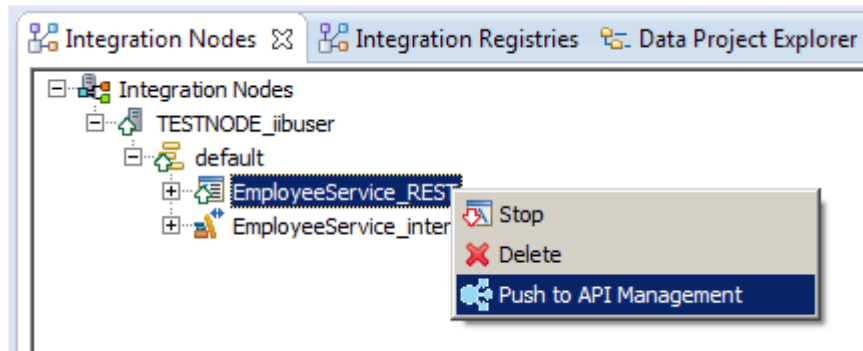
http://192.168.126.180:7800/TestWebApp/resources/employees/000010

Paste this into a browser address. If the REST API is working correctly, the details for employee 000010 should be returned:

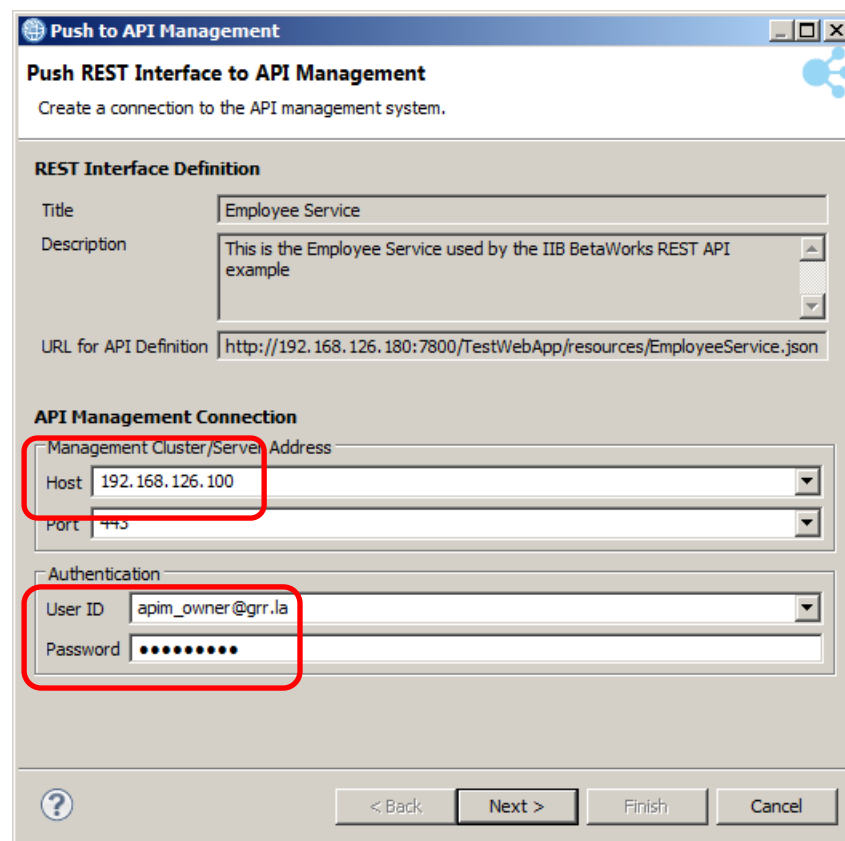


4.2 Push deployed REST API to IBM API Management

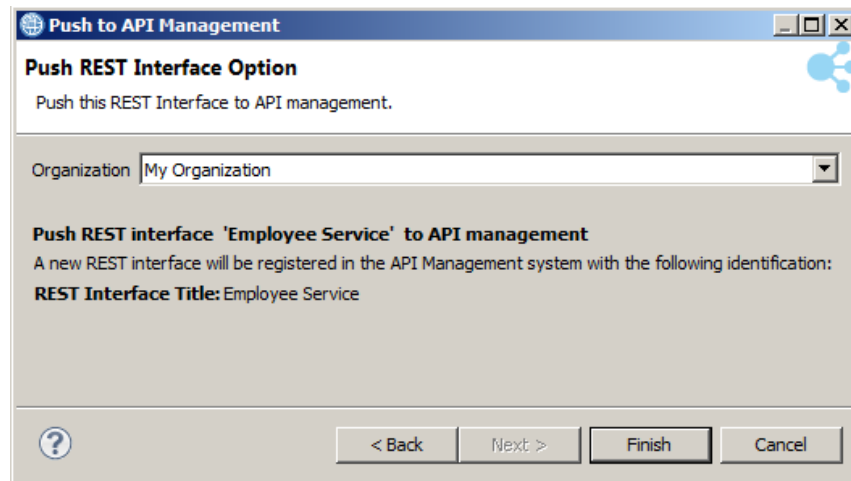
1. In the Integration Toolkit, navigate to the Integration Nodes view in the bottom left and right click the EmployeeService_REST that has been deployed.



2. The **Push to API Management** wizard will appear. Provide the following details:
 - Host: IP address of the IBM API Management virtual appliance
 - (In the IIB workshop, 192.168.126.100)
 - User ID: apim_owner@grr.la
 - Password: passw0rd! (note the '!' at the end)

The screenshot shows the 'Push to API Management' wizard window. The title bar says 'Push to API Management'. The main heading is 'Push REST Interface to API Management' with the instruction 'Create a connection to the API management system.' The 'REST Interface Definition' section includes: Title: Employee Service; Description: This is the Employee Service used by the IIB BetaWorks REST API example; URL for API Definition: http://192.168.126.180:7800/TestWebApp/resources/EmployeeService.json. The 'API Management Connection' section includes: Management Cluster/Server Address: Host (192.168.126.100) and Port (443). The 'Authentication' section includes: User ID (apim_owner@grr.la) and Password (masked with dots). At the bottom, there are buttons for '< Back', 'Next >', 'Finish', and 'Cancel'. The 'Next >' button is highlighted.

- The wizard will confirm which Organization you wish to push the REST API to. Ensure that **My Organization** is selected, and click **Finish**:



- The wizard will close, and the results of the operation will be displayed.

Note: at this point, the deployed REST API is now published to IBM API Management, but is not exposed to clients.

Defect warning - the Close button does not work. Click the Window cross to close this window.



5. Configure REST API in IBM API Management

5.1 Locate REST API

1. In a browser, go to: `https://< IP address of API Management appliance >/apimanager` (e.g. `192.168.126.100/apimanager`).

Log on with the API Manager user account:

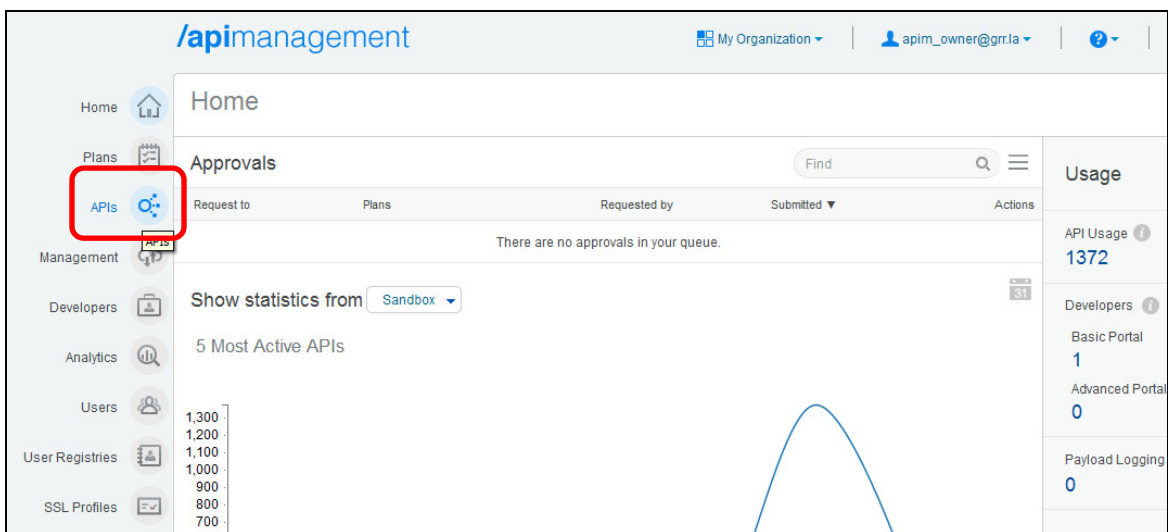
UserID = **apim_owner@grr.la**

Password = **passw0rd!** (note the '!' at the end)

You are now logged on to the IBM API Management Appliance as an API manager.

2. The Home page will be displayed.

Click on the APIs button on the left.



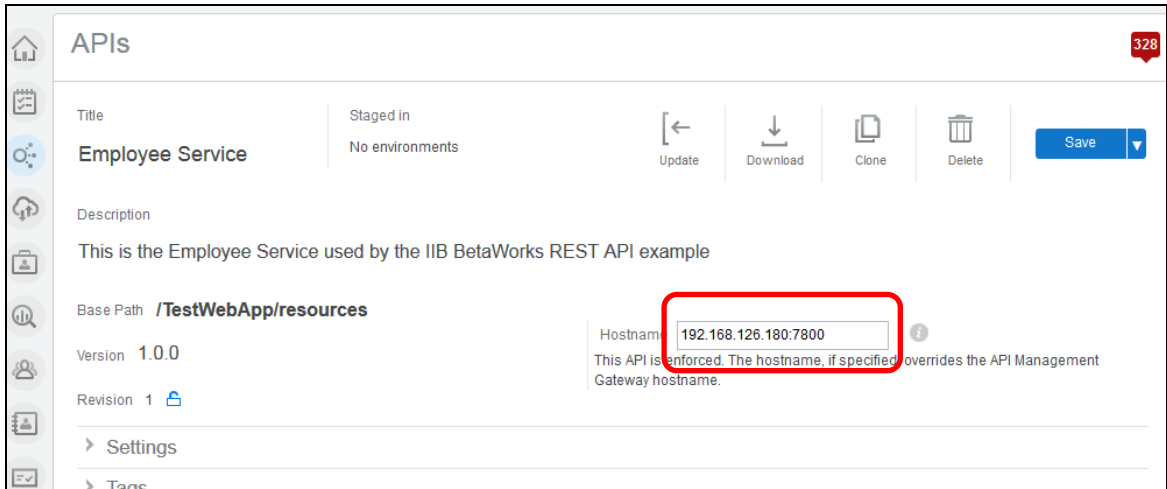
3. The **Employee Service** API should be displayed. This is the API that you pushed into IBM API Management. Click the arrow to show further details.

The click on **Employee Service** to navigate to the details of that API.

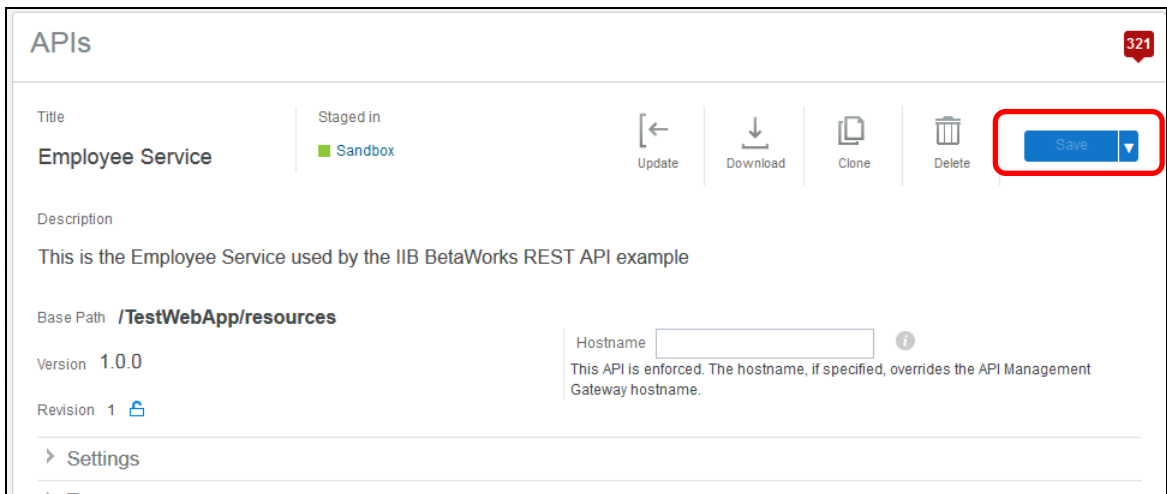


5.2 Enable enforcement by IBM API Management Gateway

1. Remove the entry in **Hostname** if present. By doing so, the API Management Gateway will be used to access the published API.



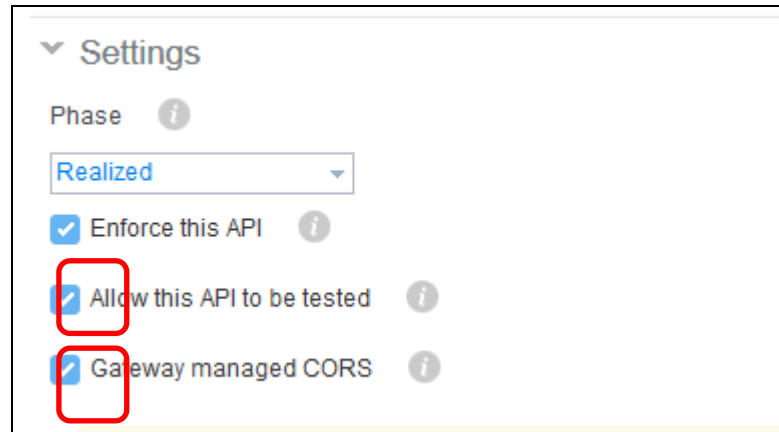
2. Save the API:



5.3 Add security settings

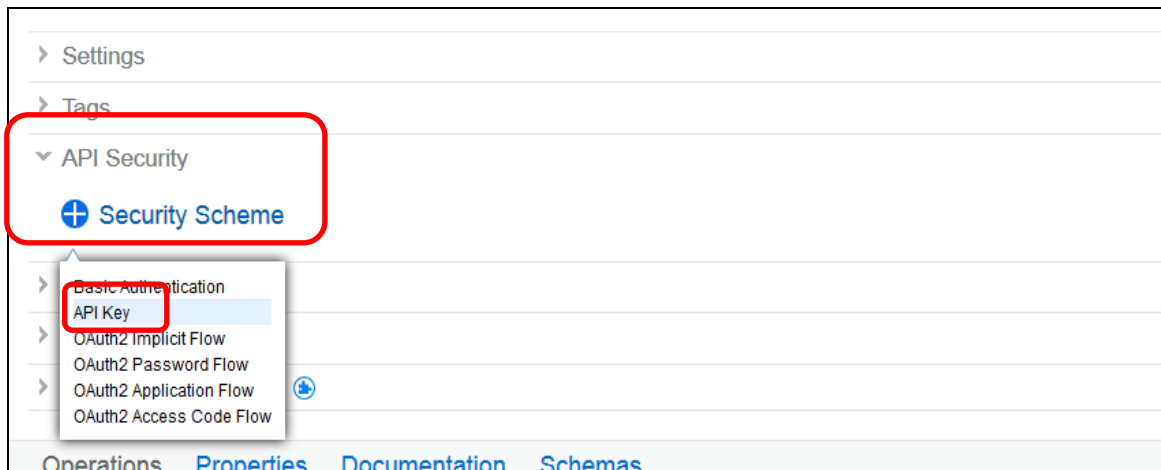
When the REST API is published, we will only accept requests submitted with a valid Client ID and Client Secret. This requirement will now be added to the API security settings.

1. Expand the Settings folder.
 - Select "Allow this API to be tested".
 - This will automatically select "Gateway managed CORS".



2. Expand **API Security**, click **+ Security Scheme**.

Select **API Key** from the drop-down menu.

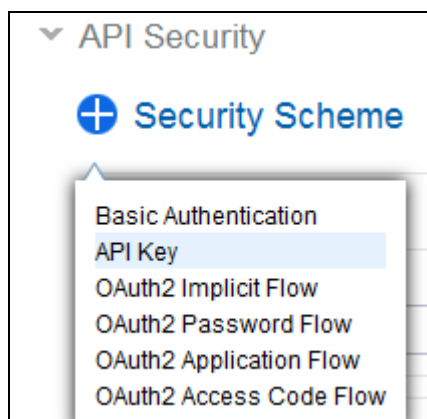


- Rename the scheme from **API Key** to **Client ID**.

Keep the default **Parameter Name** (*X-IBM-Client-Id*).

The screenshot shows the 'API Security' configuration page. Under the 'Security Scheme' section, a form for 'Client ID' is visible. The 'Name' field contains 'Client ID' and the 'Parameter Name' dropdown menu is set to 'X-IBM-Client-Id'. Both the text in the 'Name' field and the text in the 'Parameter Name' dropdown are enclosed in red rectangular boxes.

