



TGH

Making Integrations Simpler

boomi
Partner



Developer Portal

Author

Sowjanya Gurrala



Contents

Developer Portal.....	2
What is Developer Portal?	2
What are the Benefits of Using the Developer Portal?	2
1.Engagement:	2
2.Self-Service:	2
3.Control:	3
Preconfiguration before creating a developer portal:	3
How to configure basic authentication source:	4
How to Configure Developer portal in Boomi.....	10
References:.....	26

Developer Portal

What is Developer Portal?

- The API Developer Portal is where developers explore and subscribe to published APIs, even if they aren't Boomi platform users.
- As organizations look to extend the reach of their businesses, they require a mechanism to interact with a broader population of users.
- The Developer Portal provides a means of engagement with developers who may be internal or external to your organization.
- The hosting of a Developer Portal is on an API Gateway. There is a 1-1 correlation of the Developer Portal to API Gateway.
- The URL used for interaction with the Developer Portal is configured on the API Gateway. By default, the Developer Portal uses **port 18077**.
- Users must be authenticated in order to access the Developer Portal.
- Developer Portal users often do not have Atmosphere accounts, so they are authenticated using an authentication source defined in the Developer Portal Settings tab of the Gateway.
- Users signed in to the Developer Portal are able to register their applications, review available services, and request access to specific APIs in order to use them as part of their application.

What are the Benefits of Using the Developer Portal?

Using the Developer Portal allows users to access published APIs and has a number of benefits.

1.Engagement:

Your developer community can browse the API Catalog to:

- Find available APIs
- Subscribe to available APIs
- Use an embedded swagger UI to explore and test API.

2.Self-Service:

- The developer portal allows developers to register their applications and send subscription requests
- After their requests are approved and configured from within Atmosphere developers can retrieve their Api keys for subscribed APIs from the portal and can generate a new key if necessary.

3.Control:

- The authentication source you define controls access to the developer portal.
- Only those APIs published to an environment that is attached to gateway will be available in the API Catalog.

Preconfiguration before creating a developer portal:

1.Install the Gateway in your machine

2.Attach an environment to the gateway. Deploy some APIs.

(Here I'm deploying only two APIs Employee API & Token API

- Employee API is an Api having one endpoint. It is used to retrieve employee data from database based on Uri parameter (empid)
- Token API is used to generate an access token
Request profile-JSON {"ClientID": "value", "client secret": "value"}
Response Profile-JSON {"Access Token": "Value"}

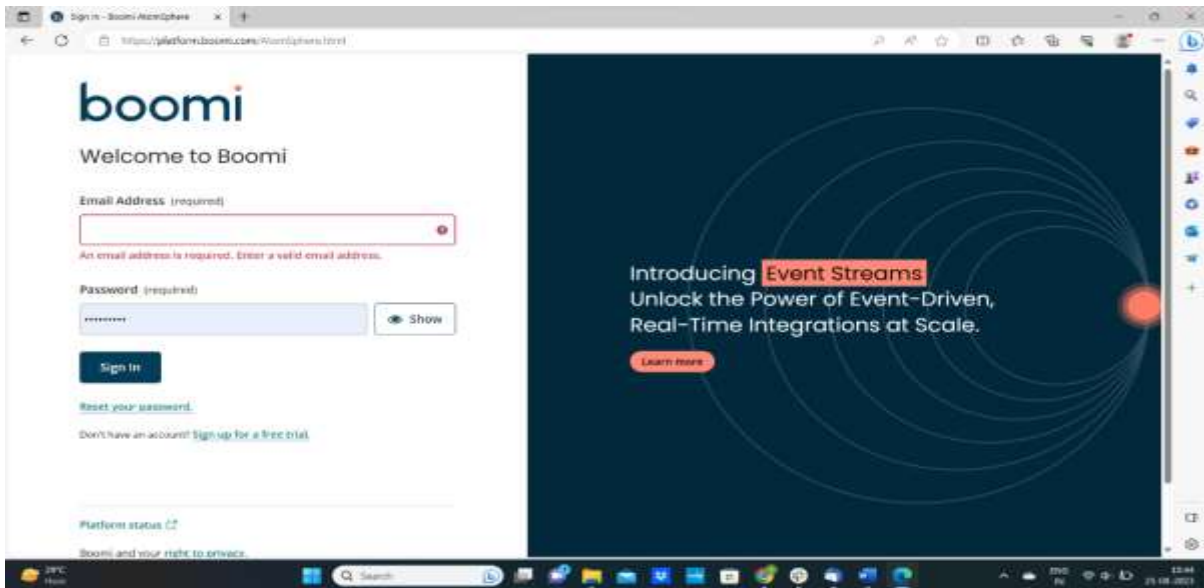
Both the Api's are authenticated using Basic authentication source and Api

Key.

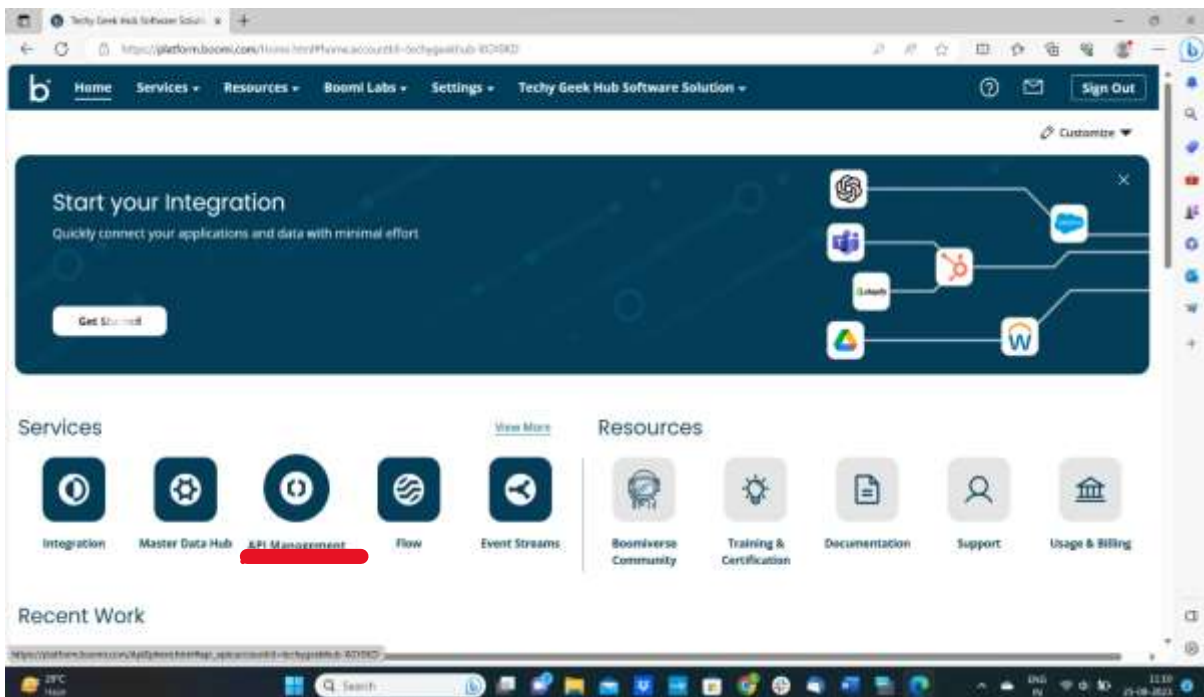
3.Create a basic authentication source (later we can use this same authentication source to authenticate both the APIs & developer portal)

How to configure basic authentication source:

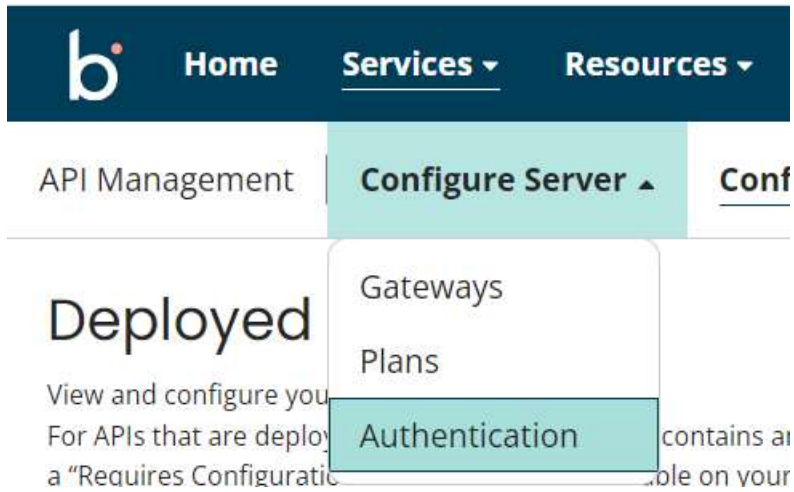
S1: Log onto the Boomi platform (<https://platform.boomi.com/>) with the required credentials (Email Address and Password).



S2: Go to API Management

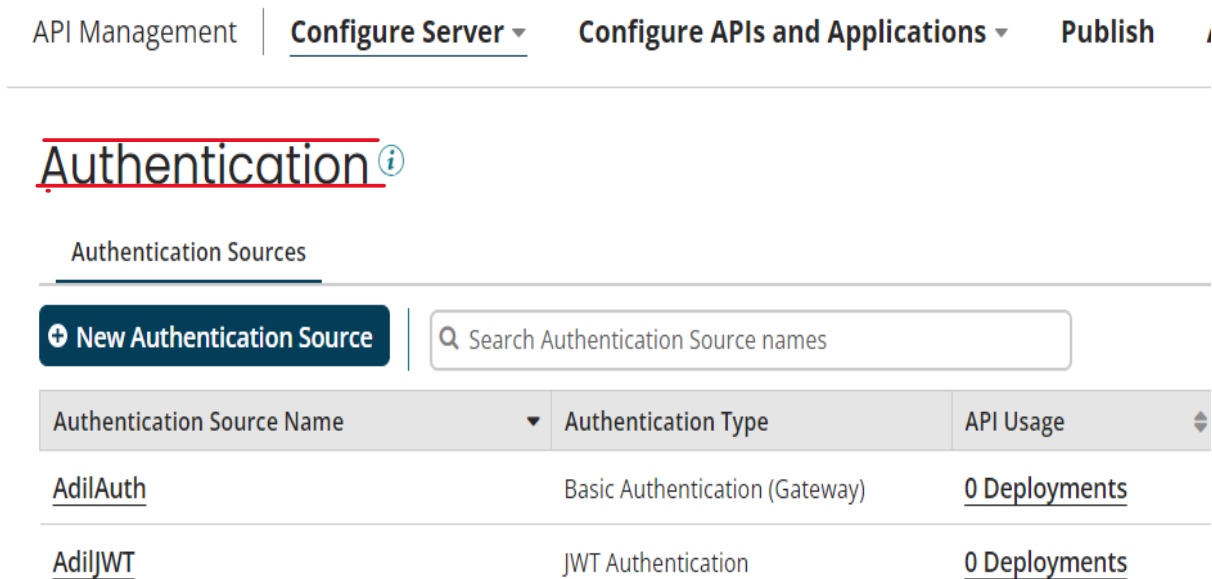


S3: Click on configure server → Authentication



The screenshot shows a navigation bar with 'Home', 'Services', and 'Resources'. Below it, 'API Management' is selected, and the 'Configure Server' dropdown menu is open, showing 'Gateways', 'Plans', and 'Authentication' (highlighted). The background shows a 'Deployed' section with text about configuring APIs.

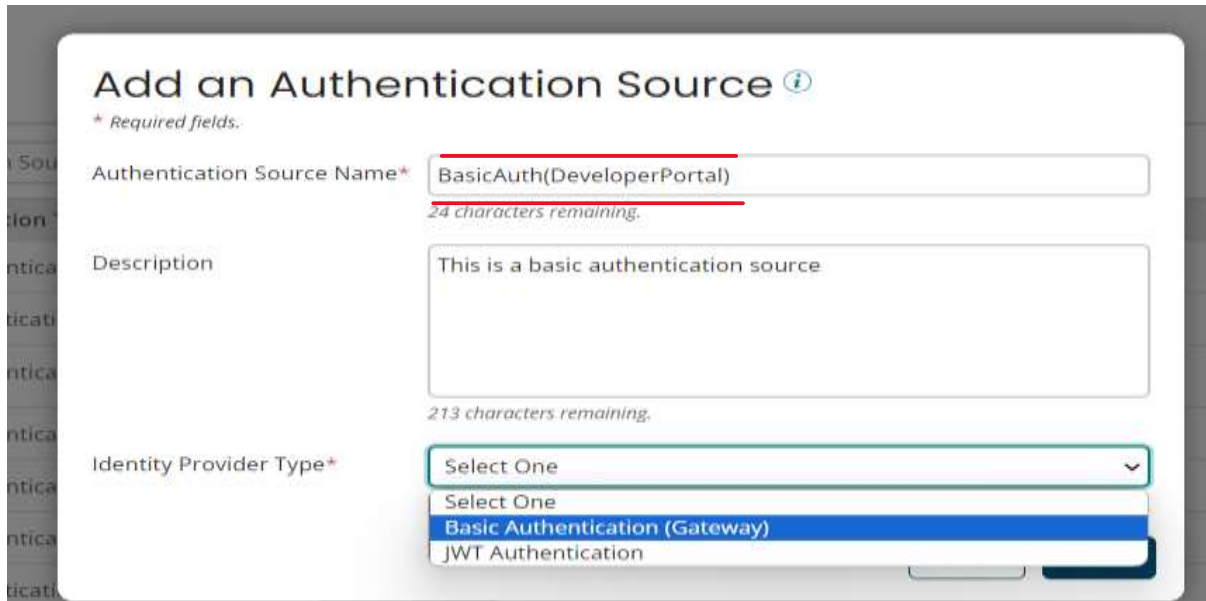
S4: click on new authentication source



The screenshot shows the 'Authentication Sources' page. It has a navigation bar with 'API Management', 'Configure Server', 'Configure APIs and Applications', and 'Publish'. The main heading is 'Authentication' with an info icon. Below it is a sub-heading 'Authentication Sources' and a '+ New Authentication Source' button. A search bar is present with the text 'Search Authentication Source names'. A table lists the existing authentication sources:

Authentication Source Name	Authentication Type	API Usage
AdilAuth	Basic Authentication (Gateway)	0 Deployments
AdilJWT	JWT Authentication	0 Deployments

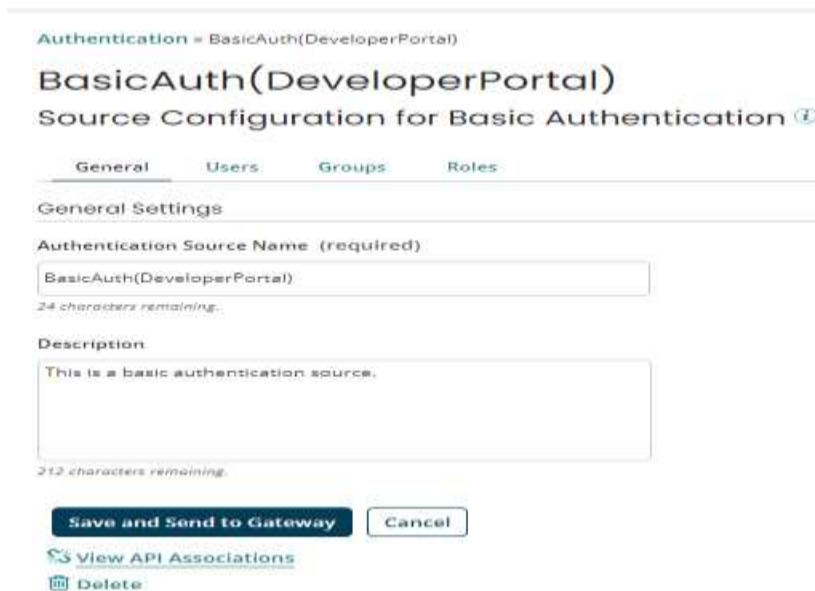
S5: Configure authentication source name & select Identity provider type as Basic authentication (Gateway). Click on ok



The screenshot shows a web form titled "Add an Authentication Source" with an information icon. Below the title is a note: "* Required fields." The form contains three main sections: 1. "Authentication Source Name*" with a text input field containing "BasicAuth(DeveloperPortal)" and a red underline. Below the field is the text "24 characters remaining." 2. "Description" with a text area containing "This is a basic authentication source" and "213 characters remaining." 3. "Identity Provider Type*" with a dropdown menu. The dropdown is open, showing four options: "Select One", "Select One", "Basic Authentication (Gateway)" (highlighted in blue), and "JWT Authentication".

S6: Now we have to configure users, groups, roles.

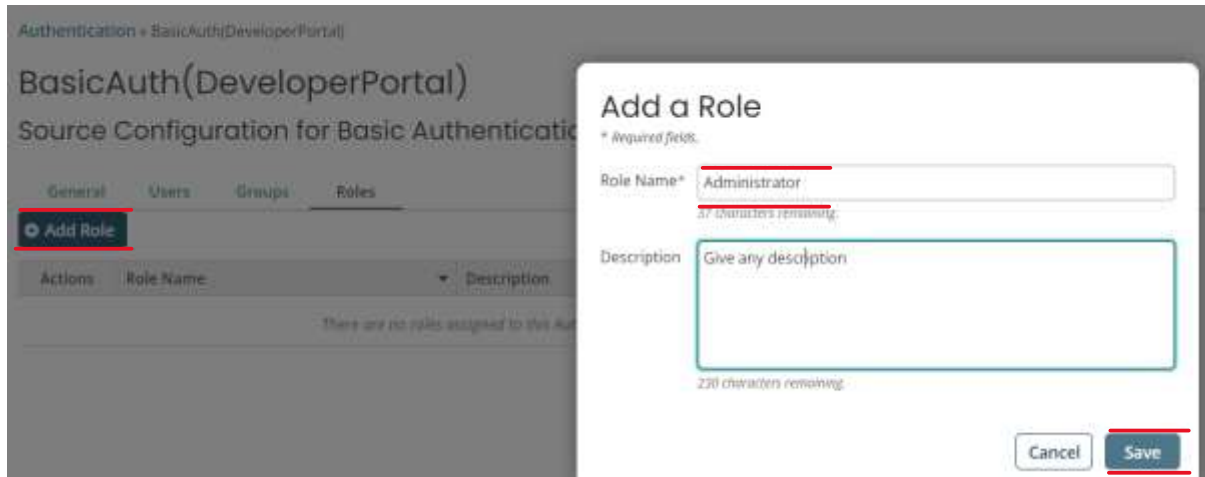
- Roles are the group of users who serve a specific function (ex: Administrator, General)
- Groups are used to organize the users
- Users are the actual entities or people who will make requests to the Api



The screenshot shows a configuration page for "BasicAuth(DeveloperPortal)". At the top, it says "Authentication = BasicAuth(DeveloperPortal)". The main heading is "BasicAuth(DeveloperPortal) Source Configuration for Basic Authentication" with an information icon. Below the heading are four tabs: "General", "Users", "Groups", and "Roles". The "General" tab is selected. Under "General Settings", there are two text input fields: "Authentication Source Name (required)" containing "BasicAuth(DeveloperPortal)" with "24 characters remaining." below it, and "Description" containing "This is a basic authentication source." with "213 characters remaining." below it. At the bottom, there are two buttons: "Save and Send to Gateway" (dark blue) and "Cancel" (white with blue border). Below the buttons are two links: "View API Associations" (with a magnifying glass icon) and "Delete" (with a trash icon).