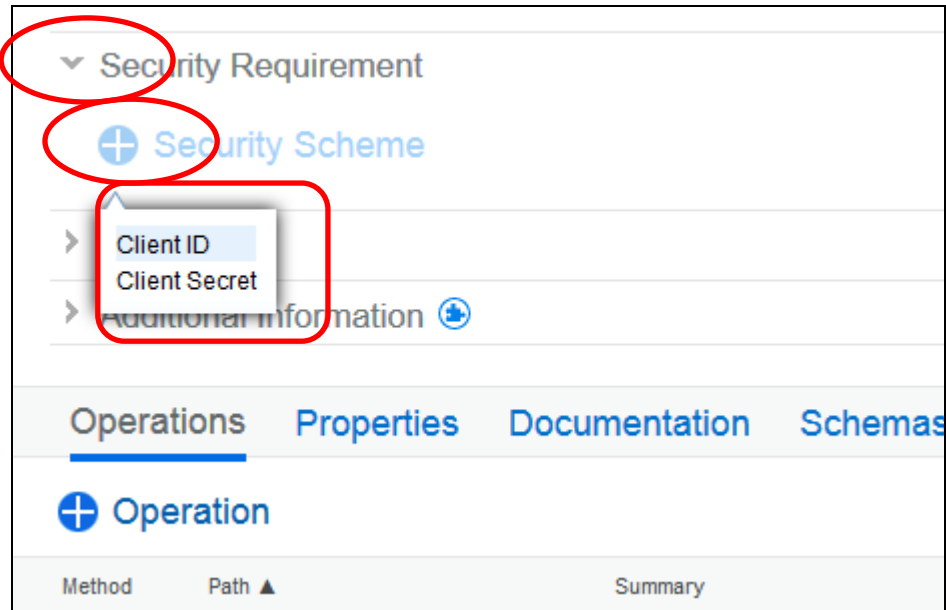
- Add another API Key Security Scheme (click + Security Scheme, select API Key from the menu).



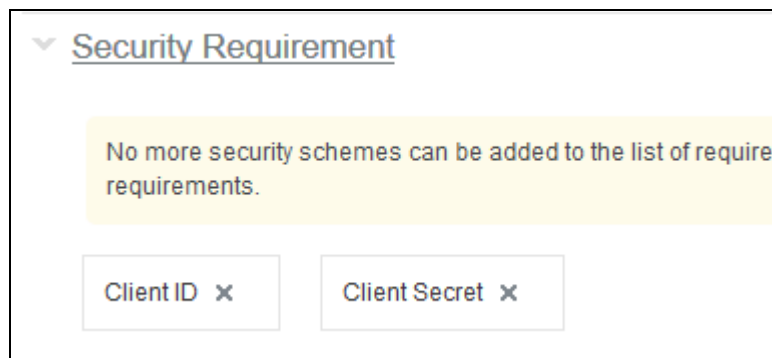
Name this scheme **Client Secret**, but change the Parameter Name to **X-IBM-Client-Secret**.

The screenshot displays the 'API Security' configuration page with two security schemes. The top scheme is named 'Client Secret'. Its 'Name' field contains 'Client Secret' and its 'Parameter Name' dropdown is set to 'X-IBM-Client-Secret'. Both the text in the 'Name' field and the text in the 'Parameter Name' dropdown are enclosed in red rectangular boxes. Below it, the 'Client ID' scheme is visible, with its 'Name' field containing 'Client ID' and its 'Parameter Name' dropdown set to 'X-IBM-Client-Id'.

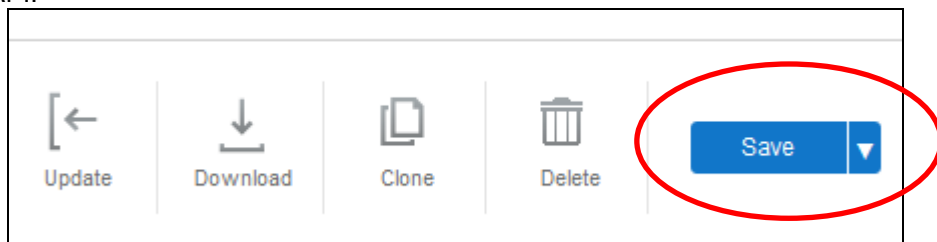
- 5. Expand **Security Requirement** and add these schemes in turn (click + Security Scheme).



- 6. Confirm that the **Security Requirement** looks like this:



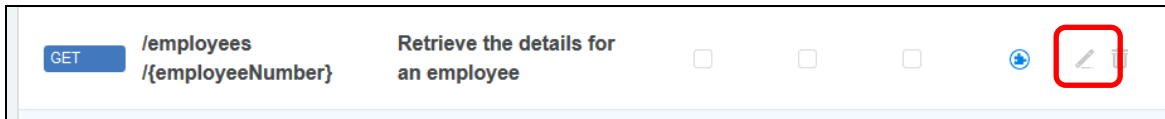
- 7. Save the API.



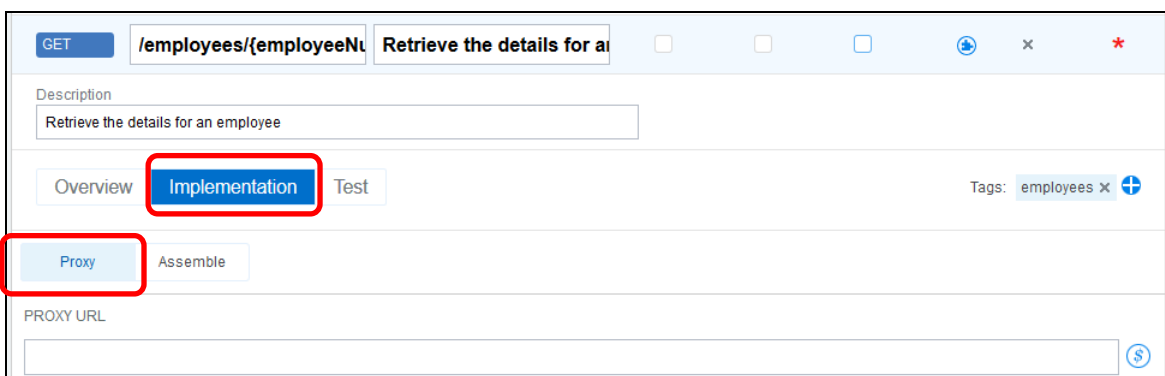
5.4 Add proxy URL

1. IBM API Management must be configured to proxy the requests for the REST API into IBM Integration Bus.
2. Locate the **Get /employees/{employeeNumber}** operation (further down the current window) and click on the **Edit** button (pencil) on the right.

The details of the operation are expanded.



3. Click on **Implementation**, and then click on **Proxy**.

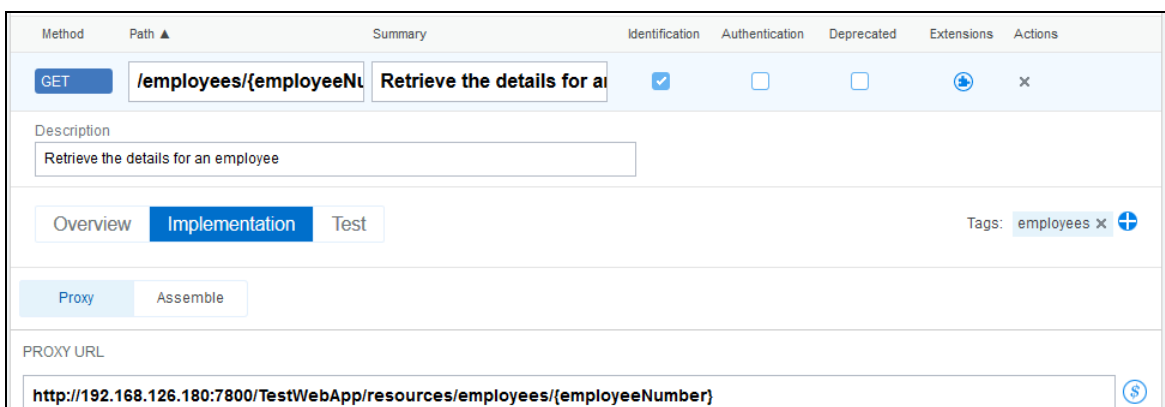


4. You must enter the full URL for the operation (not just the REST API) that is proxied to IBM Integration Bus into the Proxy URL field.

Append "**employees/{employeeNumber}**" to the **Base URL for remote invocations** that you noted earlier (section 4.1 on page 10).

In the IIB workshop system, the Proxy URL will be:

```
http://192.168.126.xxx:7800/TestWebApp/resources/employees/{employeeNumber}
```



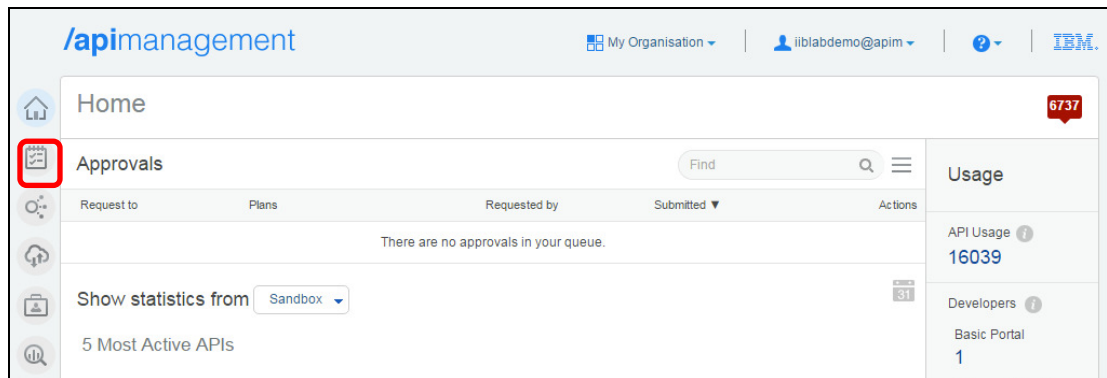
When you have set the proxy URL, go to the top of the page and click **Save**.

6. Create and publish use plan for REST API

6.1 Add REST API to new API Management plan

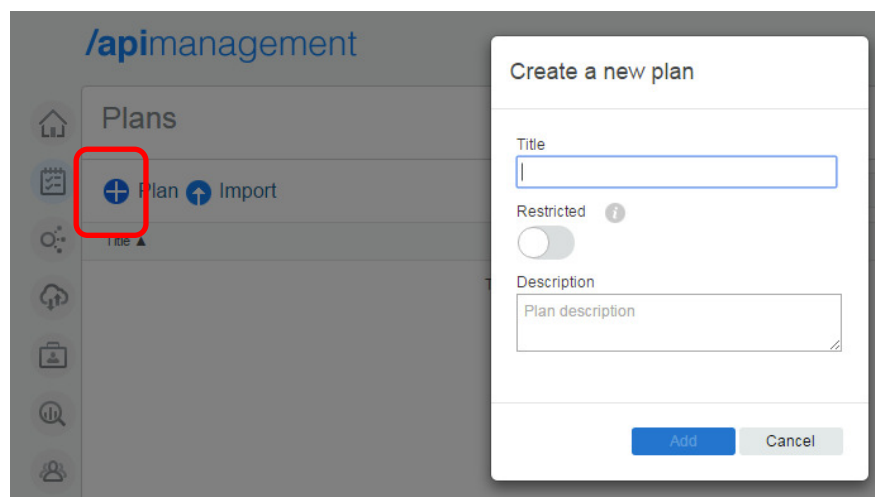
The REST API is now configured in IBM API Management. In order to expose the REST API to clients, it must be first put into a plan. Developers can then request access to the plan in order to use the REST API.

1. Click on the **Plans** button on the left. The Plans page will be displayed.



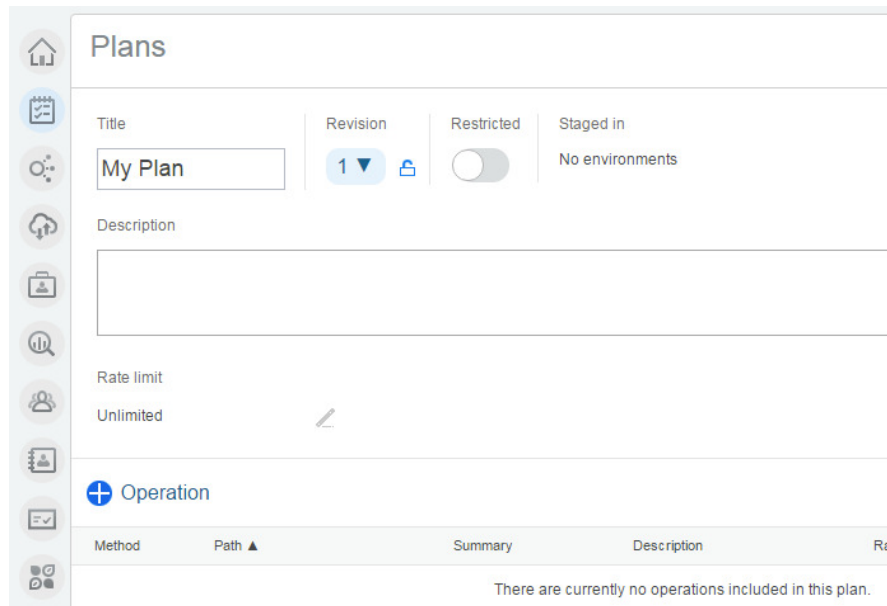
2. Click on the **+** button next to Plan to open the "Create a new plan" dialog.

Give the plan a name, for example **My Plan**, and click **Add**. The page for that plan will then be displayed.

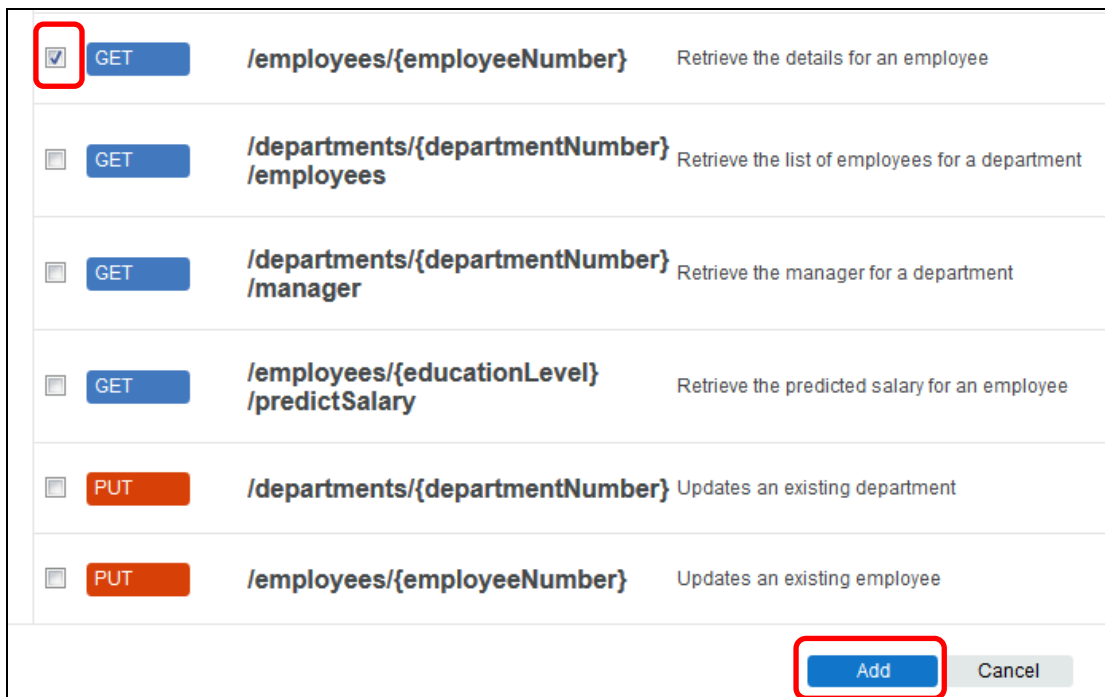


- At the bottom of this page, you can see that there are no operations included in this plan. You must add the operations from the REST API into this plan.

Click on the + button next to Operation in order to open the Add operations dialogue.



- Select the **GET /employees/{employeeNumber}** and click **Add**:



- The operation is displayed at the bottom of the plan. Now you will apply a limit to the number of requests per minute that will be accepted by the Gateway under this plan.

(In practice, you may want to create different plans with different limits that can be charged accordingly, e.g. a free basic plan with a low limit and a chargeable plan with a high limit.)

(Note: it is also possible to apply rate limits to the individual operations within a plan. In this case, there is just one operation and the limit is being defined at the plan level).

Click on the Edit symbol (pencil) for the rate limit, highlighted below.

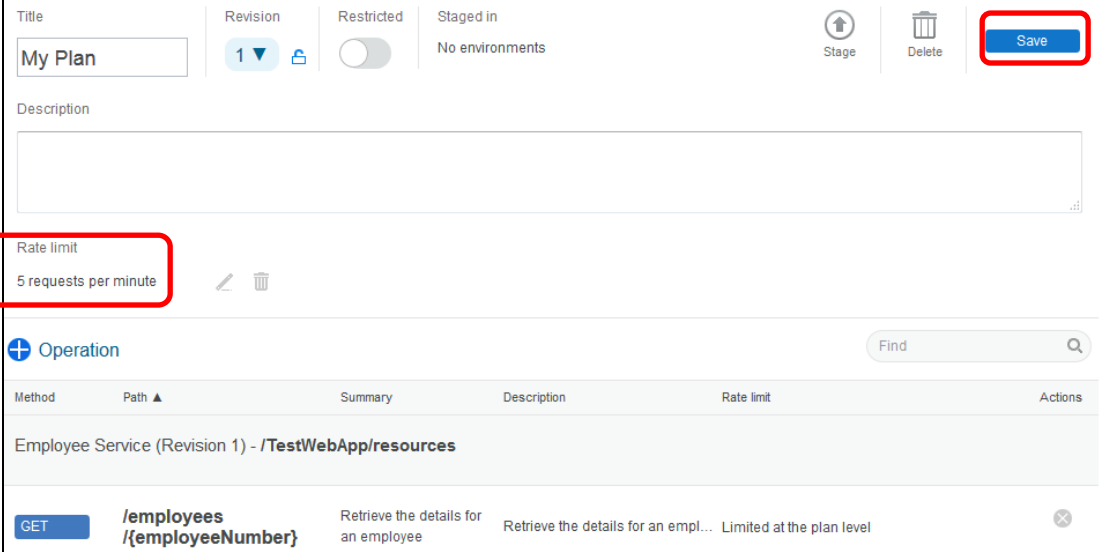
The screenshot shows the IBM API Management console interface. At the top, there is a header with 'Title: My Plan', 'Revision: 1', 'Restricted: [toggle]', and 'Staged in: No environments'. There are buttons for 'Stage', 'Delete', and 'Save'. Below the header is a 'Description' field. The 'Rate limit' section shows 'Unlimited' with a red box around the edit pencil icon. Below that is an 'Operation' section with a table listing operations. The first operation is 'Employee Service (Revision 1) - /TestWebApp/resources' with a 'GET' method and path '/employees/{employeeNumber}'. The 'Rate limit' column for this operation is 'Unlimited', and a red box highlights the edit pencil icon next to it.