S7: To configure roles, go to Roles tab → click on Add Role → configure role name as Administrator then click on save.

Repeat the same to configure one more role as General

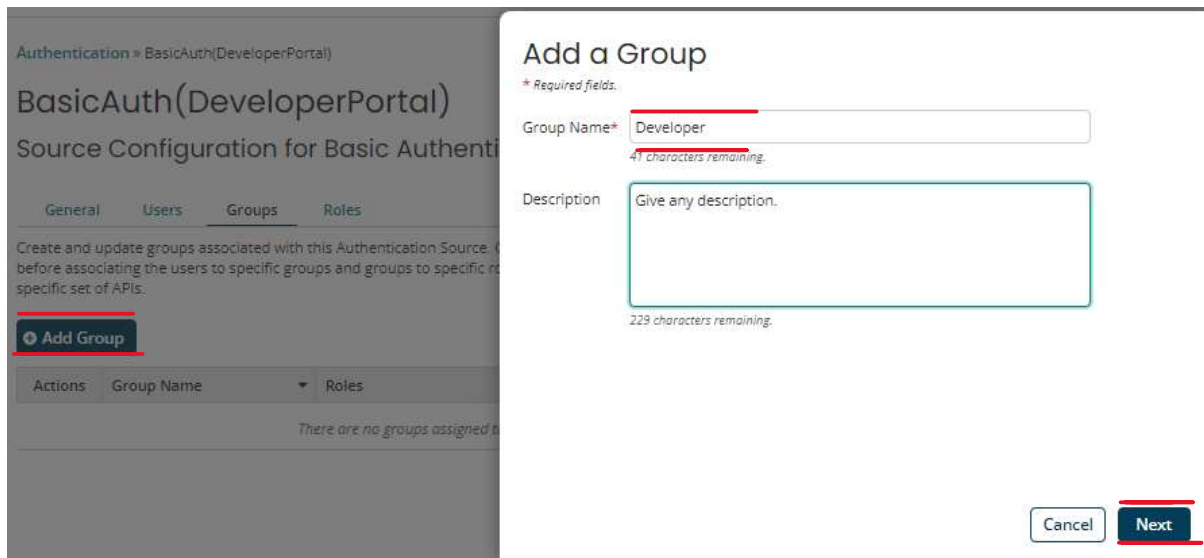


S8: The changes will look as shown below

General			Users			Groups			Roles		
+ Add Role											
Actions	Role Name		Description								
	Administrator		Give any description								
	General		Give any description								

S9: Now configure Groups. Go to Groups tab → click on Add Group →

Configure Group name as Developer → next



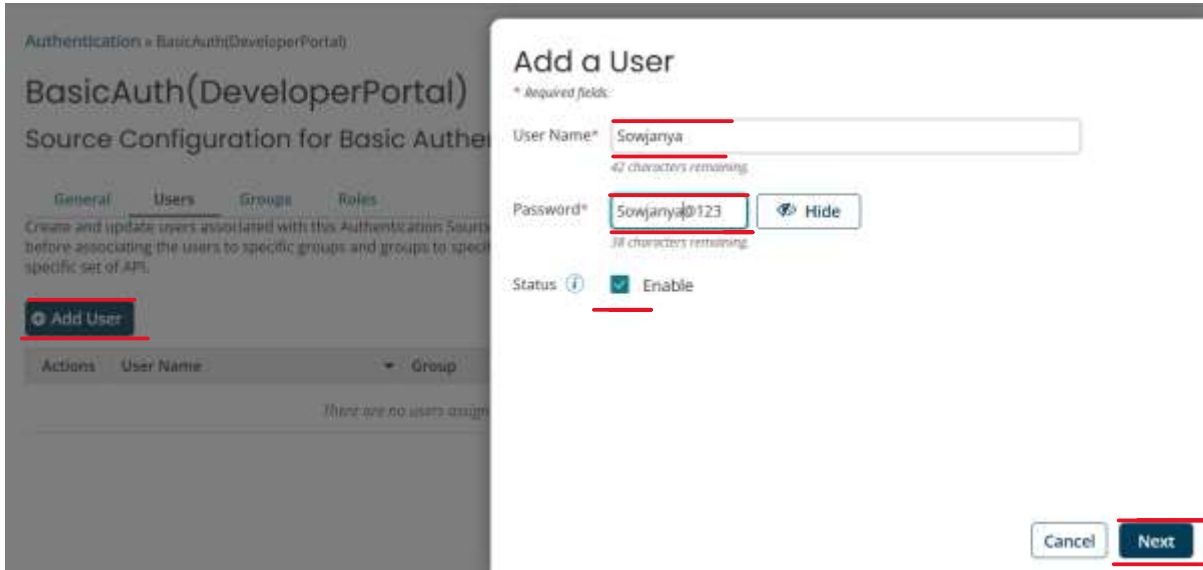
The screenshot shows the 'Add a Group' form in the authentication configuration interface. The form is titled 'Add a Group' and has a red underline. It contains two main input fields: 'Group Name*' and 'Description'. The 'Group Name*' field contains the text 'Developer' and has a red underline. Below it, it says '41 characters remaining'. The 'Description' field is empty and has a red underline. Below it, it says '229 characters remaining'. At the bottom right of the form, there are two buttons: 'Cancel' and 'Next'. The 'Next' button has a red underline.

Now check the checkbox and then click on next → finish



The screenshot shows the 'Select Roles' form in the authentication configuration interface. The form is titled 'Select Roles' and has a red underline. It contains a search bar with the text 'Search for a role'. Below the search bar, there are two roles listed: 'Administrator' and 'General'. Both roles have a checked checkbox. At the bottom right of the form, there are three buttons: 'Cancel', 'Back', and 'Next'. The 'Next' button has a red underline.

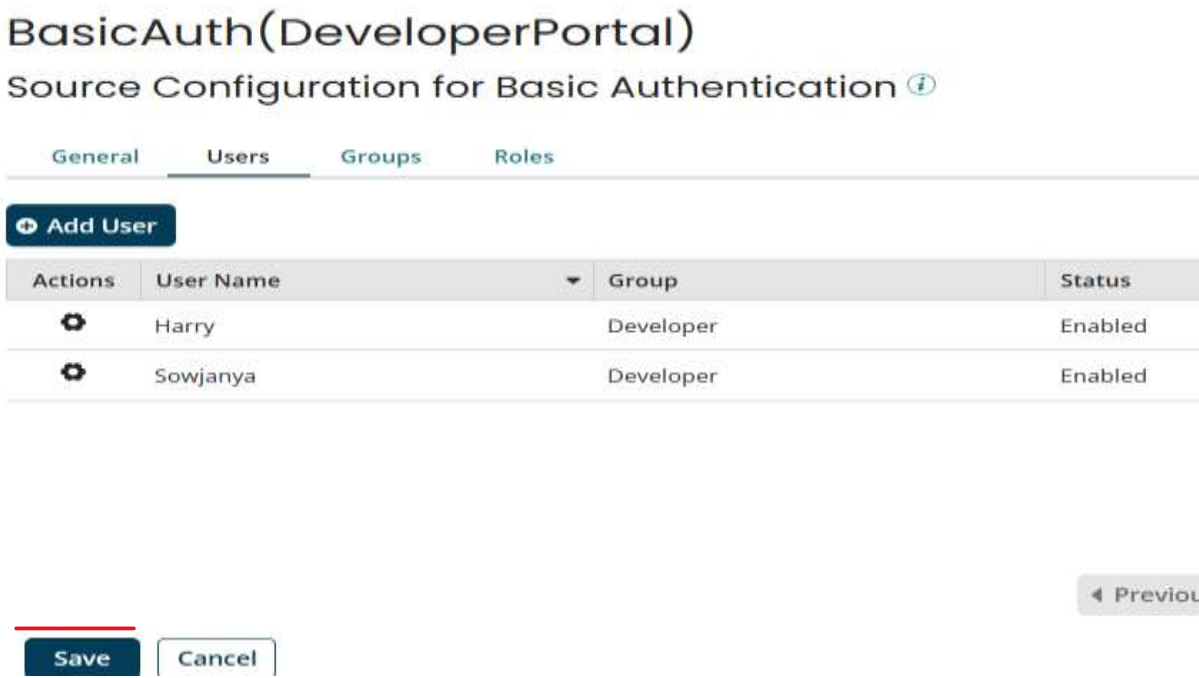
S10: Now configure Users. Go to Users tab. Click on Add user. Configure the fields and click on next



Check the check box and click on next and then finish.

Repeat the same to add another user with **username as Harry and password Harry@123**.