- At the prompt, set the **Number of Requests** to 5, and click **Apply**.

Make sure the box "Reject calls when limit is reached" is ticked.

The screenshot shows the 'Rate limit' dialog box in the IBM API Management console. The dialog has a title 'Rate limit' and two input fields: 'Number of Requests' set to 5 and 'Time Interval' set to 1 Minutes. There is a checkbox labeled 'Reject calls when limit is reached' which is checked. A red box highlights the 'Apply' button at the bottom right of the dialog. The background shows the same 'Employee Service' operation as in the previous screenshot.

7. The **Rate limit** has been changed. Save the plan by clicking on the **Save** button at the top of the page.



The screenshot displays the configuration page for a plan named "My Plan". At the top, there are fields for "Title" (My Plan), "Revision" (1), "Restricted" (toggle off), and "Staged in" (No environments). Action buttons for "Stage", "Delete", and "Save" are visible. The "Rate limit" section shows "5 requests per minute" with edit and delete icons. Below is a table of operations.

Method	Path ▲	Summary	Description	Rate limit	Actions
Employee Service (Revision 1) - /TestWebApp/resources					
GET	/employees/{employeeNumber}	Retrieve the details for an employee	Retrieve the details for an empl...	Limited at the plan level	✕

6.2 Test REST API (as API manager)

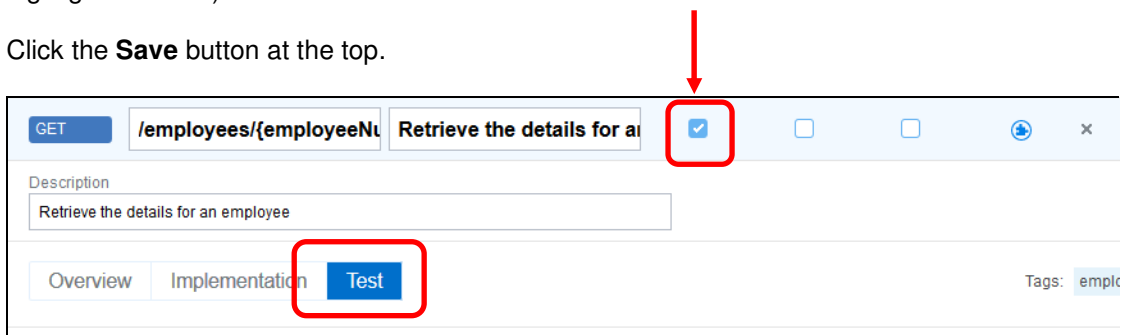
1. Click on the APIs button at the left and navigate once more to the **Get /employees/{employeeNumber}** operation in the **Employee Service** API (reminder - expand EmployeeService, click Employee Service).

Click the **Edit** button (pencil).

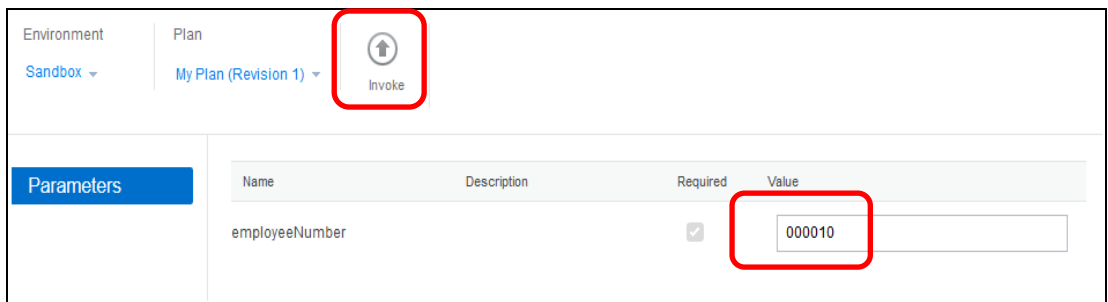


2. Click on the **Test** tab, and place a tick in the identification column (it's the first column, as highlighted below).

Click the **Save** button at the top.




3. Enter a value of '000010' for employeeNumber and click on the **Invoke** button (highlighted below).



4. The details of the employee should be returned:

Parameters	200 OK
Response	<pre>X-Global-Transaction-ID: 19840 Access-Control-Allow-Origin: * Date: Sun, 10 Jan 2016 11:47:21 GMT Transfer-Encoding: chunked X-Backside-Transport: OK OK X-RateLimit-Remaining: 4 X-RateLimit-Limit: 5 APIM-Debug-Trans-Id: 55e709bae4b07be2adf593ee-57391ae2-511 APIM-Debug-Filename: temporary:///apimdebug051d9.json Content-Type: application/json; charset=utf-8 Connection: Keep-Alive Server: Apache-Coyote/1.1</pre>
	<pre>{ "EmployeeResponse": { "DBResp": { "UserReturnCode": 0, "RowsRetrieved": 1, "RowsAdded": 0, "RowsUpdated": 0, "RowsDeleted": 0, "SQLCode_ErrorCode": 0, "SQLState_SQLState": null, "SQL_Error_Message": null }, "EMPLOYEE": { "EMPNO": "000010", "FIRSTNAME": "CHRISTINE", "MIDINIT": "I", "LASTNAME": "HAAS", "WORKDEPT": "A00", "PHONENO": "3978",</pre>

- Invoke this test a few more times. On the sixth try in one minute, the request should be rejected. This is because the Gateway is enforcing the limit for this API (as defined in the plan).



The screenshot displays the response of an API Gateway. The title is "429 Too Many Requests" with a "Debug" link in the top right. On the left, there are tabs for "Parameters" and "Response", with "Response" selected. The response content is as follows:

```
Retry-After: 20
X-Backside-Transport: FAIL FAIL
Access-Control-Allow-Origin: *
X-RateLimit-Remaining: 0
X-RateLimit-Limit: 3
APIM-Debug-Trans-Id: 55e709bae4b07be2adf593ee-ae2a6231-3558-444c-bbc6-85529c989f8a
APIM-Debug-Filename: temporary:///apimdebug82088.json
X-RateLimit-Reset: 20
Connection: close
Content-Type: application/json

{
  "statusCode": "429",
  "httpMessage": "Too Many Requests",
  "moreInformation": "Rate Limit exceeded"
}
```

Note that the rate limit and number of remaining tries are returned by the plan. Also note the time that you have to wait until sending the next request ("Retry-After").

If you send another request before this time interval, you will see the remaining time decrease in the subsequent response.

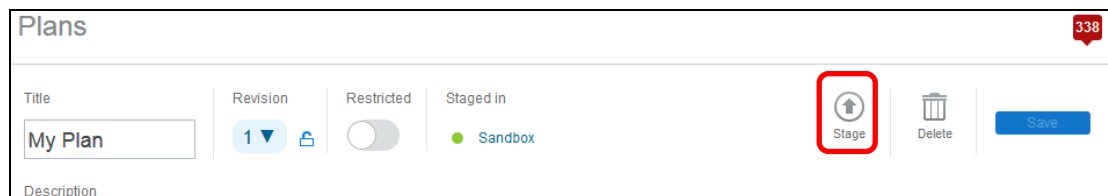
6.3 Stage and publish plan

The plan must now be staged into an environment, and then published into that environment. This activity pushes configuration details onto the IBM DataPower Gateway appliance that will then proxy requests to the deployed REST API on IBM Integration Bus.

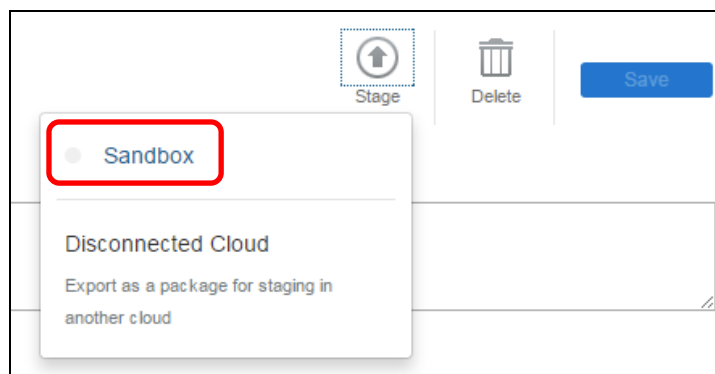
1. Click the Plans icon to return to the page for the plan created in the previous step.

Click "My Plan".

Click on the **Stage** button:

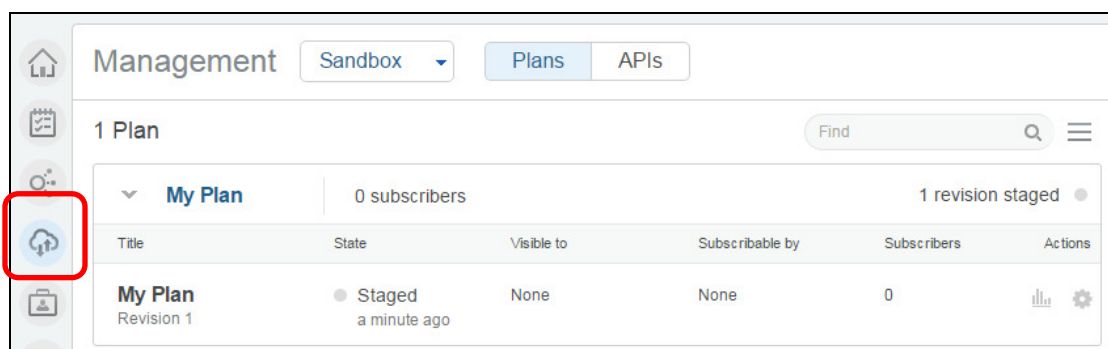


2. Click on the **Sandbox** environment:

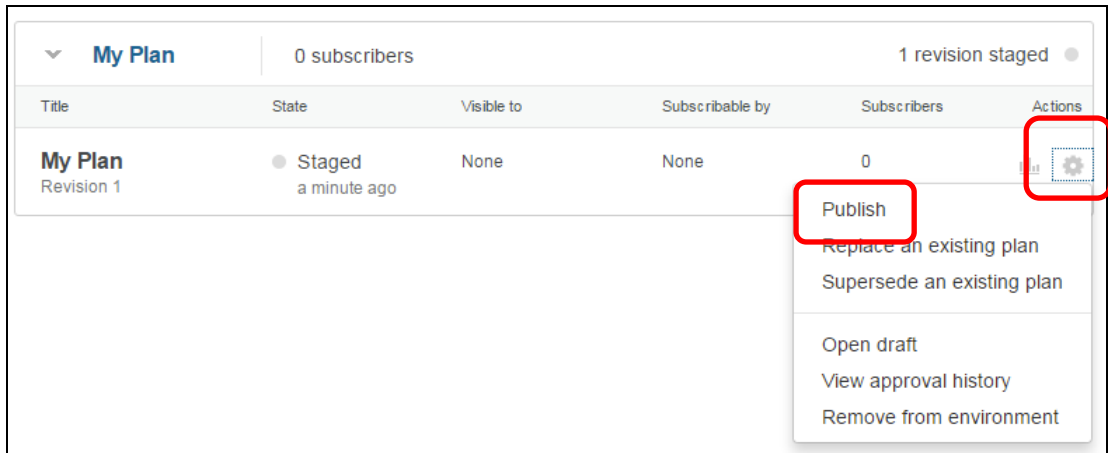


3. Once the plan has been staged, it must be published.

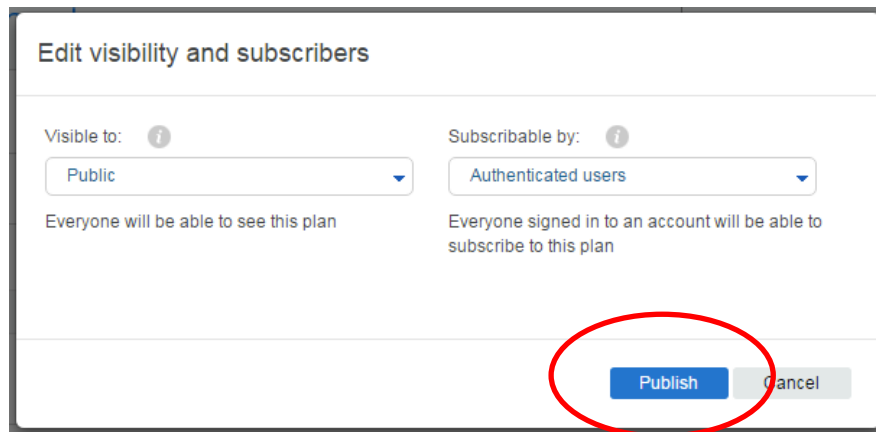
Click on the Management button on the left. The Management page will be displayed, and should show the plan in Staged state:



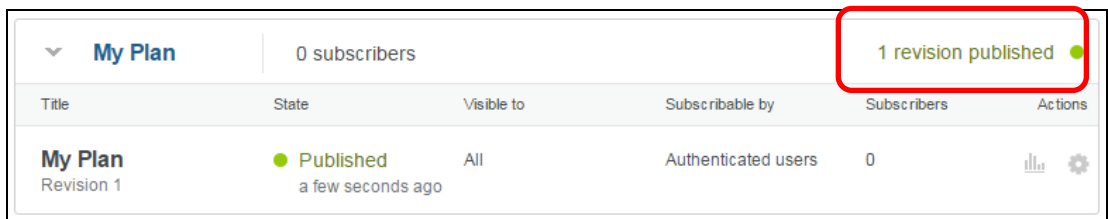
- 4. Click on the cog icon on the right and then click on **Publish**:



- 5. The **Edit visibility and subscribers** dialogue will appear. Click **Publish**:



- 6. The plan should now be shown as **Published**:



7. Publish REST API

7.1 Document application to use REST API

Now that the plan has been published, developers can associate the REST API with an application.

1. In the Firefox browser, open a new tab and login as an APIM Developer.

In the IIB workshop, use the shortcut in the APIM folder (APIM Developer).

This will be:

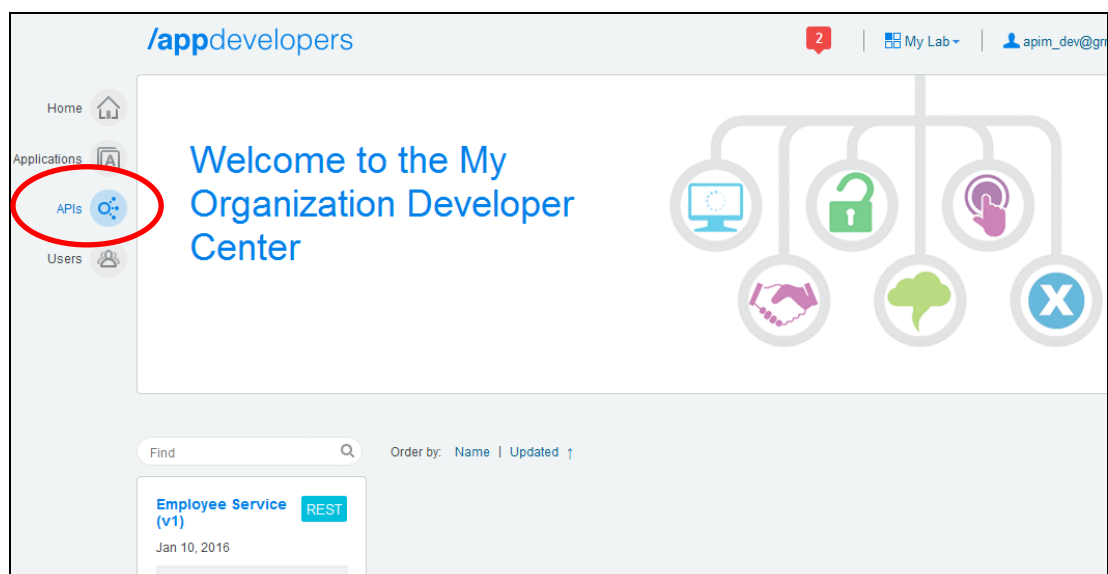
`https://192.168.126.100/myorg/sb#/apis`

Click "Sign in", and login with the API Manager Developer account:

- UserID: apim_dev@grr.la
- Password: passw0rd! (note the '!' at the end).

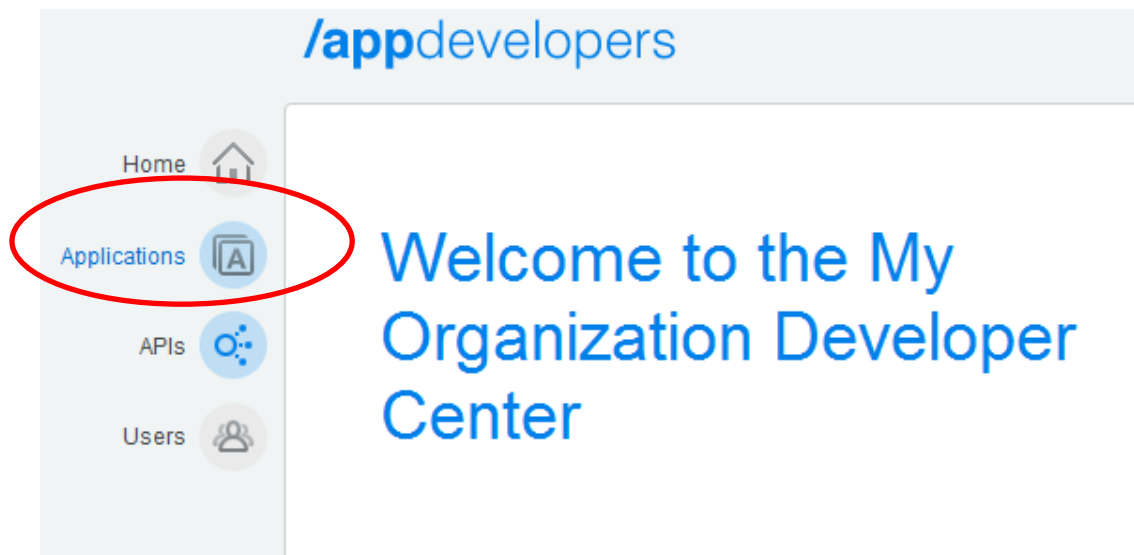
You are now logged on to the Basic Developer Portal as a developer.

2. When you have logged in, click the APIs button in the navigator. The Home page will be displayed.

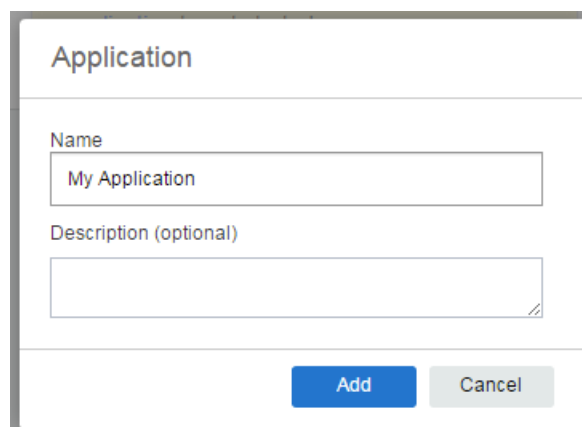


3. You can see your published REST API at the bottom of the page. In order to request access to the REST API, you first need to create a record of the client application that will be accessing this REST API.

Click on **Applications** on the left. The **Applications** page will be shown:

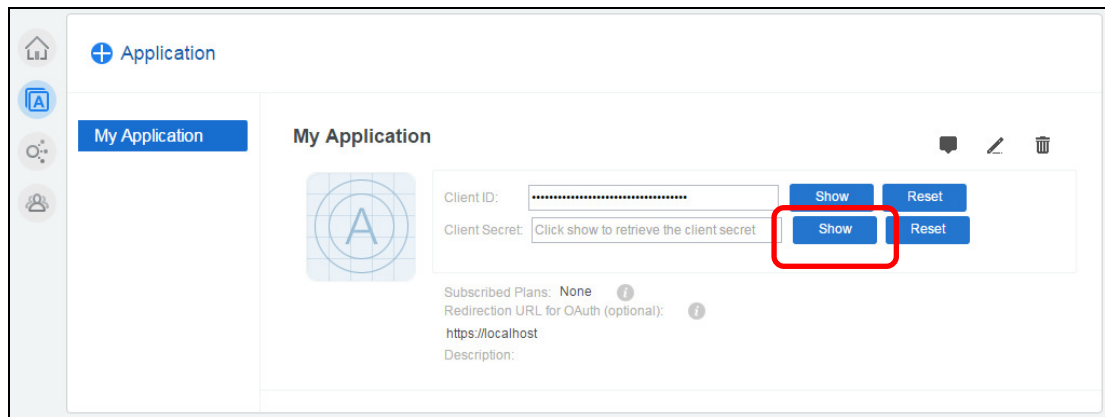


4. Create a new application by clicking the **+** button next to Application. Give the application a name, for example **My Application**, and click **Add**:

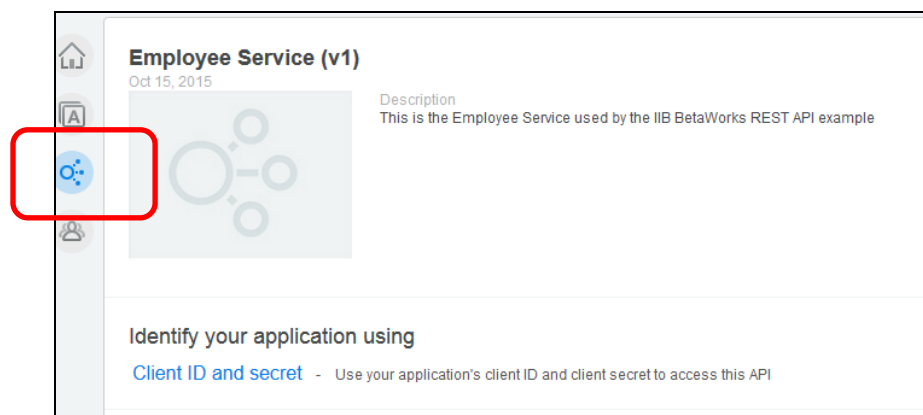
A screenshot of a form titled 'Application'. It contains two input fields: 'Name' with the text 'My Application' and 'Description (optional)' which is empty. At the bottom right, there are two buttons: 'Add' (blue) and 'Cancel' (grey).

- The application will now appear in the list of applications. Show and copy the **Client Secret**. (Use **Ctrl-A**, then **Ctrl-C**).

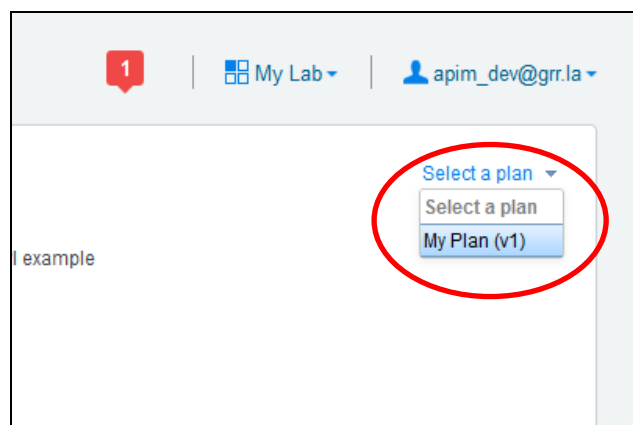
Note: this will be the only opportunity to see the Client Secret, so for safe-keeping, store (paste) this string into the txt file you created earlier.



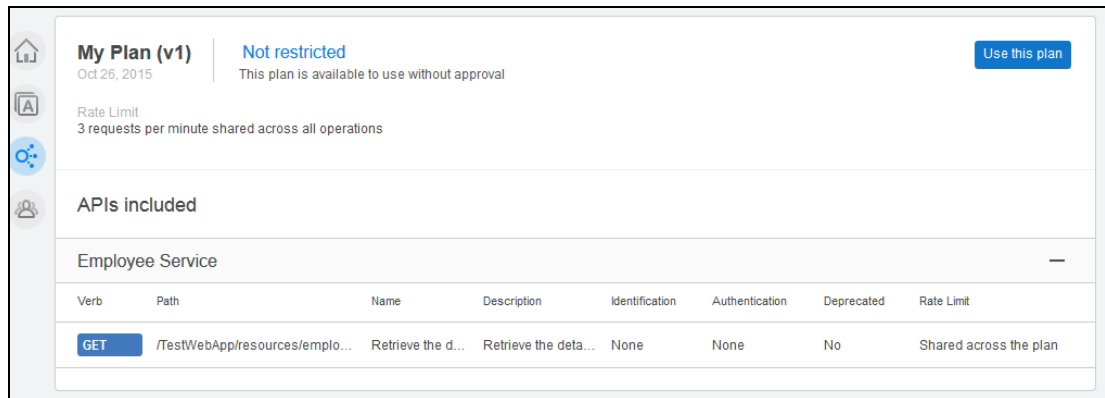
- Click on the **APIs** button on the left and then click on **Employee Service (v1)** at the bottom of the page. The page for that REST API will be displayed, along with the GET operation:



- In the list of operations at the bottom of the page, you can see which operations are available in which plans. In order to request access to the REST API, click on the **Select a plan** link at the top of the page. Click on the name of the plan you created earlier (My Plan).



8. The details of the plan then appear:



My Plan (v1) Not restricted Use this plan
Oct 26, 2015 | This plan is available to use without approval

Rate Limit
3 requests per minute shared across all operations

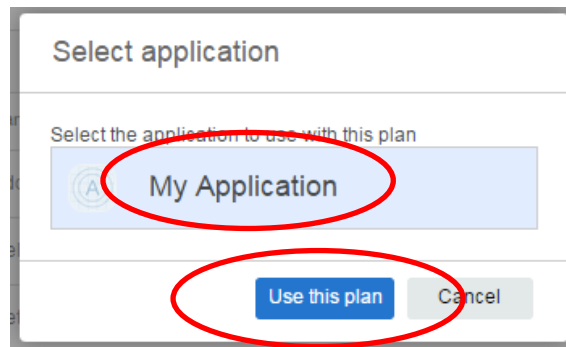
APIs included

Employee Service

Verb	Path	Name	Description	Identification	Authentication	Deprecated	Rate Limit
GET	/TestWebApp/resources/emplo...	Retrieve the d...	Retrieve the deta...	None	None	No	Shared across the plan

9. Click on **"Use this plan"**. The **Select application** dialog then appears. Click on the application you documented earlier, and then click on **Use this plan**.

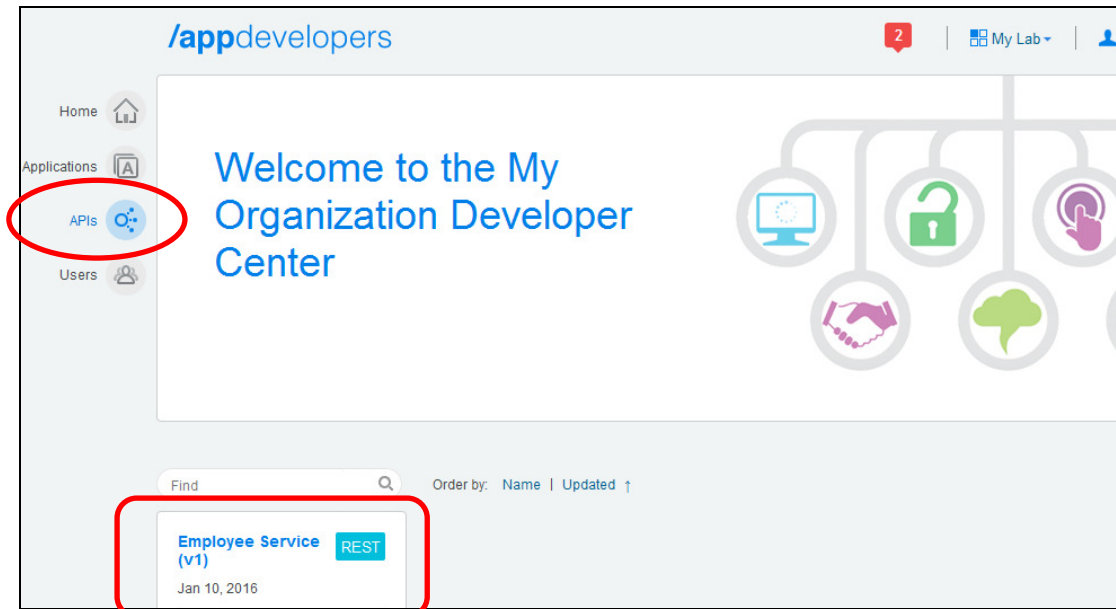
Now that your application is configured to use the plan, it can invoke the REST API through IBM API Management.



7.2 Discover URL for published REST API

In associating the application with the REST API, the published REST API is now available for use. This REST API will be subject to the restrictions (security and rate-limits) configured by the API manager earlier on and enforced at the IBM DataPower Gateway.

1. Click on the APIs button on the left and then click on **Employee Service (v1)** at the bottom of the page.



2. The page for that REST API will be displayed. Find the GET operation at the bottom of the API.

Click on the + button in the Details column for that operation.

Operations							Plans
Verb	Path ▲	Name	Identification	Authentication	Deprecated	Details	My Plan (v1) ▼
GET	/TestWebApp/resources/employees/...	Retrieve the d...	None	None	No	+	✓

- Note the URL of the published API. The IP address is now that of the IBM DataPower Gateway.

The following variables are to be substituted when using this URL:

- Employee Number: {employeeNumber}
- Client ID: <client_id>
- Client Secret: <client_secret>

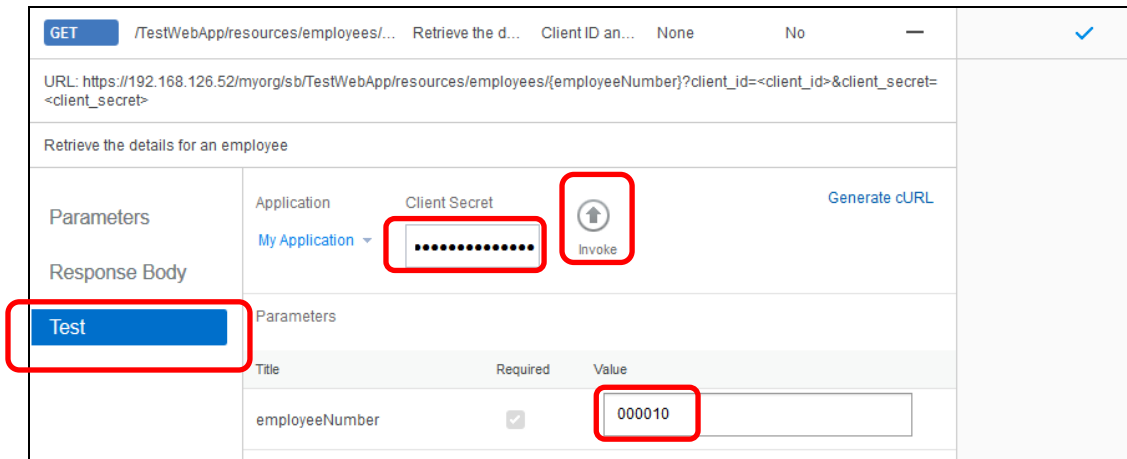
Operations							Plans
Verb	Path ▲	Name	Identification	Authentication	Deprecated	Details	My Plan (v1) ▾
GET	/TestWebApp/resources/employees/...	Retrieve the d...	Client ID an...	None	No	—	✓
URL: <code>https://192.168.126.52/myorg/sb/TestWebApp/resources/employees/{employeeNumber}?client_id=<client_id>&client_secret=<client_secret></code>							
Retrieve the details for an employee							
Parameters		Type	Name	Description	Required		
		🔗	employeeNumber		Yes		
Response Body							
Test							

7.3 Test published REST API

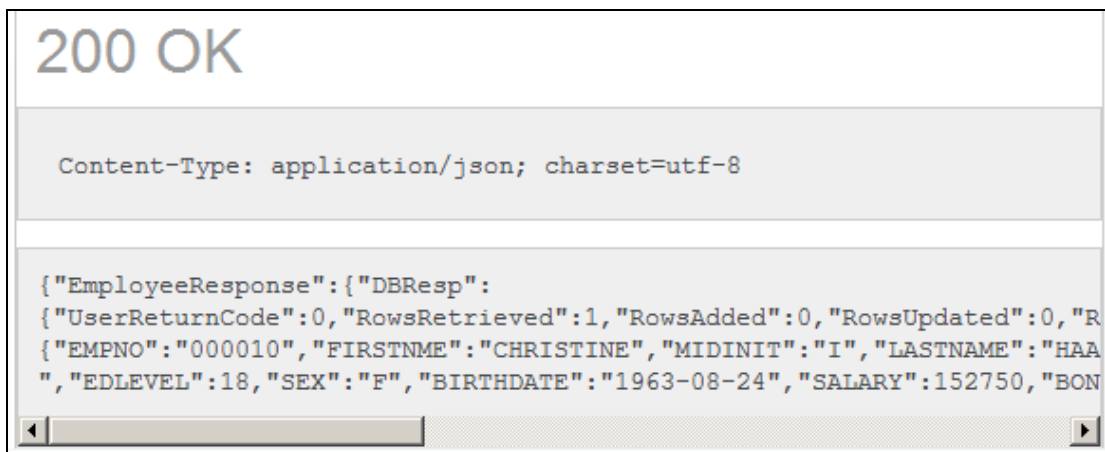
Now that the REST API has been associated with the application, the IBM DataPower Gateway appliance can be used to manage access for the API.

1. First, we will test the published REST API using the facility provided. To do this, click on the **Test** button, enter a valid employeeNumber (e.g. 000010), enter the **Client Secret** (Ctrl-V to paste from the clipboard, or from the txt file), and then click on the **Invoke** button.

Note: there is no prompt for **Client ID**, as that is already known (from the documented application).