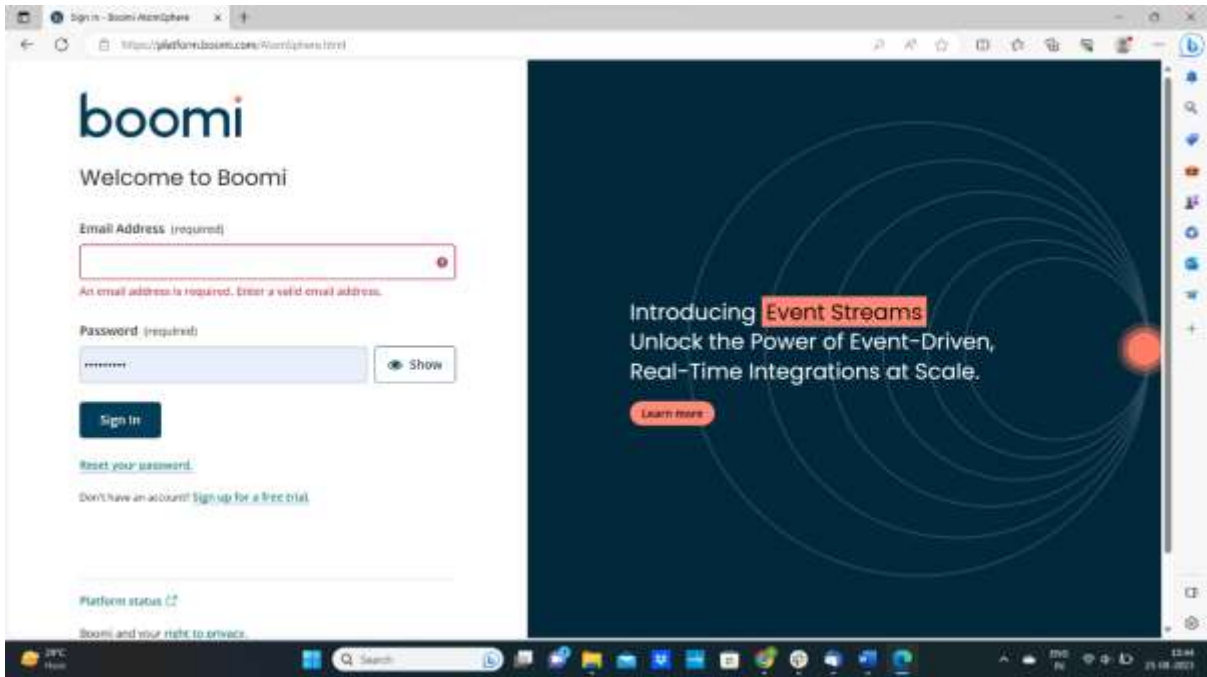
S11: Now the complete authentication source will look as shown below. Click on save .



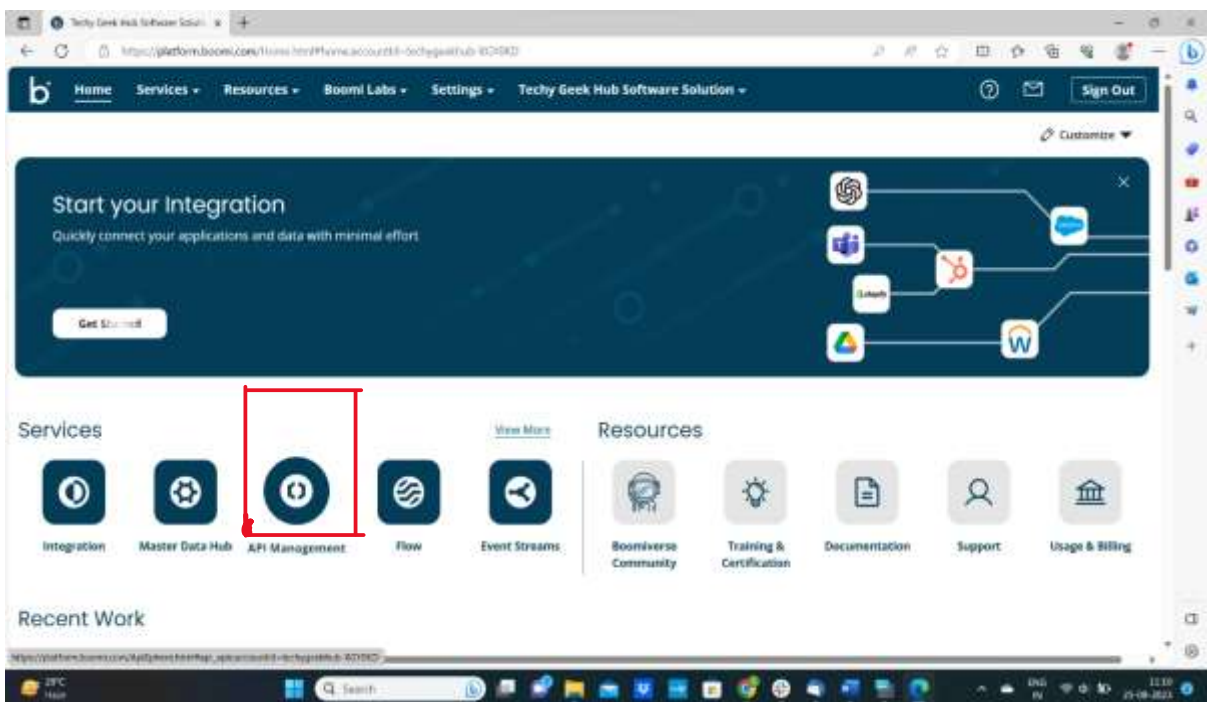
Actions	User Name	Group	Status
	Harry	Developer	Enabled
	Sowjanya	Developer	Enabled

How to Configure Developer portal in Boomi

Step 1: Log onto the Boomi platform (<https://platform.boomi.com/>) with the required credentials (Email Address and Password).



Step 2: Go to API Management

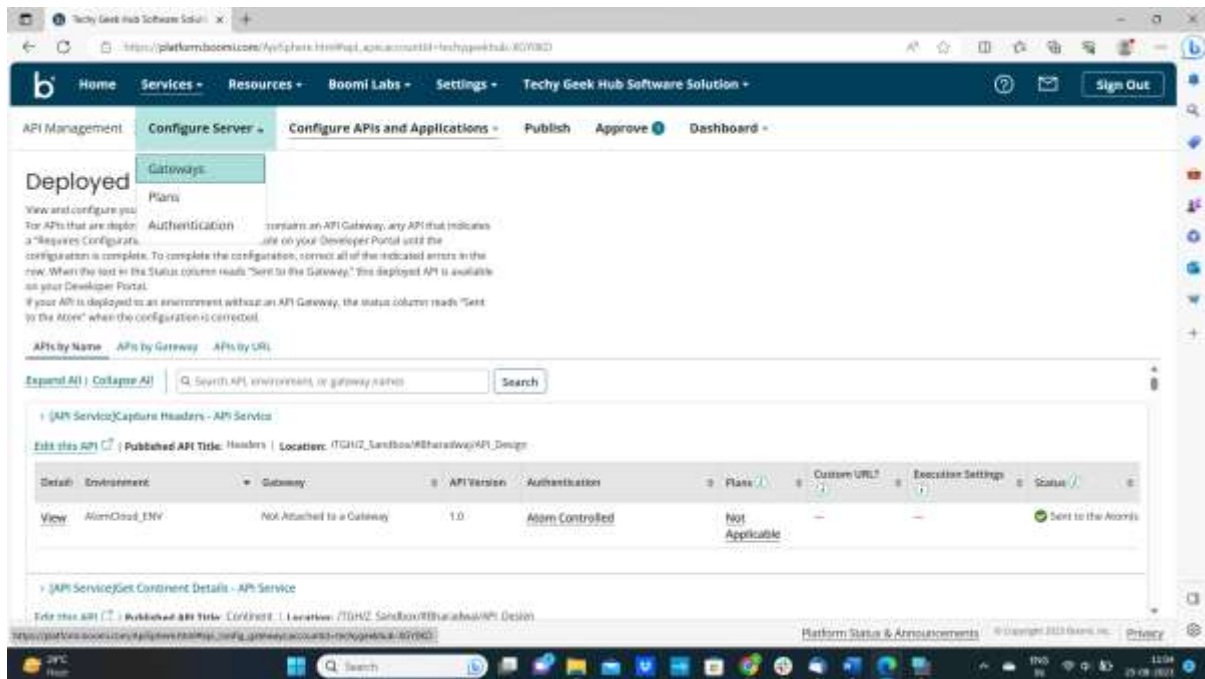


©TGH Software Solutions Pvt. Ltd.

No part of this document may be copied, reproduced, republished, uploaded, posted, publicly displayed, encoded, translated, transmitted or distributed in any way to any other computer, server, website or other medium for publication or distribution, without TGH's prior written consent



Step 3: Go to Configure Server → gateways



Step 4: Search for your gateway and click on the hyperlink



Step 5: Go to Developer Portal settings

Do the following configurations

(i) Enable the portal status

(ii) configure the public URL as <http://localhost:18077>

(iii) Enable Http security headers

(iv) Specify the appropriate **Authentication Source** for the Developer portal.

[select Basic AUTH (Developer Portal) which we have created previously]

©TGH Software Solutions Pvt. Ltd.

(v) select the roles you want give access

(vi) click on save

API Gateways > sowjanya gateway

sowjanya gateway

Information:

- Gateway Information
- Startup Properties
- Cluster Status
- Log Files
- Java Information

Settings & Configuration:

- Properties
- Location Settings
- Forward Proxy Settings
- Developer Portal Settings**
- Execution Settings

Deployment:

- Gateway Version
- Runtime Release Scheduling

Developer Portal Settings ?