2. The details of the employee should be returned:



3. Invoke this test a few more times. On the sixth try in one minute, the request should be rejected. This is because the Gateway is enforcing the limit for this API (as defined in the plan). Note the URL used includes the Client ID and Client Secret.

```
Response

429 Too Many Requests

Unable to load https://192.168.126.52/myorg/sb/TestWebApp/resources/employees
/000010?client_id=9f361d9e-9fff-4d4e-8ce8-2cf0f583555a&
client_secret=aL3wD6el6gS4bR7mY3cL3wC5oG2fY5xJ7vC1cO1aM6oL1qV5gU status: 429

Content-Type: application/xml

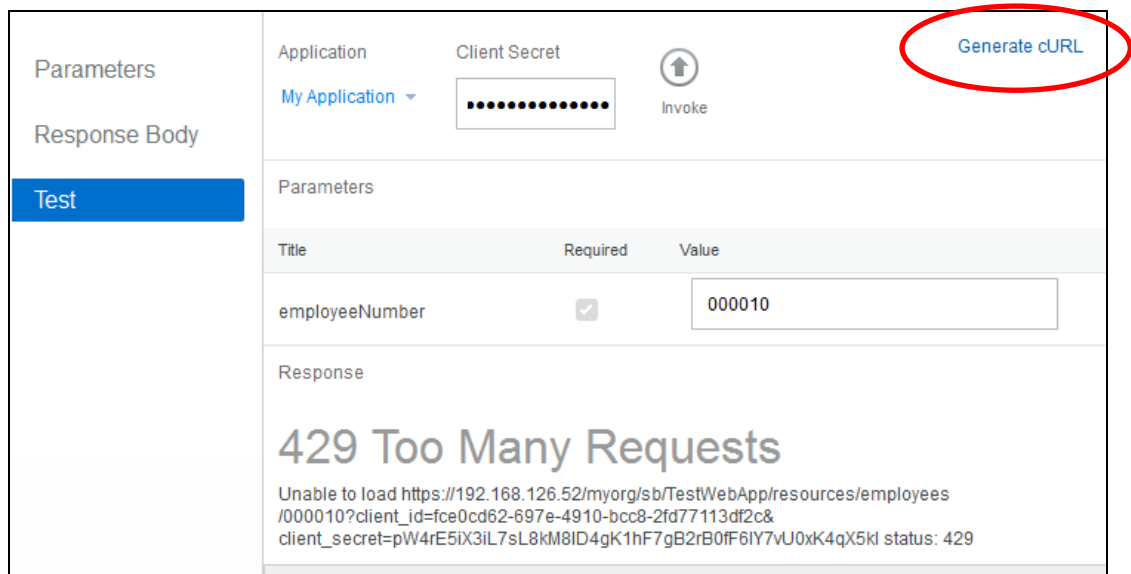
<!--
  ?xml version="1.0" encoding="UTF-8"?
-->
<errorresponse>
```

8. Invoke the published REST API

In this section, you will make requests to the published REST API, firstly from a browser and then from SOAPUI. (SOAPUI can be used to test REST APIs as well as SOAP APIs).

8.1 Invoke from browser

1. To use the API outside of the APIM environment, obtain the URL. Do this by clicking "Generate cURL".



The screenshot shows the API Management console interface. On the left, there are tabs for 'Parameters', 'Response Body', and 'Test'. The 'Test' tab is selected. The main area shows the API configuration with 'Application' set to 'My Application' and 'Client Secret' masked with dots. A 'Generate cURL' button is circled in red. Below the configuration, a table lists parameters, with 'employeeNumber' set to '000010'. The response area displays a 429 status code: '429 Too Many Requests'.

Title	Required	Value
employeeNumber	<input checked="" type="checkbox"/>	000010

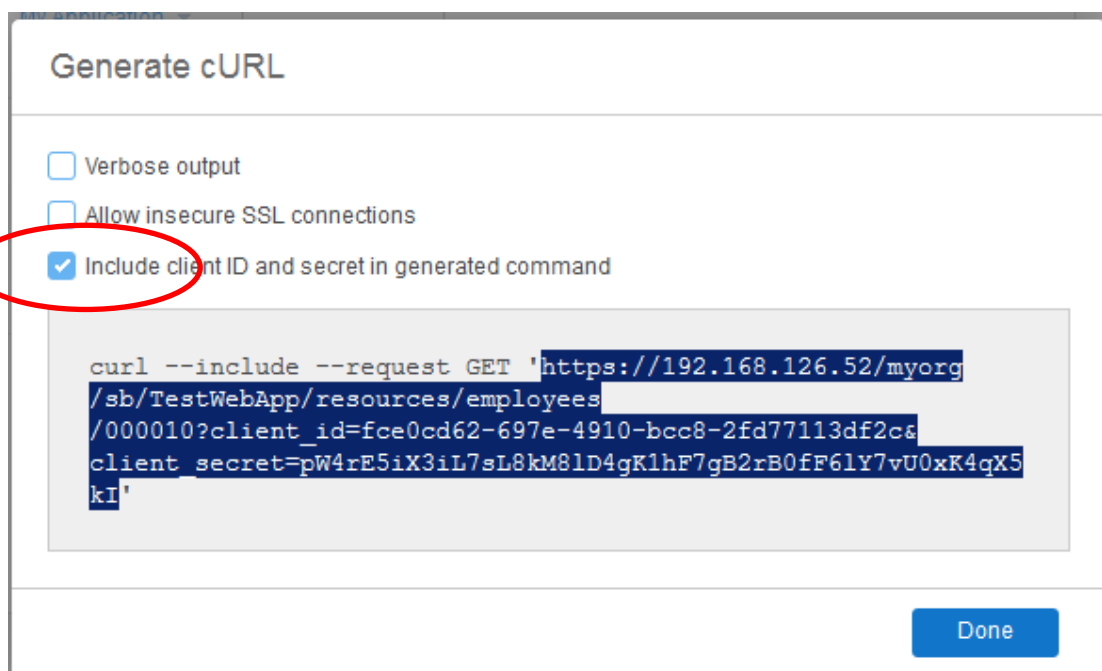
Response

429 Too Many Requests

Unable to load https://192.168.126.52/myorg/sb/TestWebApp/resources/employees/000010?client_id=fce0cd62-697e-4910-bcc8-2fd77113df2c&client_secret=pW4rE5iX3iL7sL8kM8lD4gK1hF7gB2rB0f6lY7vU0xK4qX5kl status: 429

2. In the cURL dialogue, select "Include client ID and secret.....".

Carefully select the URL (excluding quotation marks), then Copy to the clipboard (Ctrl-C).



The screenshot shows the 'Generate cURL' dialog box. It has three checkboxes: 'Verbose output', 'Allow insecure SSL connections', and 'Include client ID and secret in generated command'. The third checkbox is checked and circled in red. Below the checkboxes, a text area contains the generated cURL command:

```
curl --include --request GET 'https://192.168.126.52/myorg/sb/TestWebApp/resources/employees/000010?client_id=fce0cd62-697e-4910-bcc8-2fd77113df2c&client_secret=pW4rE5iX3iL7sL8kM8lD4gK1hF7gB2rB0f6lY7vU0xK4qX5kl'
```

A 'Done' button is located at the bottom right of the dialog.

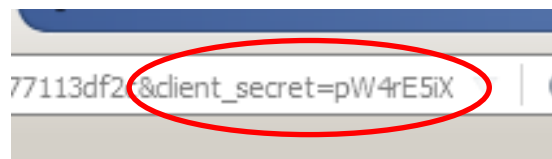
- Open a new browser tab, paste the URL into the address and click return. The employee's details should be returned.



Again, if you exceed the rate limit (5 times in one minute), the threshold will be exceeded and an error message will occur:

```
<errorResponse>
  <httpCode>429</httpCode>
  <httpMessage>Too Many Requests</httpMessage>
  <moreInformation>Rate Limit exceeded</moreInformation>
</errorResponse>
```

- Make a change to the Client Secret in the URL and submit the request. It should now be rejected:



```
<errorResponse>
  <httpCode>401</httpCode>
  <httpMessage>Unauthorized</httpMessage>
  <moreInformation>Invalid client id or secret.</moreInformation>
</errorResponse>
```

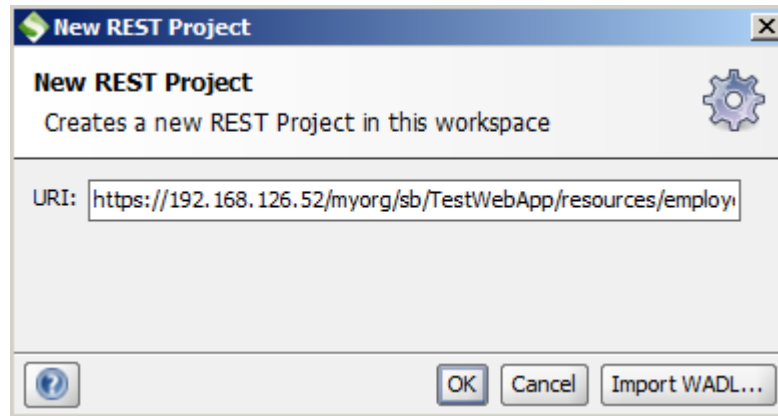
- Correct the client secret in the URL (or re-paste the original URL) and re-submit the request. It should be accepted once more.

Keep the browser tab open – you will need it again.

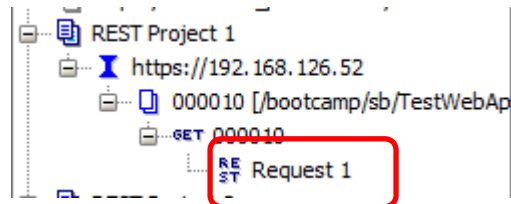
8.2 Request from SOAPUI

1. Locate and start SOAPUI from the Start Menu.
2. Click on **File**, then **New REST Project**.
3. The **New REST Project** dialogue will open. You must specify an example of the URL of the operation in the published REST API. Use the URL you used when you tested the published REST API in a browser (last section). This includes the client-secret.

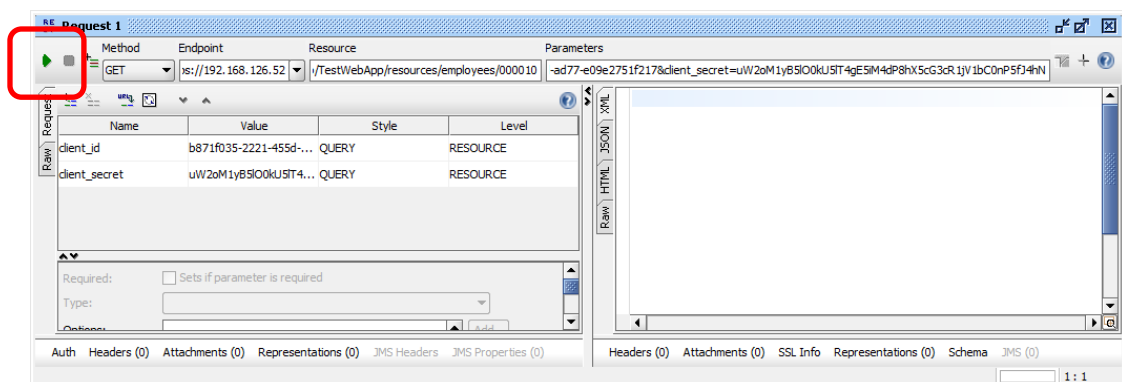
Click **OK**.



4. A new REST API project will be created and within it, a new request:

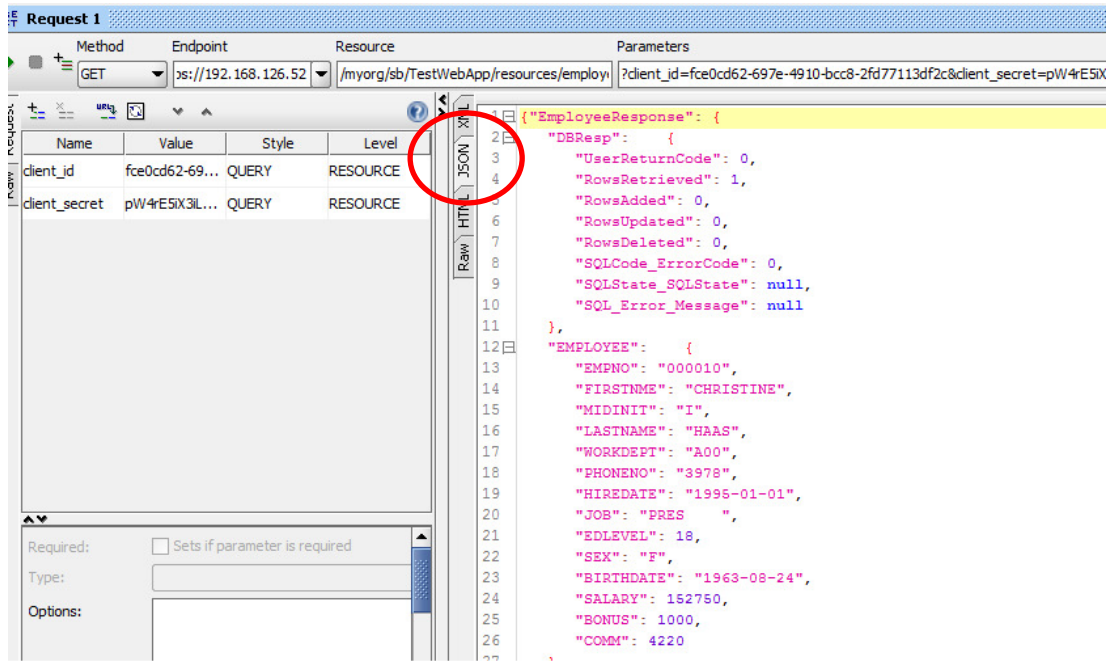


5. The new request will appear as follows. Click on the play button (green arrow) on the request.



6. The results will be displayed on the right.

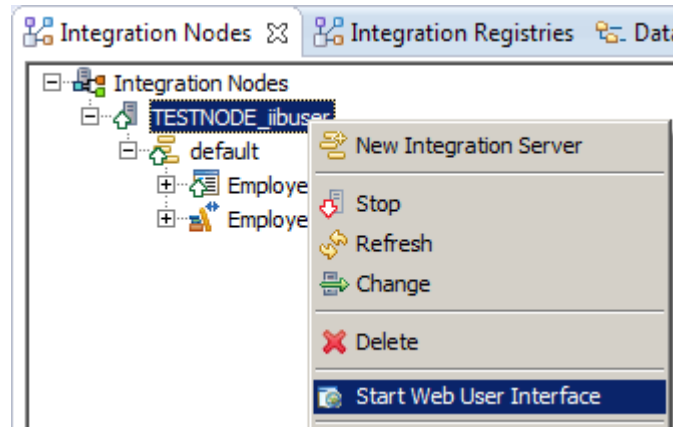
Click the JSON tab to make sure the data is shown in JSON format.



8.3 View throughput for published REST API in IIB Web UI

The web user interface for an integration node can be used to view throughput information for a REST API.

1. In the Integration Toolkit, navigate to the Integration Nodes view. Right click **TESTNODE_iibuser**, and click on **Start Web User Interface**:

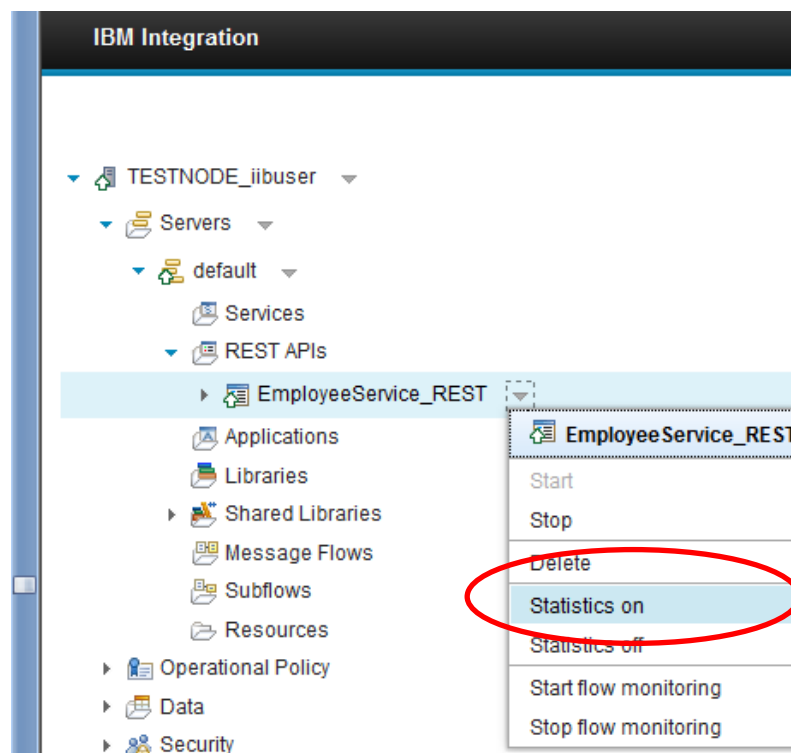


A web browser will automatically open and open the web user interface.

2. In the web user interface, expand **TESTNODE_iibuser** to find the REST API that you have deployed.

Click on the drop down arrow to the right of the **EmployeeService_REST** label. (Do not click on the **EmployeeService_REST** API!)