Specify the Developer Portal settings for this API Gateway. These settings control the external Developer Portal that your API users will access to work with your APIs.

* Required fields.

Location Information

Configure the Developer Portal's location and status. When you save **certain settings** ?, the Developer Portal restarts causing a brief interruption of service.

Portal Status ? Enabled

Bind Address* ?
⚠ This URL is not secure, because it uses an HTTP protocol. It is not recommended for production use. Use an HTTPS protocol for a secure address. (Example: https://localhost:443)

Public URL ?
Example: https://devportal.yourcompany.com:443

Security Settings

Specify whether the API Gateway can respond with HTTP Security Headers to requests made by the browser for the Developer Portal. By default, the security settings are enabled.

HTTP Security Headers ? Enabled

Developer Portal Authentication Source

The API Gateway uses two authentication sources, one for the endpoints (determining which application's API calls can be processed) and another for the Developer Portal (determining which users can log into the Portal). The endpoint settings are set for each API deployment on the [Deploy > Packaged APIs page](#).

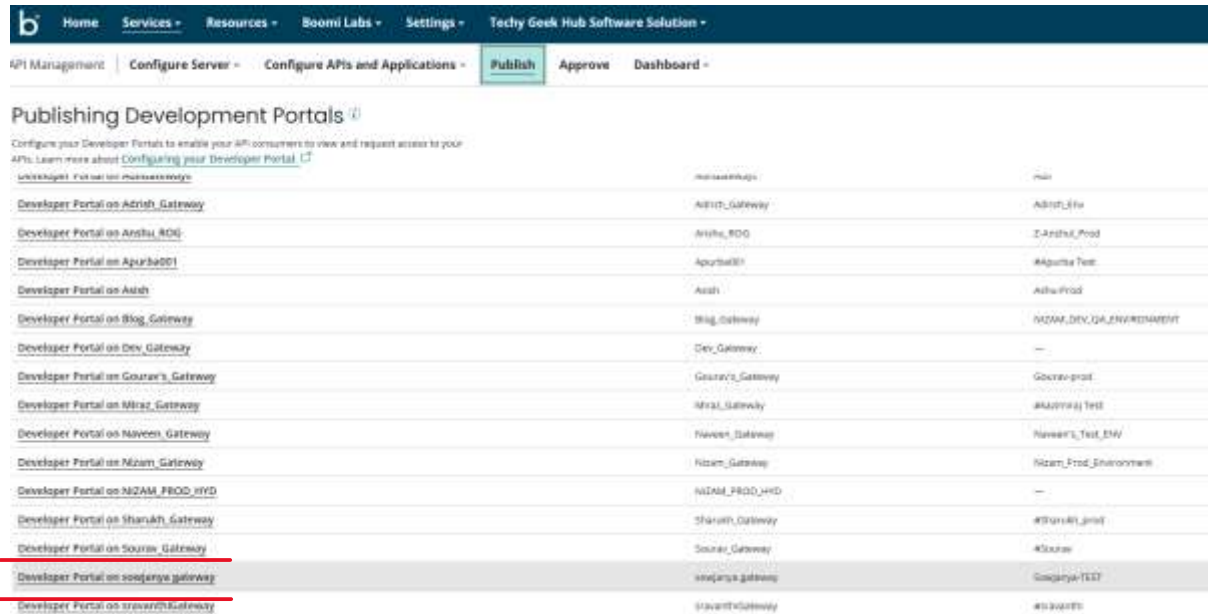
Authentication Source* ?

Restrict Access by Role ?

 Administrator General

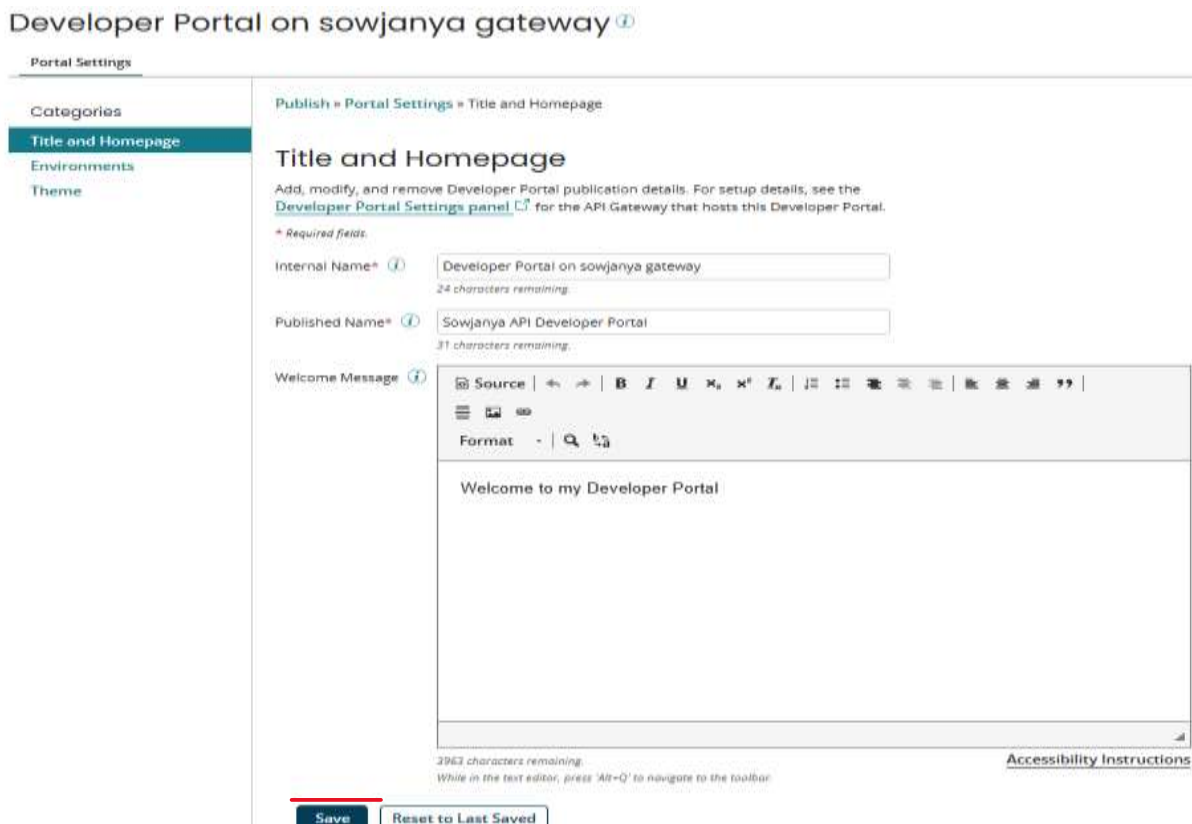
Restrict access by role information.

Step 6: Navigate to the **Publish** page and select your Developer Portal from list.



Developer Portal on	Internal Name	Publ
Developer Portal on Adrish Gateway	ADRIH_Gateway	ADRIH_Effw
Developer Portal on Anshu_RDD	Anshu_RDD	I-Anshu_Prod
Developer Portal on ApurbaDD1	ApurbaDD1	APurba Test
Developer Portal on Ashish	Ashish	AshishProd
Developer Portal on Blog Gateway	Blog_Gateway	NDW_DEV_QA_ENVIRONMENT
Developer Portal on Dev Gateway	Dev_Gateway	---
Developer Portal on Gourav's Gateway	Gourav's_Gateway	Gourav-prod
Developer Portal on Miraz Gateway	Miraz_Gateway	MirazProd Test
Developer Portal on Naveen Gateway	Naveen_Gateway	Naveen's_Test_ENV
Developer Portal on Nizam Gateway	Nizam_Gateway	Nizam_Prod_Environment
Developer Portal on NIZAM_PROD_HYD	NIZAM_PROD_HYD	---
Developer Portal on Sharath Gateway	Sharath_Gateway	SHarath_prod
Developer Portal on Sourav Gateway	Sourav_Gateway	KSourav
Developer Portal on Sowjanya gateway	Sowjanya gateway	Sowjanya-TEST
Developer Portal on Sravanthi Gateway	SravanthiGateway	SRAVANTH

Step7: From the Title and Homepage category, enter an **Internal Name**, **Published Name**, and **Welcome Message** for your Developer Portal and click on save.



Developer Portal on Sowjanya gateway

Portal Settings

Categories

Title and Homepage

Environments

Theme

Publish » Portal Settings » Title and Homepage

Title and Homepage

Add, modify, and remove Developer Portal publication details. For setup details, see the [Developer Portal Settings panel](#) for the API Gateway that hosts this Developer Portal.

* Required fields

Internal Name* 24 characters remaining.

Published Name* 31 characters remaining.

Welcome Message

2963 characters remaining. While in the text editor, press 'Alt+Q' to navigate to the toolbar.

Save | Reset to Last Saved

[Accessibility Instructions](#)

Step 8: From the **Theme** category, specify the theme colours and site logo with alternative text for your Developer Portal. Click **Preview Before Saving** and then Click **Publish**.

Developer Portal on sowjanya gateway [?]

Portal Settings

Categories

Title and Homepage

Environments

Theme


Publish » Portal Settings » Theme


Theme


Add, modify, or remove Developer Portal theme constants to match your Developer Portal to your organization's branding.


* Required fields.


Theme Colors


Site Background Color* 
Enter a hex code value. The acceptable formats are either #000000 or #000.


Content Background Color* 
Enter a hex code value. The acceptable formats are either #000000 or #000.

Border Color* 
Enter a hex code value. The acceptable formats are either #000000 or #000.