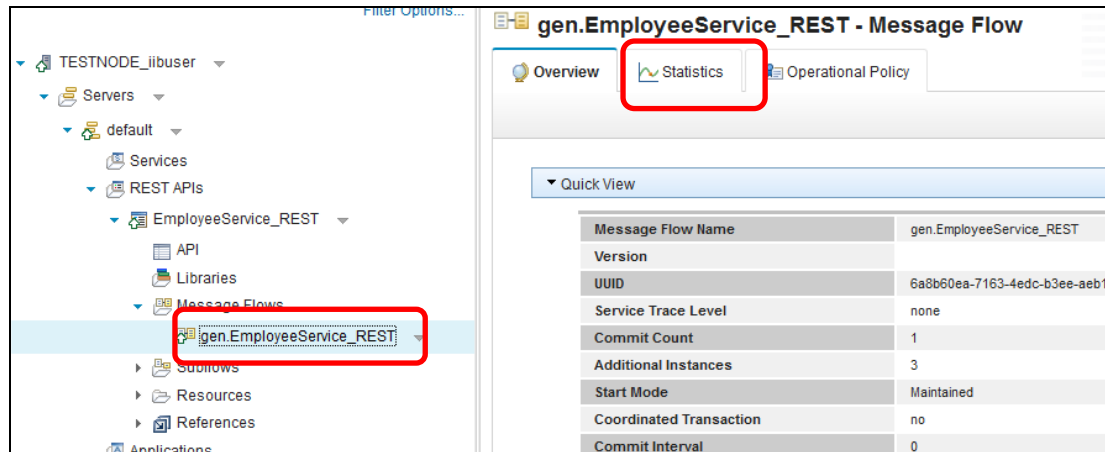
Click on **Statistics on** to enable statistics collection for this REST API:



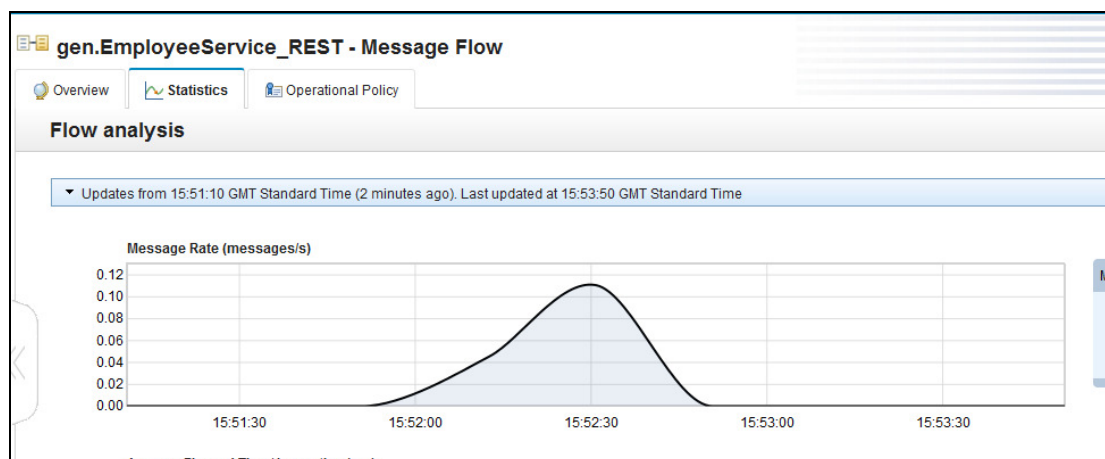
- A message will appear after a few seconds to confirm that flow statistics have been successfully turned on. Statistics will now be collected for all requests made to the published REST API.

In order to view these statistics, navigate to message flow **gen.EmployeeService_REST**.

Click on the message flow, and then click on the **Statistics** tab at the right.



- The statistics view is updated every 20 seconds. Use SOAPUI to manually submit several requests to the published REST API and you should see the statistics view in the web user interface updated accordingly:



9. Load Test published REST API

A load test will be run to show how IBM API Management can be used to control throughput (at the application level) so that a backend system such as a database is not adversely affected by traffic spikes.

Note: throughput is controlled by the IBM DataPower Gateway which can be placed at the edge of a network.

In order to do this, the API Management plan **My Plan** will be retired.

9.1 Change use plan rate limit

1. First, in the API Manager Appliance UI, click on the **Management** icon at left.

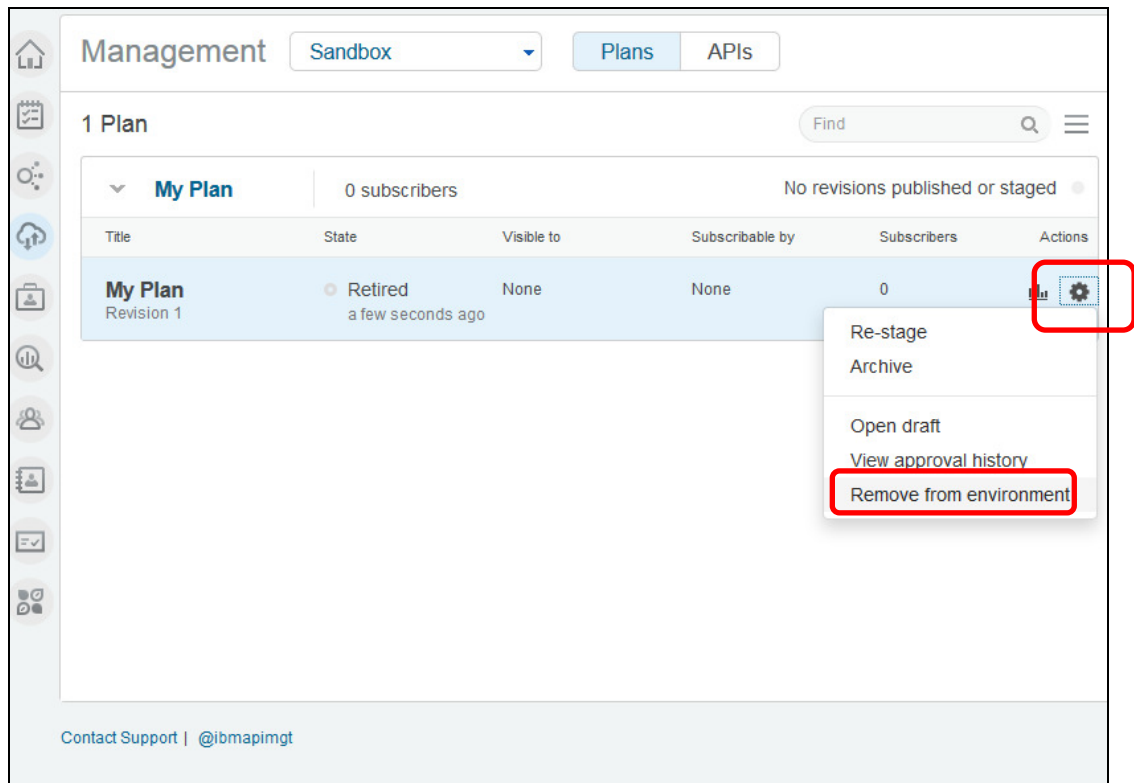
Select plan **My Plan**, and click on the **Actions** icon (cog icon),

Select **Retire** from the menu, and click **OK** to confirm.

The screenshot shows the IBM API Management UI. The top navigation bar includes 'Management', 'Sandbox', 'Plans', and 'APIs'. The main content area displays '1 Plan' with a search bar and a table listing plans. The table has columns for Title, State, Visible to, Subscribable by, Subscribers, and Actions. The 'My Plan' row is highlighted, and the 'Actions' icon (cog) is highlighted with a red box. A dropdown menu is open, showing options: Deprecate, Retire, Migrate subscriptions, Edit visibility and subscribers, Open draft, and View approval history. The 'Retire' option is highlighted with a red box. The left sidebar contains various icons, with the 'Management' icon (a gear with a plus sign) highlighted with a red box. The footer includes 'Contact Support | @ibmapimgt'.

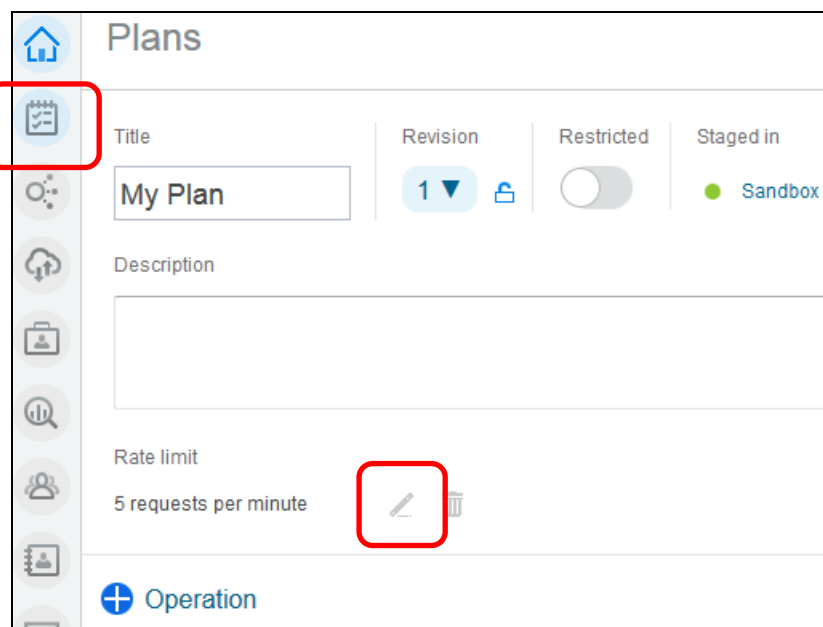
Title	State	Visible to	Subscribable by	Subscribers	Actions
My Plan Revision 1	Published 16 minutes ago	All	Authenticated users	1	

- Then click on the **Actions** icon again, and select "Remove from environment", and confirm.



- Select the **Plans** icon at the left and open plan **My Plan**.

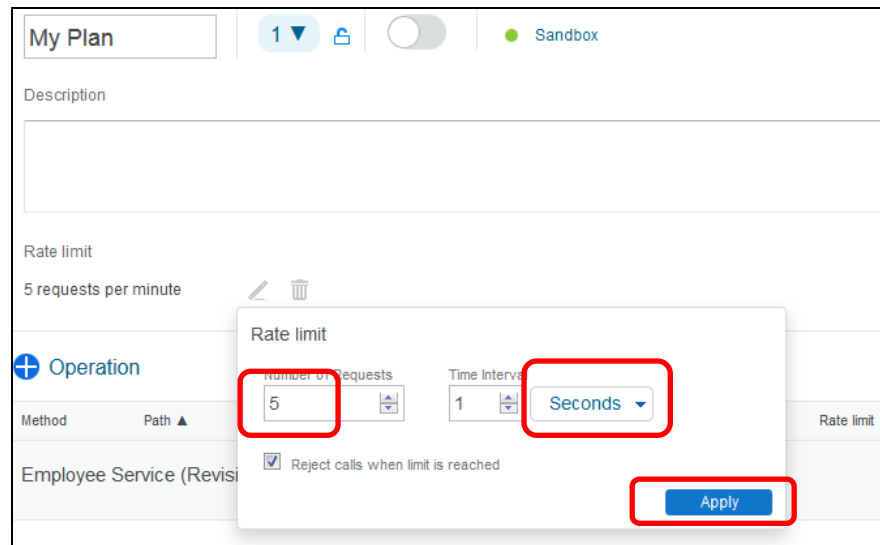
Click the pencil icon to edit the rate limit.



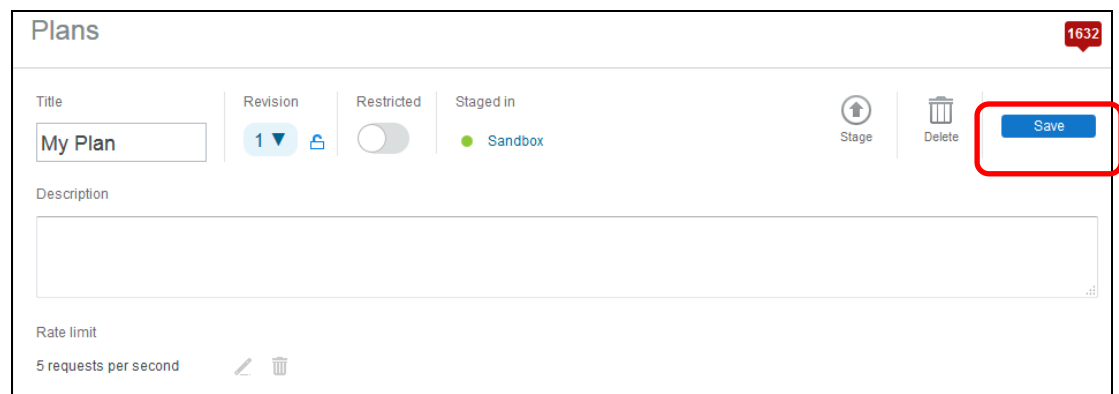
4. Change the rate limit to 10 requests per second.

Ensure the **Reject calls when limit is reached** option is selected.

Click **Apply**.



5. Save the plan.

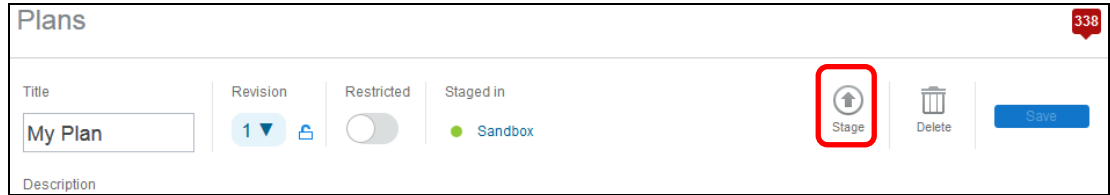


9.1.1 Stage and republish the plan

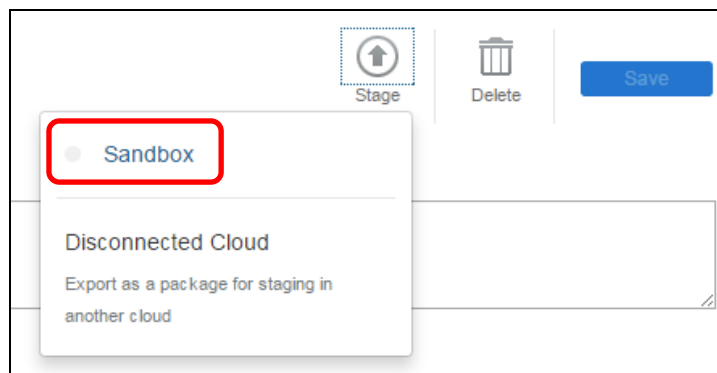
1. Click the Plans icon to return to the page for the plan.

Click "My Plan".

Click on the **Stage** button:

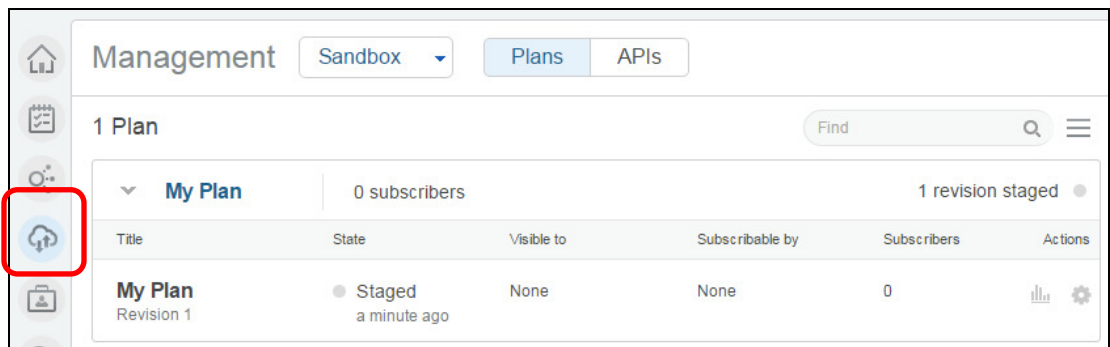


2. Click on the **Sandbox** environment:




3. Once the plan has been staged, it must be published.

Click on the Management button on the left. The Management page will be displayed, and should show the plan in Staged state:





4. Click on the cog icon on the right and then click on **Publish**:

Title	State	Visible to	Subscribable by	Subscribers	Actions
My Plan Revision 1	● Staged a minute ago	None	None	0	 Publish Replace an existing plan Supersede an existing plan Open draft View approval history Remove from environment

5. The **Edit visibility and subscribers** dialogue will appear. Click **Publish**:

Edit visibility and subscribers

Visible to: 



Subscribable by: 

Everyone will be able to see this plan

Everyone signed in to an account will be able to subscribe to this plan

Publish Cancel

6. The plan should now be shown as **Published**:

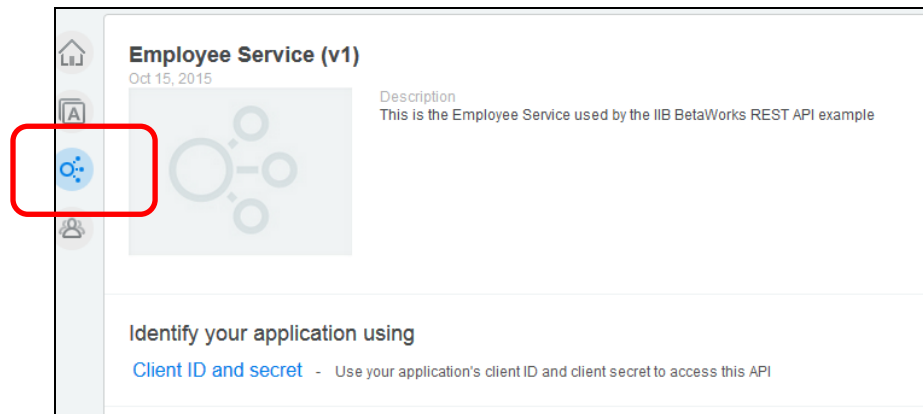
Title	State	Visible to	Subscribable by	Subscribers	Actions
My Plan Revision 1	● Published a few seconds ago	All	Authenticated users	0	 

9.1.2 Publish the REST API again from Developer Portal

By retiring the plan, the REST API needs to be published again from the API Developer Portal. You did this earlier in section 7.1, but this is reproduced here for ease.

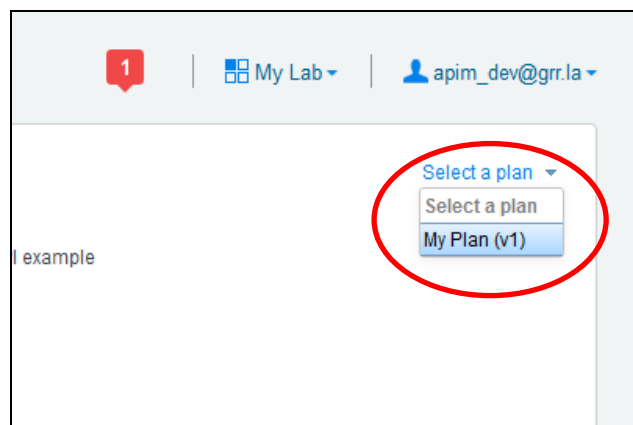
Switch to the APIM Developer Portal tab.

1. Click on the **APIs** button on the left and then click on **Employee Service (v1)** at the bottom of the page. The page for that REST API will be displayed, along with the GET operation:

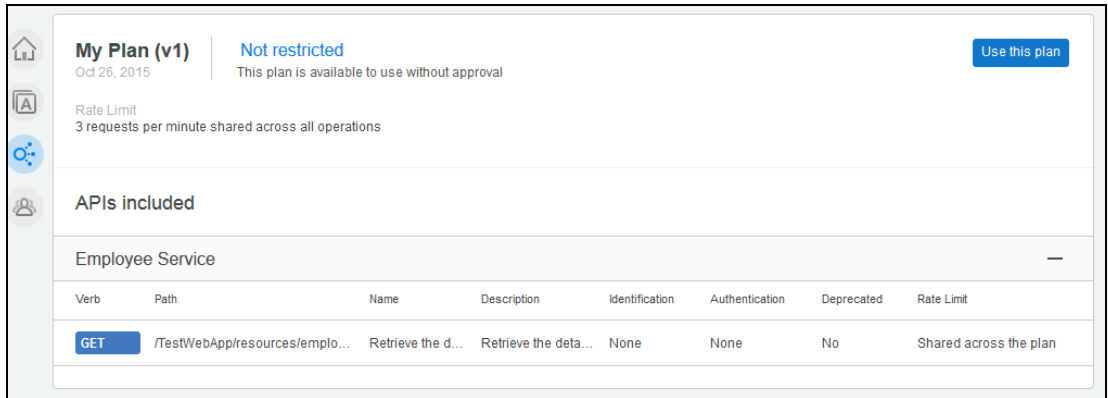


2. In the list of operations at the bottom of the page, you can see which operations are available in which plans. In order to request access to the REST API, click on the **Select a plan** link at the top of the page.

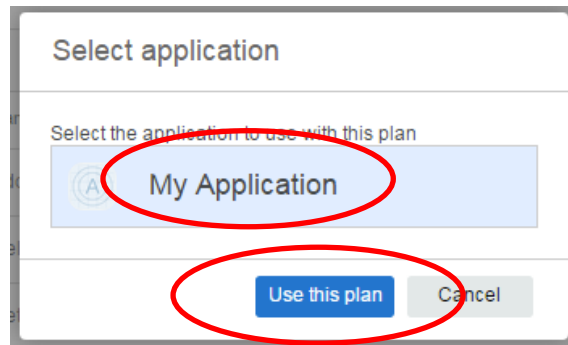
Even though there is only one plan to select, and which has already been selected, this must be selected again.



- The details of the plan then appear:

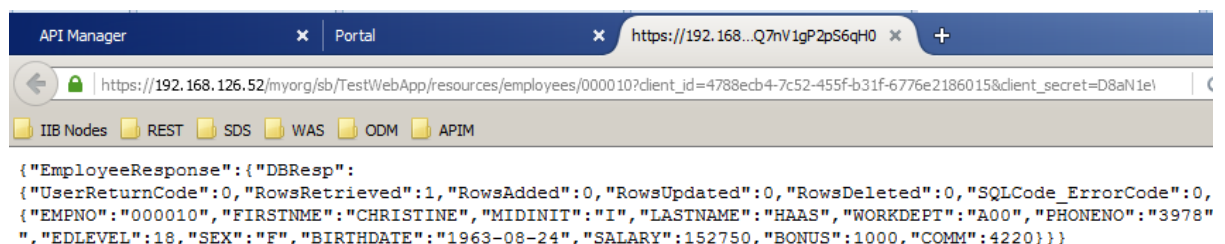


- Click on "Use this plan". The **Select application** dialog then appears. Click on the application you documented earlier, and then click on **Use this plan**.



9.1.3 Test the published URL

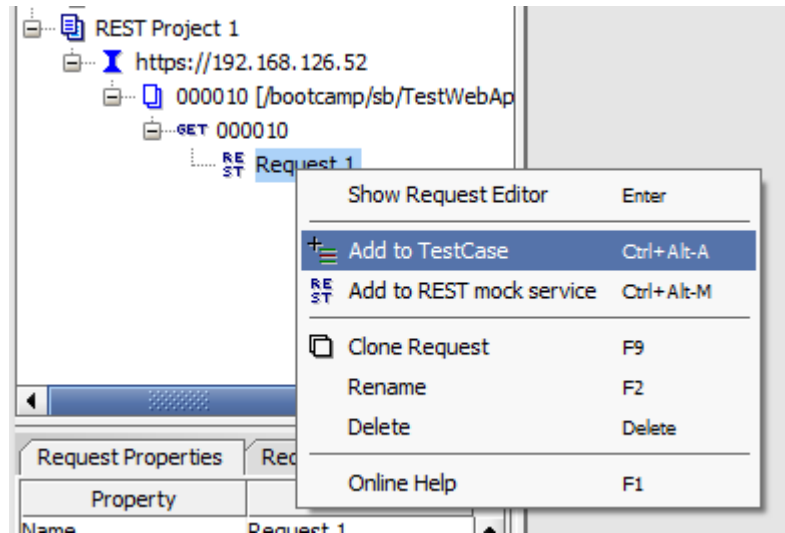
Test the published URL in a browser once more, beyond the original rate limit (5 calls per minute) to show that the limit has been raised.



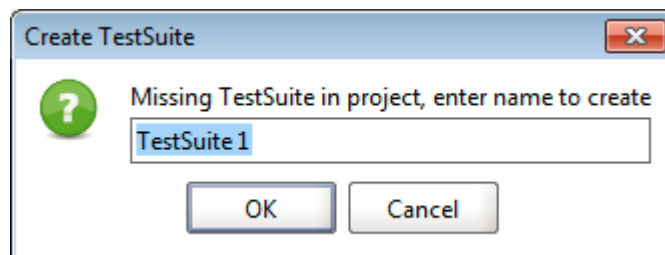
9.2 Create and run load test

The current rate limit (5 calls per minute) in the plan containing the REST API has been replaced with a much higher one appropriate for a load test (10 calls per second). You will now create a LoadTest in SOAPUI to demonstrate this.

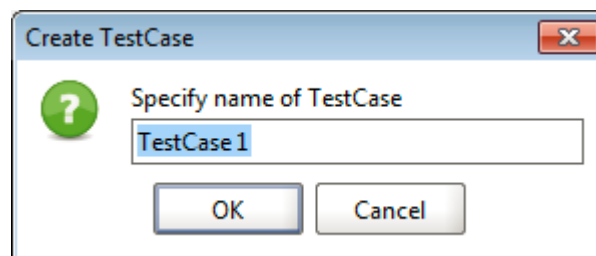
1. Switch back to SoapUI and right click **Request 1** in the project tree, and click on **Add to TestCase**:



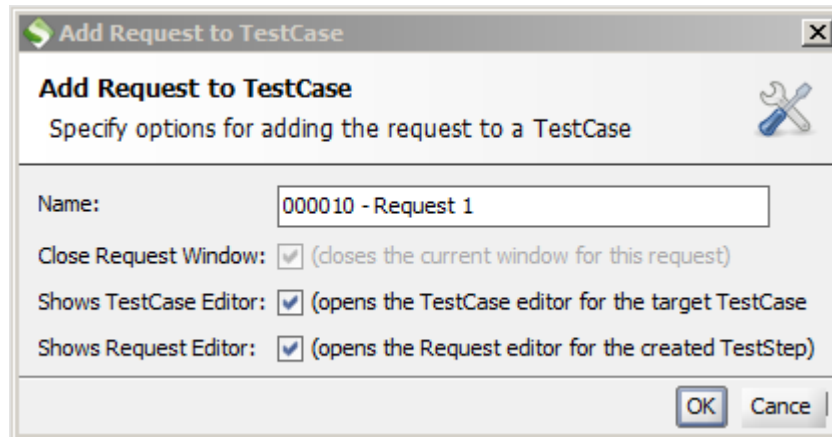
2. The **Create TestSuite** dialogue opens. Click **OK**.



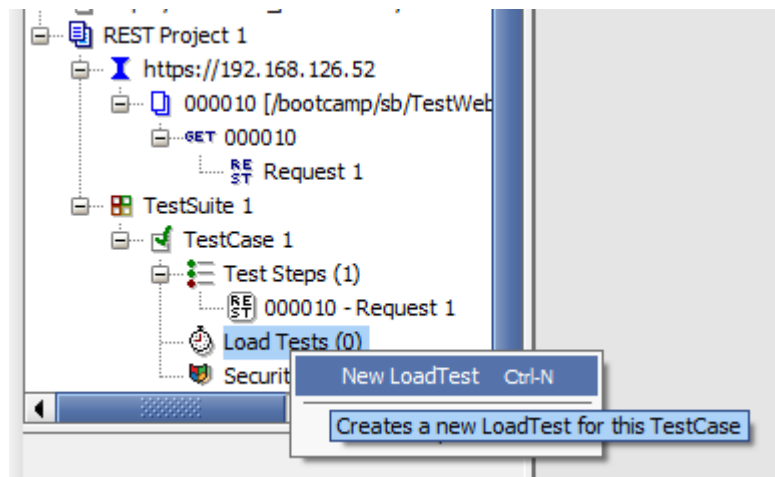
3. The **Create TestCase** dialog opens. Click **OK**.



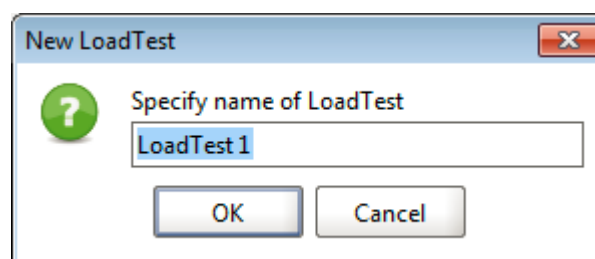
- The **Add Request to TestCase** dialog opens. Click **OK**.



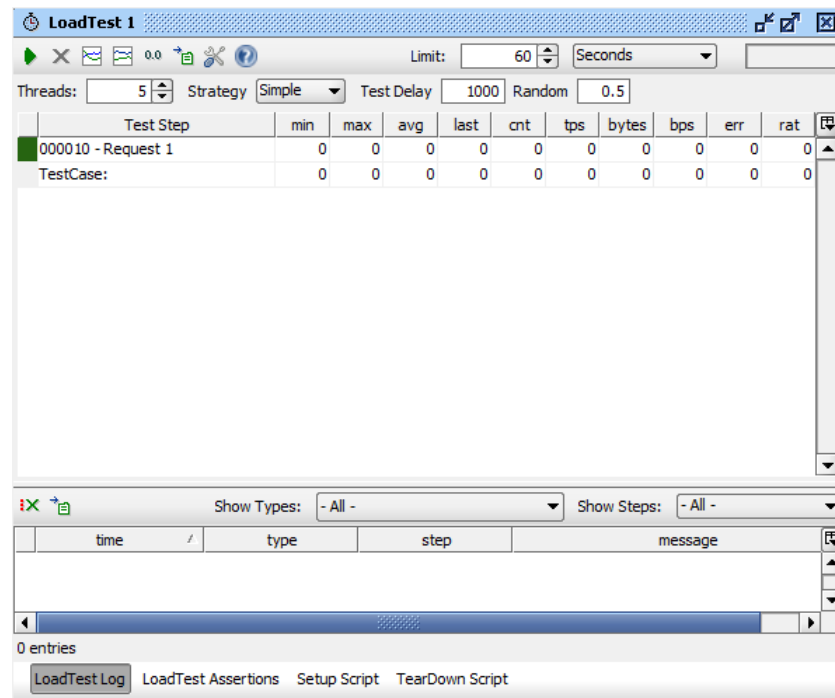
- The new TestSuite and associated artefacts now appear in the project tree.
Right click **Load Tests** in the project tree, and click on **New LoadTest**.



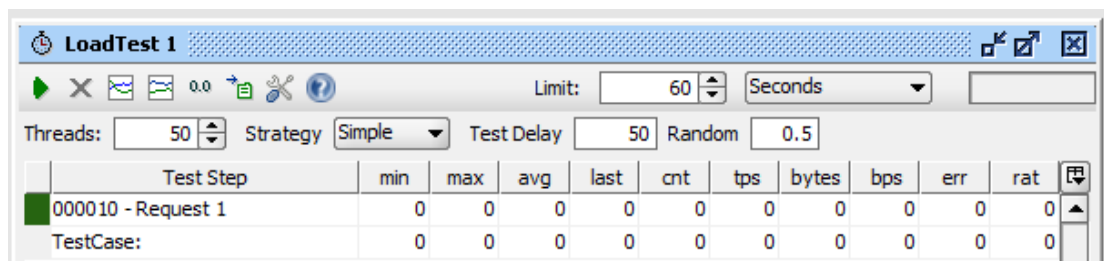
- The New LoadTest dialogue appears. Click **OK**.



- A new load test appears:

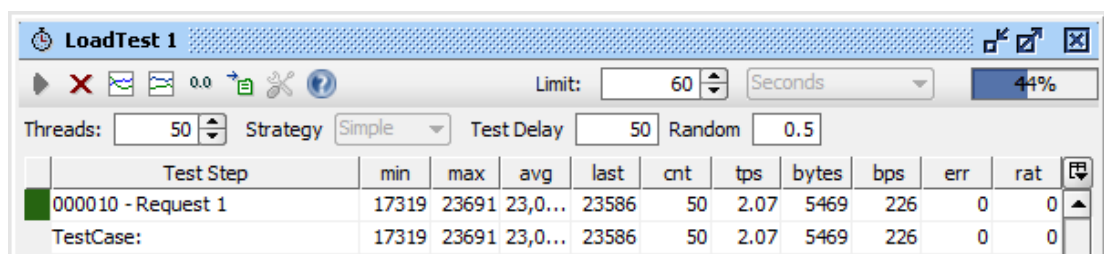


- Change the value of **Threads** to 50, and the value of **Test Delay** to 50 (ms):



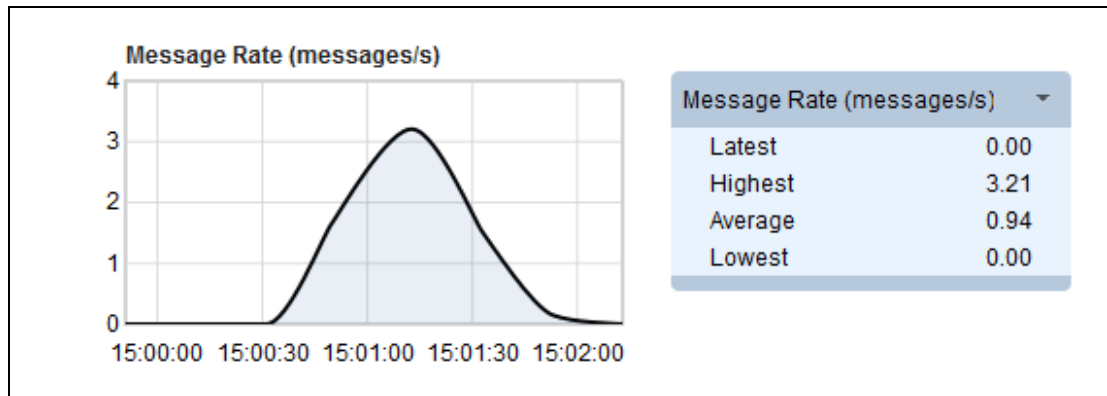
- Click on the play button on the load test. It will run for 60 seconds by default unless stopped using the stop button.

You will see the results of the load test update in SoapUI.



- The statistics view in the web UI will show that the message rate has been limited by the IBM DataPower Gateway, as per the limit set by the API Management plan for the deployed REST API.

Note the rate in IIB may not reach the full limit controlled by APIM, if other factors such as memory and processor provide additional constraints.



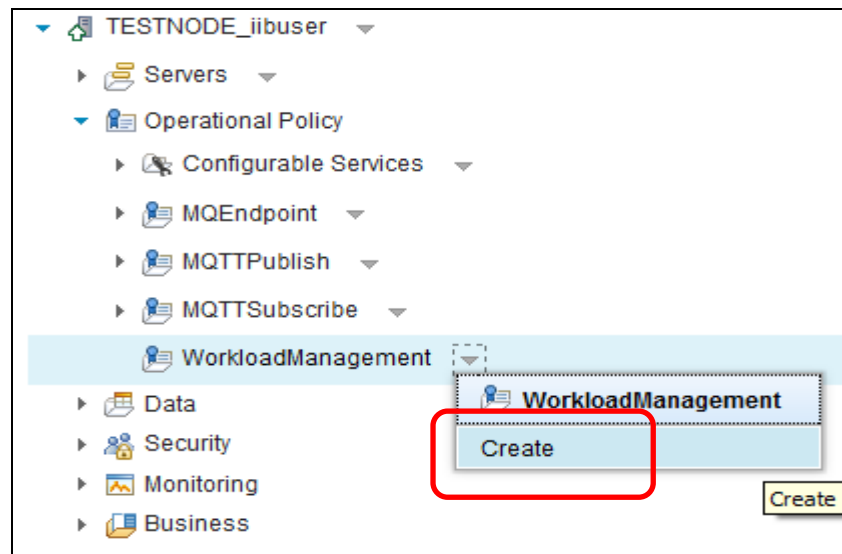
10. Load Test Deployed API using IIB WLM

The throughput in the load test in the last section was throttled by rate limits enforced by the DataPower Gateway, at the edge of the network, at the application level.