Primary Text Color* 
Enter a hex code value. The acceptable formats are either #000000 or #000.


Link Text Color* 
Enter a hex code value. The acceptable formats are either #000000 or #000.

Selected Item Color* 
Enter a hex code value. The acceptable formats are either #000000 or #000.

Heading Color* 
Enter a hex code value. The acceptable formats are either #000000 or #000.

Site Logo

Site Logo:
Maximum file size is 50x200px in the jpg, png, or svg format.

Site Logo Preview: 

Site Logo Alternative Text:
96 characters remaining.
Leaving this field blank generates an empty <alt> tag.

Configuration of Developer Portal is completed by following steps 1-8.

Now it's the time to make the developer portal available to the users.

Step 9: Send your Developer Portal URL to your Developer Portal users so that they can sign in and begin working with your APIs.

Step 10: To get the developer portal URL go back to **developer portal settings** and copy the public URL which we have configured in **step 5**.

API Gateways » sowjanya gateway

sowjanya gateway

Information:

Gateway Information

Startup Properties

Cluster Status

Log Files

Java Information

Settings & Configuration:

Properties

Location Settings

Forward Proxy Settings

Developer Portal Settings

Execution Settings

Deployment:

Gateway Version

Runtime Release Scheduling

Developer Portal Settings ?

Specify the Developer Portal settings for this API Gateway. These settings control the external Developer Portal that your API users will access to work with your APIs.

* Required fields

Location Information

Configure the Developer Portal's location and status. When you save **certain settings** ?, the Developer Portal restarts causing a brief interruption of service.

Portal Status ?

Enabled

Bind Address* ?

⚠ This URL is not secure, because it uses an HTTP protocol. It is not recommended for production use. Use an HTTPS protocol for a secure address. (Example: https://localhost:443)

Public URL ?

Example: https://devportal.yourcompany.com:443

Security Settings

Specify whether the API Gateway can respond with HTTP Security Headers to requests made by the browser for the Developer Portal. By default, the security settings are enabled.

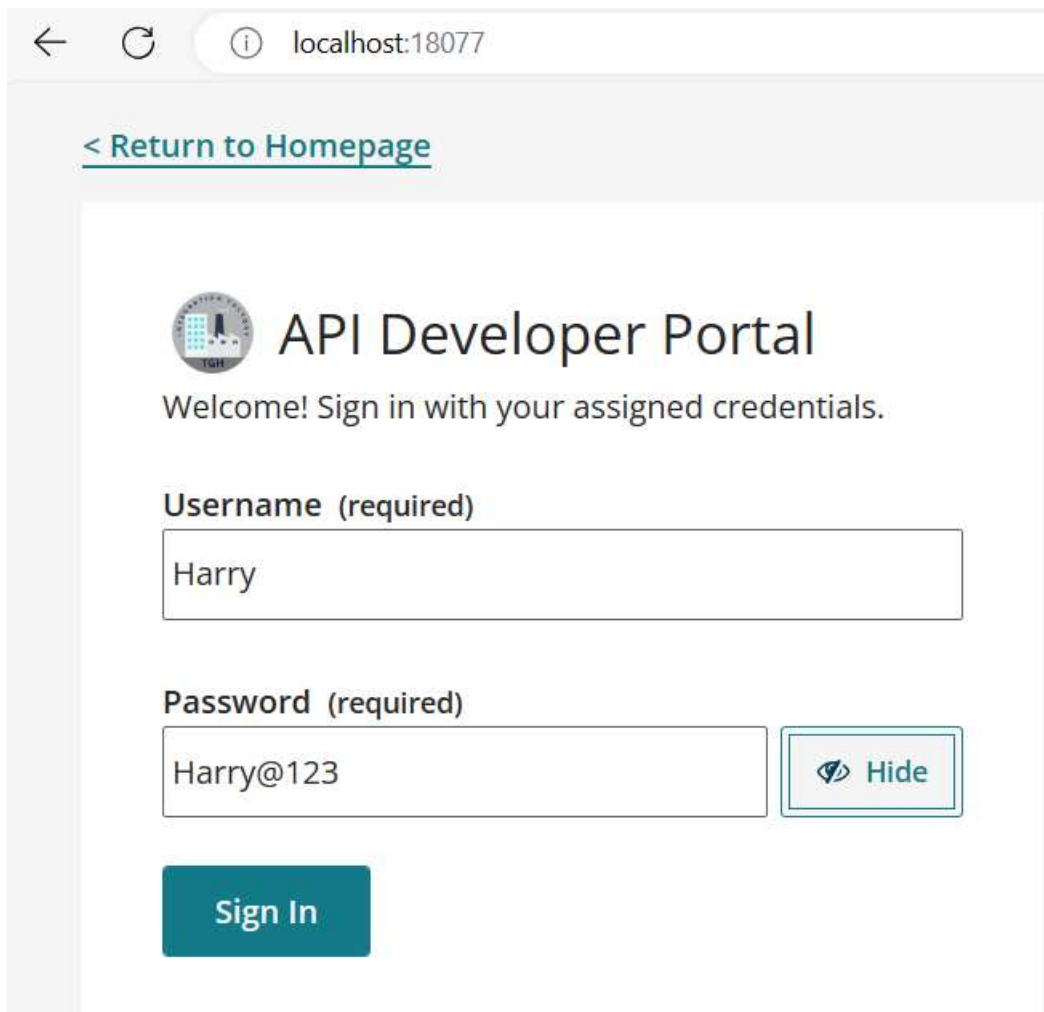
HTTP Security Headers ?

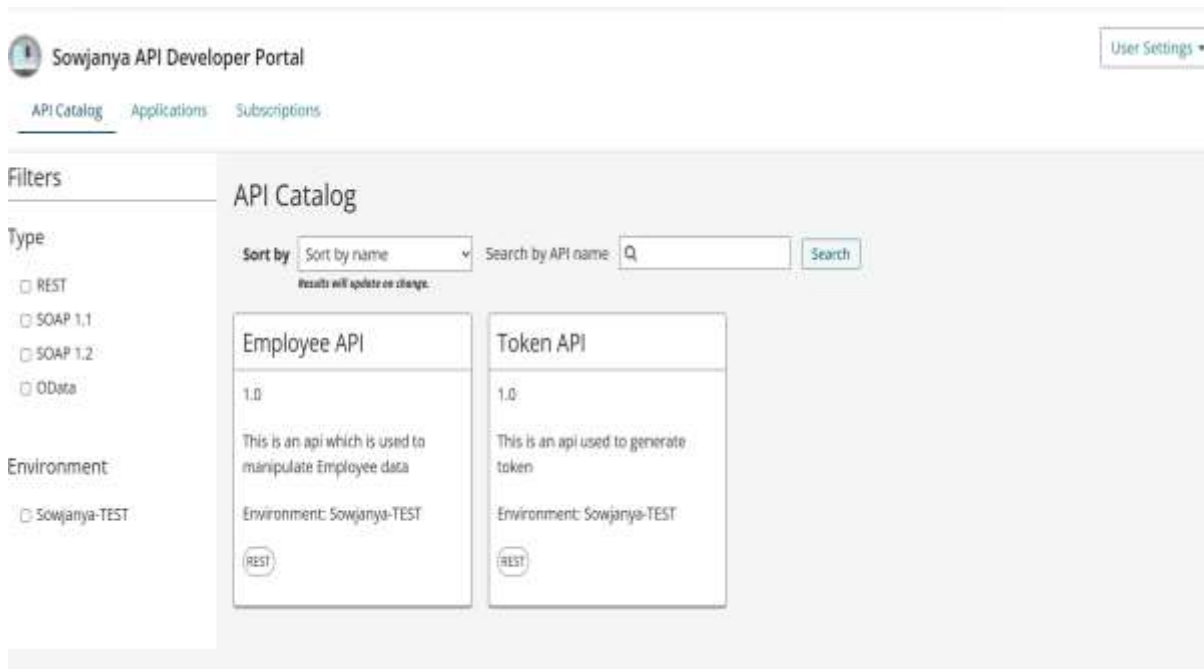
Enabled

Step 11: Now assume yourself as a developer portal user and open a new tab in browser and paste the public URL .The portal will look as shown in the below image.



Step 12: Sign in with username and password (which we have configured while creating basic authentication source refer to Basic Authentication Source Configuration). The portal will look as shown below.





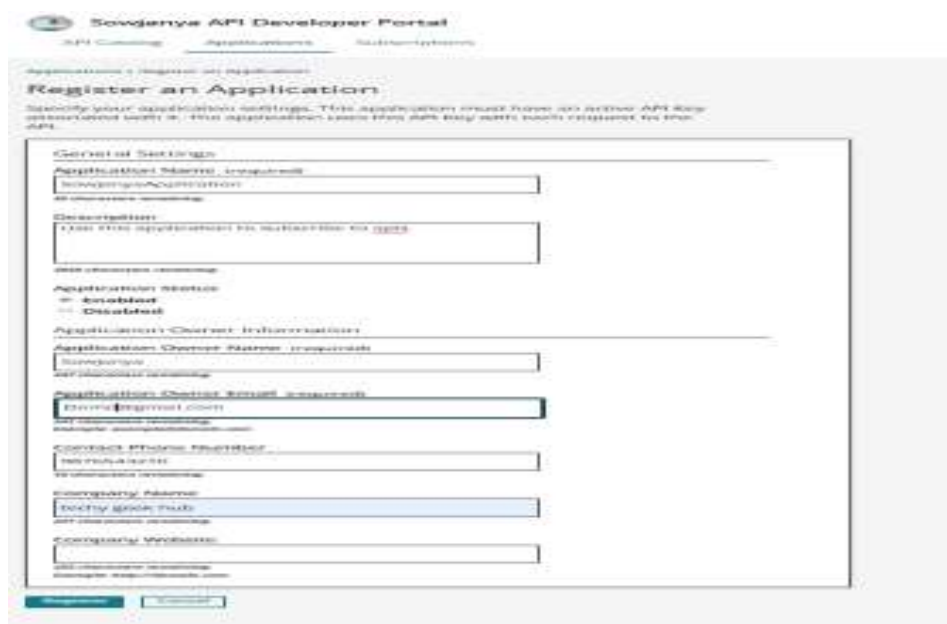
Step 13: By default, we will be in API Catalog. In API Catalog we can find all the APIs which were deployed to environment that is attached to the gateway.

Here you can find only 2 APIs since I have deployed only Employee API and Token API to my gateway.

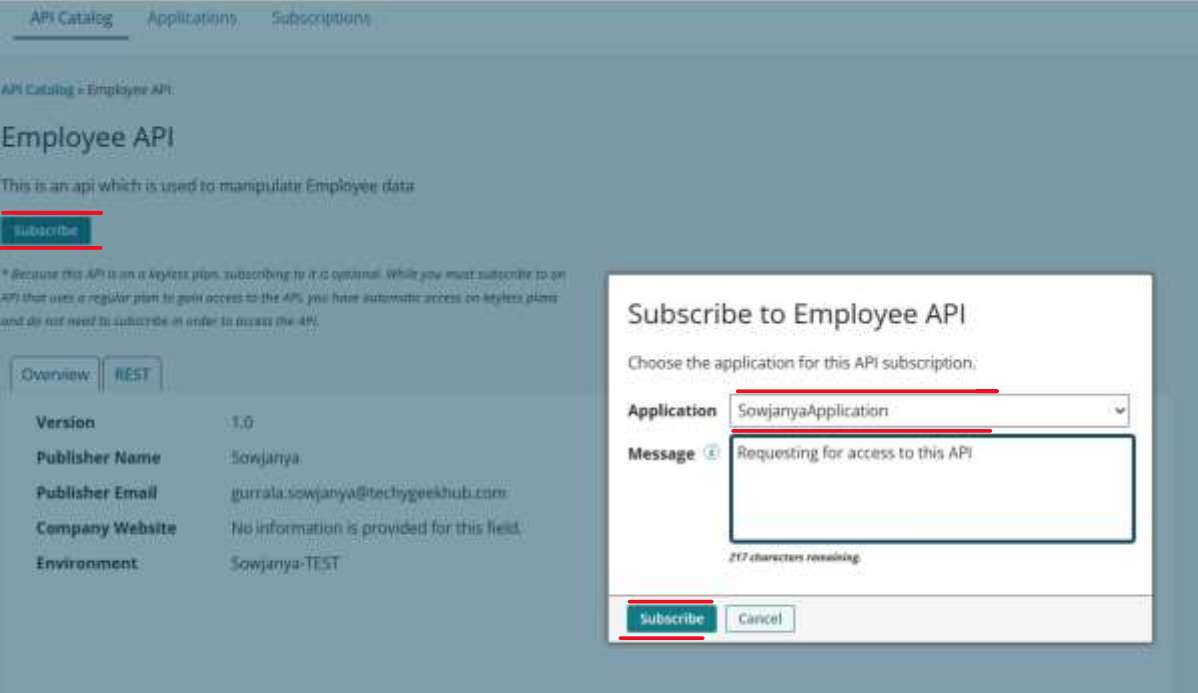
Step 14: Before subscribing to any API, it is mandatory to create an application.

Step 15: Go to Applications tab and click on register an application.

Fill the fields and click on register.

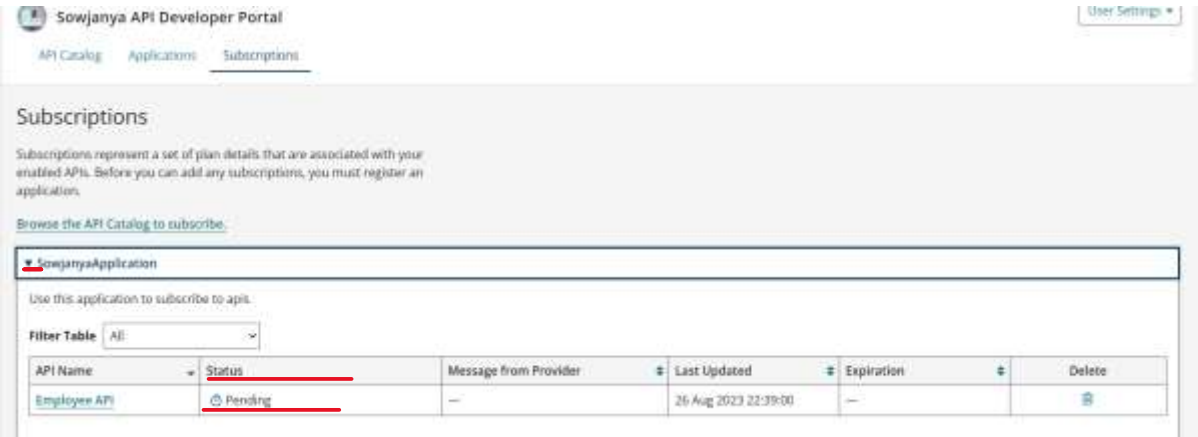


Step 15: Click on the API for which you want to get subscription and click on subscribe button. Choose the Application from the dropdown and click on subscribe.



The screenshot shows the 'Employee API' page in the API Catalog. A modal titled 'Subscribe to Employee API' is open, prompting the user to 'Choose the application for this API subscription'. The 'Application' dropdown is set to 'SowjanyaApplication'. The 'Message' field contains the text 'Requesting for access to this API'. There are 'Subscribe' and 'Cancel' buttons at the bottom of the modal.

Step 16: Go to the subscriptions tab and expand your application .You can see the status as pending for Employee API.

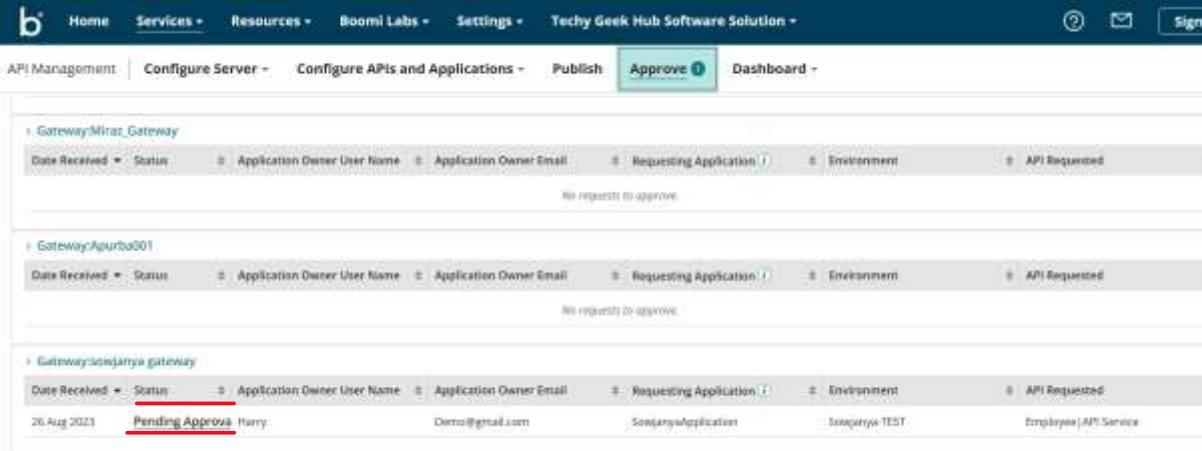


The screenshot shows the 'Subscriptions' tab in the 'Sowjanya API Developer Portal'. It displays a table of subscriptions for the 'SowjanyaApplication'. The table has columns for API Name, Status, Message from Provider, Last Updated, Expiration, and Delete. One subscription is listed for 'Employee API' with a status of 'Pending'.

API Name	Status	Message from Provider	Last Updated	Expiration	Delete
Employee API	Pending	—	26 Aug 2023 22:39:00	—	

Step 17: Now acting as Api provider, go to Boomi atmosphere API Management to approve the request. In Approve tab we can see all the subscription requests.

Click on Approve and search for your gateway. You can see the status as pending.



Date Received	Status	Application Owner User Name	Application Owner Email	Requesting Application	Environment	API Requested
No requests to approve						
No requests to approve						
26 Aug 2023	Pending Approval	Harry	Demo@gmail.com	SowjanyaApplication	Sowjanya-TEST	Employee API Service

Step18: Click on the pending Approval link and click on Accept.

Approve Subscription Request ?

The following subscription request requires approval or rejection.

[Return to List](#)
[◀ Previous](#)
[Next ▶](#)
[✔ Approve](#)
[✖ Reject](#)

Basic Information

Date Received	26 Aug 2023 22:39:28
Application Owner User Name	Harry
Application Owner Name	Sowjanya
Application Owner Email	Demo@gmail.com
Requesting Application	SowjanyaApplication
Gateway	sowjanya gateway
Environment	Sowjanya-TEST
API Requested	Employee API Service
Message from Requester	Requesting for access to this API

Step 19: Select a Plan from the dropdown and configure enable and disable dates. Click on approve.