To control throughput for the deployed API overall, we will use a separate workload management (WLM) policy within IIB, i.e. at the centre.

1. Open the web user interface for the integration node. Find **WorkloadManagement** in the tree on the left under **TESTNODE_iibuser** -> **Operational Policy**.

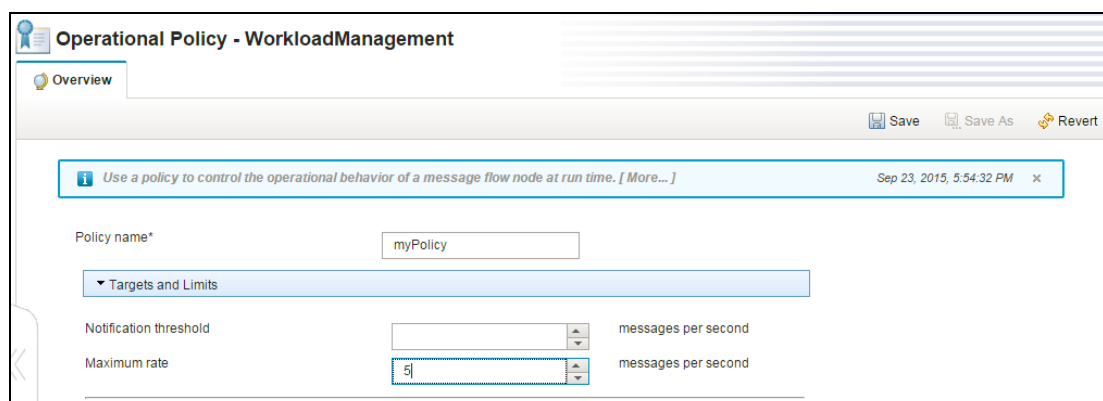
On the drop-down arrow, select Create.



2. A new WorkloadManagement policy is created and displayed.

Give the policy a name (for example, **myPolicy**), and set the Maximum rate to 5 messages per second and click the **Save** button.

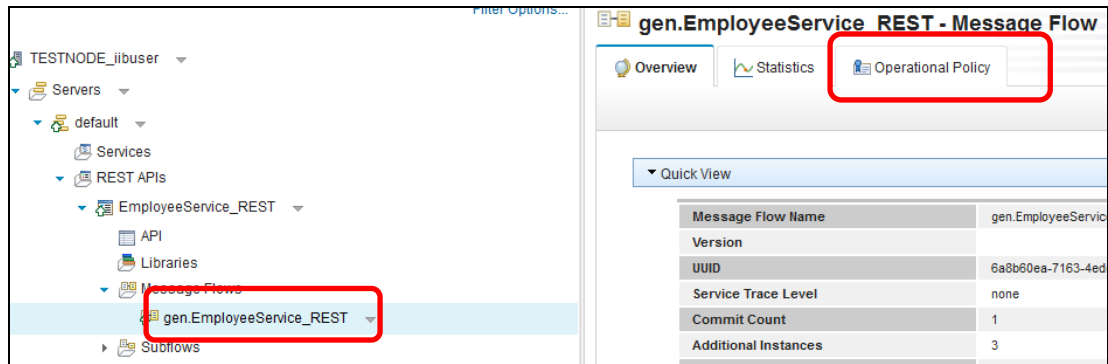
Note - normally, the limit of the backend server, such as IIB, would be higher than the limit of the front-end (APIM). For the purposes of this lab, the IIB limit will be lower than the APIM limit.



The WLM policy must be attached to a message flow in order to dynamically configure that message flow to restrict the rate of requests to the REST API to 5 messages per second.

A WLM policy can be attached to multiple message flows. If the WLM policy is updated whilst attached to message flows, all of those message flows are updated when you save the WLM policy.

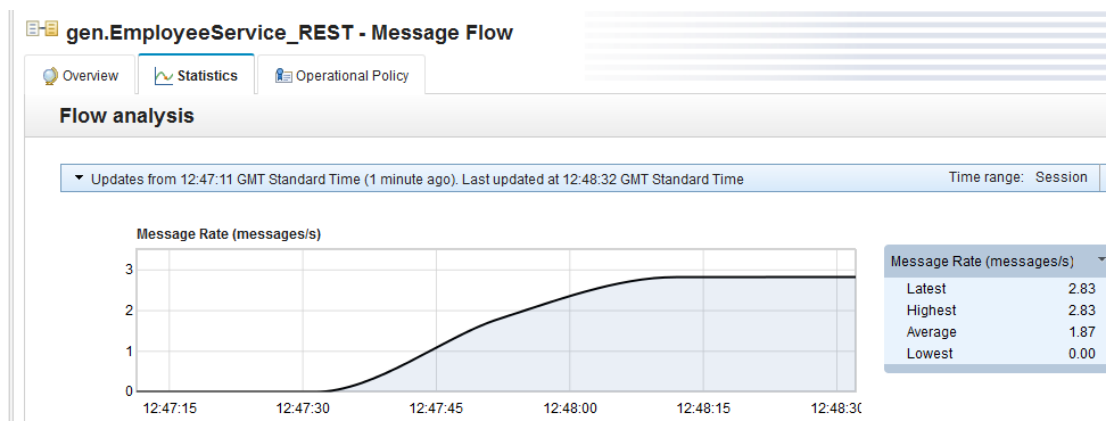
- To apply the WLM policy to the deployed message flow, navigate to message flow **gen.EmployeeService_REST** and click on the Operational Policy tab:



- Find the WLM policy you created, and select the radio button. Once the WLM policy is selected, click on **Apply** to apply the WLM policy to the message flow. The changes take effect immediately.



- Run a new load test, repeating the steps in section 9.2 (Create and run load test).
- The statistics view in the web UI will show that the message rate has been limited as it was before. In this case, though, the throughput has been controlled entirely within IIB by WLM.



11. Appendix – Installation and Configuration of API Management Environment

The following instructions show how to install and configure the API Management environment for use in this lab.

11.1 Preparation

1. The following software is required:
 - IBM API Management V4.0.2 Multilingual for VMWare, Xen and IPAS (CN5IWML). Note: this is the IBM API Management appliance.
 - IBM WebSphere DataPower Service Gateway XG45 Virtual Edition for Non-Production Environment V7.2.0 for VMware, English eAssembly (CRWD9EN)

Note:

- each is a VM with code pre-installed in an OS.
 - we are using the Basic Developer Portal provided with the the IBM API Management appliance and will not be installing the separate (Advanced) IBM API Management Developer software.
2. Each VM will need 4 GB of memory. Check that your system has sufficient installed memory to support these.
 3. The following static IP addresses are used for the BetaWorks workshops:
 - DataPower Gateway: 192.168.126.52
 - API Management Appliance: 192.168.126.100

These are defined on VMware Network Adapter VMnet8 (for NAT). The following shows the relevant output from the **ipconfig** command on the systems used to host the VMs:

```
Ethernet adapter VMware Network Adapter VMnet8:
Connection-specific DNS Suffix . . . : 
Link-local IPv6 Address . . . . . : fe80::f0d8:a24c:405f:af1b%21
IPv4 Address. . . . . : 192.168.126.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
```

If the VMnet8 network adaptor on your system has a different IPv4 address from that shown, then replace the first 3 parts of the static IP addresses to match it.

11.2 Start DataPower Gateway

1. Open the DataPower GA .ova file in VMware Workstation.
2. Select a location for the virtual machine files (ideally in a new folder).
3. Accept the license and wait for the import to finish (this will take several minutes)
4. Change the configuration on each Network Adapter from bridged to NAT. Note you only need to do this for eth0 and eth1, but it's easier to do it for all 4 network adapters in case you want to configure more interfaces in future.
5. Note that DataPower 7.0 sets the defaults for 8GB RAM and 8vCPUs, so reduce these to 4GB RAM and 4vCPUs for a "Small" installation.

6. Power on the virtual machine (it will take a few minutes to boot, but you can continue with the next steps while you wait)

11.3 Start API Management Appliance

1. Open the API Management .ova file in VMware Workstation.
2. Change the configuration on the Network Adapter from bridged to NAT
3. According to the API Management documentation, the minimum supported configuration is 4GB RAM and 1CPU.
4. Power on the virtual machine (it will take a few minutes to boot, but you can continue with the next steps while you wait).

11.4 Configure Gateway Appliance – CLI section

1. Log into the DataPower virtual appliance with username *admin* and password *admin*.
2. Press any key to continue.
3. Enter **n** to enable disaster recovery mode
4. Enter **n** to disable common criteria compatibility mode
5. Enter and confirm your new admin password.
6. Enter **y** to run the installation wizard.
7. Enter **y** to configure network interfaces.
8. Enter **y** to say you have all the information.
9. Enter **y** to configure eth0.
10. Enter **n** to disable DHCP.
11. Enter the eth0 IP address from the Static IP addresses section in CIDR notation, i.e. IP address/routing prefix. (For a subnet mask of 255.255.255, the routing prefix is 24).

In the BetaWorks workshops, the address entered is *192.168.126.52/24*.
12. Enter the IP address for the IPv4 gateway (*192.168.126.2* in the case of the BetaWorks workshops).
13. Press **enter** to skip the IPv6 gateway address.
14. Enter **n** to skip the eth1 configuration.
15. Enter **n** to skip the eth2 configuration.
16. Enter **n** to skip the eth3 configuration.
17. Enter **y** to configure network services.

18. Enter **y** to configure DNS.
19. Enter **y** to say you have all the information.
20. Enter the IP address of the DNS server (same as the IPv4 gateway, e.g. *192.168.126.2*).
21. Enter **n** to skip defining a unique system identifier for this appliance.
22. Enter **y** to configure remote management access.
23. Enter **y** to say you have all the information.
24. Enter **y** to enable ssh.
25. Press **enter** to accept the default IP address (all IP's).
26. Press **enter** to accept the default port (*22*).
27. Enter **y** to enable the Web UI.
28. Press **enter** to accept the default IP address (all IP's).
29. Press **enter** to accept the default port (*9090*).
30. Enter **n** to skip configuring a user account that reset passwords.
31. Enter **n** to skip configuring a hard disk array.
32. Enter **n** to skip reviewing the current configuration.
33. Enter "y" to save the current configuration.
34. Enter "y" to overwrite the previous configuration.

Important: Do not log out of the console until you have logged in to the Web UI and accepted the license (detailed in the next section). Otherwise, you have to work through the wizard again.

Note: to check the IP addresses you configured earlier, run the command *show int*.

11.5 Configure Gateway Appliance - accept gateway licence

Note: This may not work using the Chrome browser.

1. Navigate to the following URL in a browser: `https://<eth0 ip address of DataPower Gateway>:9090` (e.g. `https://192.168.126.52:9090`).
2. Proceed through any security warnings about the self-signed certificate.
3. Log in with username *admin*, and use the new password you specified and the default domain.
4. Click **I agree** to accept the license.

The appliance reloads. The next time you log into the console, the wizard is not displayed.

11.6 Configure Gateway Appliance - NTP & Time Zone

It is necessary to configure NTP on every server to ensure the timestamps match and to avoid issues. In the BetaWorks workshops, we use "81.168.77.149". You will need to find one that is local to you. It is also recommended to set every appliance to the same timezone to make it easier to compare logs. We have used UTC which is the default for the management server virtual appliance.

1. Log back into the DataPower Gateway Web UI with username *admin*, and the new password you specified and the default domain.
2. Select **Network > Interface > NTP Service** from the menu on the left
3. Set **Administrative State** to *enabled*.
4. Enter **NTP Server** details (e.g. *81.168.77.149*) and click **Add**.
5. Click **Apply**.
6. Check that the object status changes to **up** at the top of the page.
7. Select **Administration > Device > Time Settings** and select *UTC*.
8. Click **Apply**.
9. Select **Status > Main > Date and Time** and verify the correct time and zone is displayed.
10. Click the **Save Configuration** link at the top right.

11.7 Configure Gateway Appliance - enable XML management interface port

The XML Management Interface port must be enabled to allow IBM API Management to configure the gateway server.

1. Select **Network > Management > XML Management Interface**
2. Set **Administrative State** to *enabled*.
3. Set **Local Address** to the eth0 management IP address (e.g. *192.168.126.52*).
4. Keep the default port (*5550*) and click the Apply button and the object status should change to [up] at the top of the page.
5. Click the **Save Configuration** link at the top right.

11.8 Configure Gateway Appliance - enable statistics

The Statistics Service must be enabled in the Gateway Server to allow the Cloud Management Console to display resource utilization information.

1. Select **Administration > Device > Statistic Settings**
2. Set **Administrative State** to *enabled*.
3. Click the **Apply** button and the object status should change to **up** at the top of the page.
4. Click the **Save Configuration** link at the top right.

11.9 Configure API Management Appliance

1. Once the appliance is successfully started, you will get a login prompt. The first time you power up the management server, it might reboot itself automatically. Once it comes up again, you can log in.
2. Login with username *admin* and password *!n0r1t5@C* (on a UK keyboard in VMware Workstation the @ symbol will be where the “ symbol is displayed).
3. Enter the following commands to configure the networking and NTP. Adjust the addresses as appropriate:
 - *net set eth0 address 192.168.126.100 mask 255.255.255.0*
 - *net set gateway static 192.168.126.2 eth0*
 - *net set nameserver static 192.168.126.2*
 - *net set ntp static 81.168.77.149* (see earlier section on configuring NTP).
 - *net set search none*
 - *net restart*
 - *net show all* (if the old details are still displayed, wait a little longer for the networking to restart fully and repeat this command until the correct details display)

11.10 Configure API Management Cloud

At this point both appliances should be started.

1. Log into the Cloud Management Console (e.g. <https://192.168.126.100/cmc/>).
Note: Sometimes It takes roughly 3-5 minutes for the cmc to come up after all of the system processes come up on the management server. If the cmc page comes up blank, wait a few minutes and reload the page.
2. When the login screen pops up, log in with the default admin login & password:
(*admin/ !n0r1t5@C*)
3. If the license is displayed, click **Accept All Licenses, Terms and Notices**.
4. You will be required to change the admin password on logging in for the first time. Be sure to write it down.
Note: you should enter the old password in the first box, the new password in the next two boxes, and your email address in the last one.
5. Check the Management Cluster displays the correct IP address on the **Home** page. If the correct IP address is not displayed the system was not configured correctly during the initial boot.

If this is the case run the following commands from the CLI & then go back to step 1 of this section:

```
system clean apiconfig, system restart
```

Note you must type *yes* not *y* to confirm the system clean apiconfig command and afterwards the admin password will have been reset back to the default *!n0r1t5@C*.

6. You will need to set up a connection to an existing email server. Click on the Settings button and then fill in the information in the setup email box at the bottom of the page. The email server is used to send emails, for example, when a new organization account is requested. Example gmail settings are provided in brackets.
 - **Hostname:** (e.g. *smtp.gmail.com*)
 - **Port:** (e.g. *465*)
 - **Username:** If your email server requires you to authenticate, enter the administrative user name for the SMTP server. (e.g. your gmail email address)
 - **Password:** If your email server requires you to authenticate, enter the administrative password for the SMTP server (e.g. your gmail password)
 - **Sender Address:** (e.g. your gmail address)
 - **Sender Descriptive Name:** (e.g. *My Sandbox Support*)
 - Click **Save**
7. Define your Gateway Cluster Hostname
 - From the side menu click on **Home**.
 - Click the **Gateway cluster settings** link below the All Management Servers graph, and you will be redirected to the Clusters page with the Gateway Cluster settings opened.
 - Enter in the **Datapower eth0** IP address or hostname in the Address field (e.g. *192.168.126.52*).
 - Since this is a demo system on your laptop, load balancing can be left disabled and we will keep the default ports and SSL certificate.
 - Click **Save**.
8. Add the Gateway server to the Cluster
 - Click on the **+Server** button in the Gateway Clusters section.
 - Enter in the information for the gateway server. Use the details for the XML Management Interface (e.g. **Address** *192.168.126.52*, **Port** *5550*, DataPower admin username and password). The Network Interface field should be *eth0*. The Name field is a free form text that will be visible in the Manage Servers Screen.
 - Click **Add** when done.

It takes a few minutes to add the server to the cluster. E.g. it needs to create the domain and the requisite DataPower assets. When it's done, you'll see the gateway server icon turn green indicating that the process is complete.

9. Create your first Provider Organization
 - Click on the **Organizations** button on the menu on the left hand side of the CMC.
 - Click on the **+ Organization** button. The Provider Organization typically represents a department or project, having its own API Manager and Developer Portal although users can be members of multiple organizations.
 - The organization is called *My Organization* in the lab guide, so use this name.
 - Click the **Select** link under **Owner**, and the **New User** tab to add a new user for the owner of the organization using your email address.
 - Once you've entered all the details, click **Add**.
10. Click the link in your email to activate your user account.

Note: if you are having trouble getting the validation email, you can extract it from the logs that are generated from the CMC:

- go to the CMC, and then to the management node and click on **download logs**.
- open the tar file and navigate to and open up the `/var/log/cmc.out` file.
- search on "email to" then pull out the body of the validation mail that was sent and validate your user from there.

e.g. email to: `somemail@gmail.com`, URL:

`https://10.91.25.19/cmc/?validate=true&authId=cmc%2F5527cc73e4b0b55fe4711add%2FI3xA3rT4oE2tW8jR0nM8tV0pl6mM7IW3tX2xU2tS0e&token=m5QfcGr3KHZacaZoC3TcnqffMGsNqJYefjHINu5Tmf&username=someemail%40gmail.com`

11. Enter your user information and click **Sign Up**.
12. You will be automatically redirected to your organizations's API Manager, e.g. <https://192.168.126.100/apimanager/>.
13. Your user name and organization will be displayed at the top with a dropdown to switch between orgs if you have access to more than one.

Setup of the management node is now complete.

END OF LAB GUIDE