©[TGH Software Solutions Pvt. Ltd.](#)

(Here plan is a collection of policies which is used to set limits around the usage of an Api including maximum message size, rate limit and quota limit)

Approve Employee|API Service for SowjanyaApplication

Choose a Plan for this API and Application combination. You can also provide a message back to the subscriber.

* Required fields.

Plan* → LimitedPlan(Sowjanya)

Enable* 26 Aug 2023 at 00:00

Format: dd Mmm yyyy
⚠ Time zone is (UTC+5:30) Coordinated Universal Time

Disable* Do not automatically disable

Disable on 26 Aug 2023 at 00:00

Format: dd Mmm yyyy (for date); hh:mm (for time)
⚠ Time zone is (UTC+5:30) Coordinated Universal Time

Message to Requester Accepting the request.Thanks

996 characters remaining.

Cancel
Approve

Step 20: Go back to developer portal. Click on subscriptions tab. Expand the application which you have created in Step 15. We can see status as Enabled.

Sowjanya API Developer Portal User Settings ▾

API Catalog Applications Subscriptions

Subscriptions

Subscriptions represent a set of plan details that are associated with your enabled APIs. Before you can add any subscriptions, you must register an application.

[Browse the API Catalog to subscribe.](#)

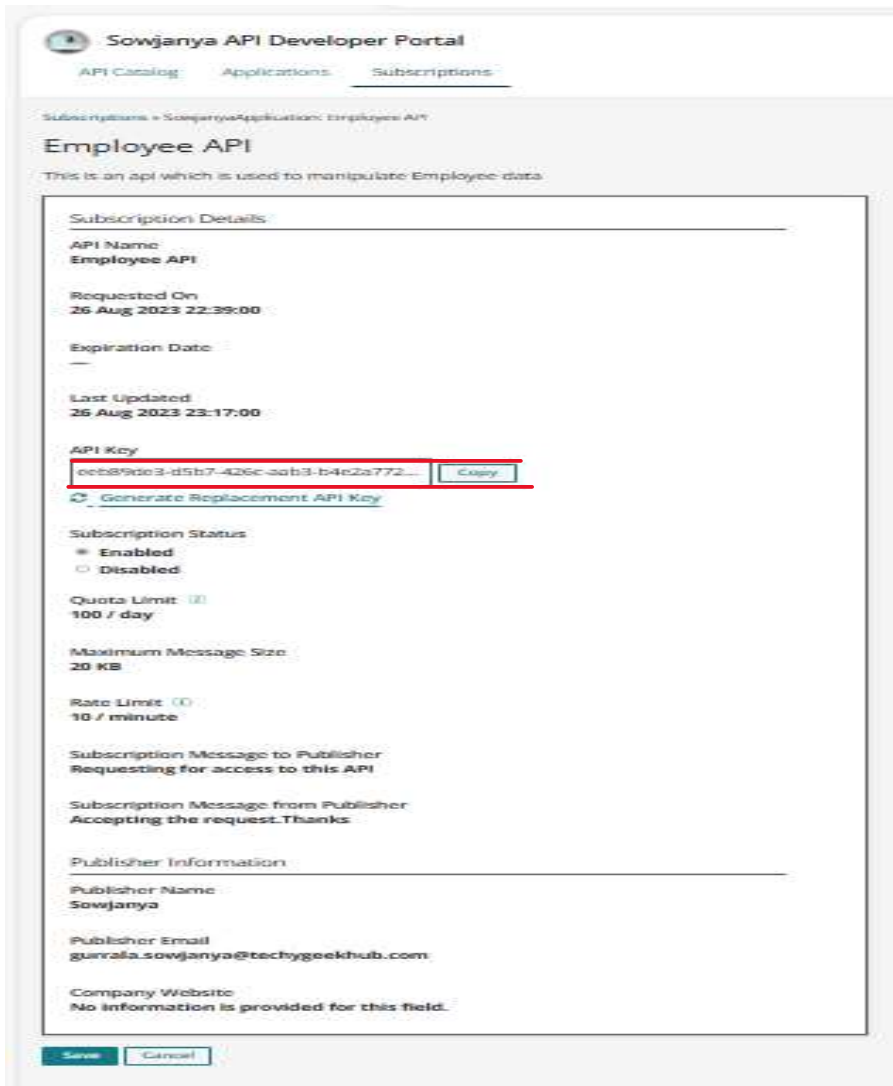
▼ SowjanyaApplication

Use this application to subscribe to apis

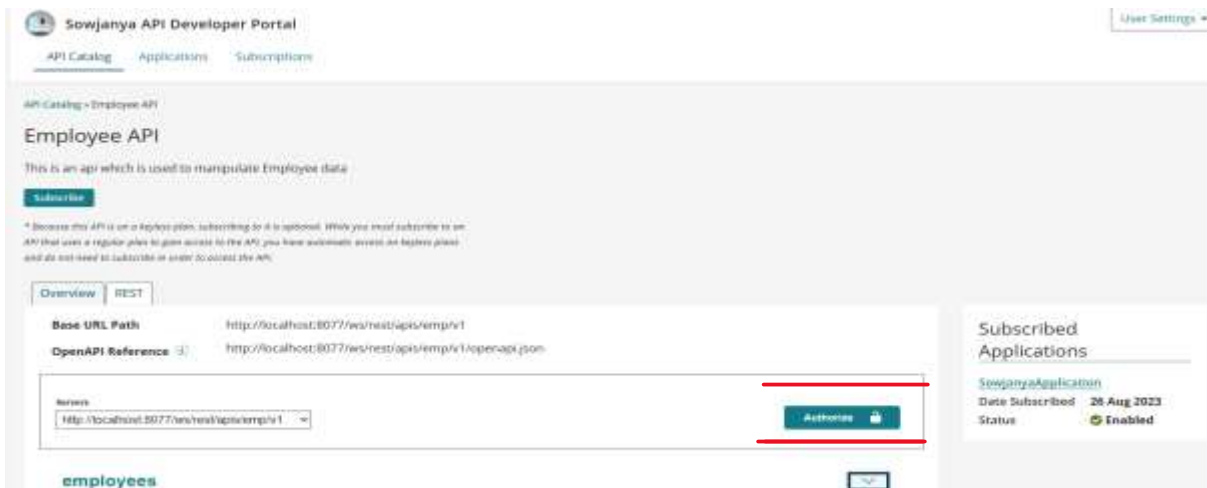
Filter Table: All

API Name	Status	Message from Provider	Last Updated	Expiration	Delete
Employee API	Enabled	Accepting the request.Thanks	26 Aug 2023 23:17:00	—	

Step 21: Click on the Employee API hyperlink. Copy the Api key and paste it in a notepad and click on save.



Step 22: Go to API Catalog tab and click on Employee API. Then click on REST We can see the new window will look as shown below.



©TGH Software Solutions Pvt. Ltd.

No part of this document may be copied, reproduced, republished, uploaded, posted, publicly displayed, encoded, translated, transmitted or distributed in any way to any other computer, server, website or other medium for publication or distribution, without TGH's prior written consent

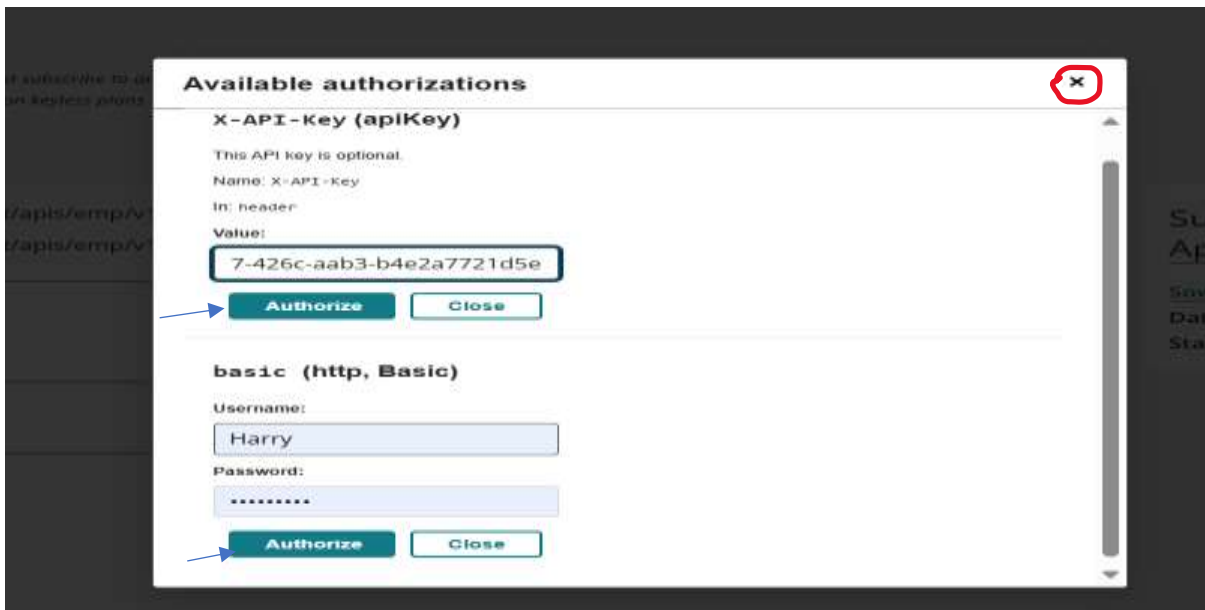


Step 23: Now we can test the Api in developer portal or we can use testing tool like postman

Step 24: To test in developer portal

In order to test in developer portal, click on Authorize and paste the Api-key which you copied in Step 21. Enter Username and password. Click on authorize and then x symbol.

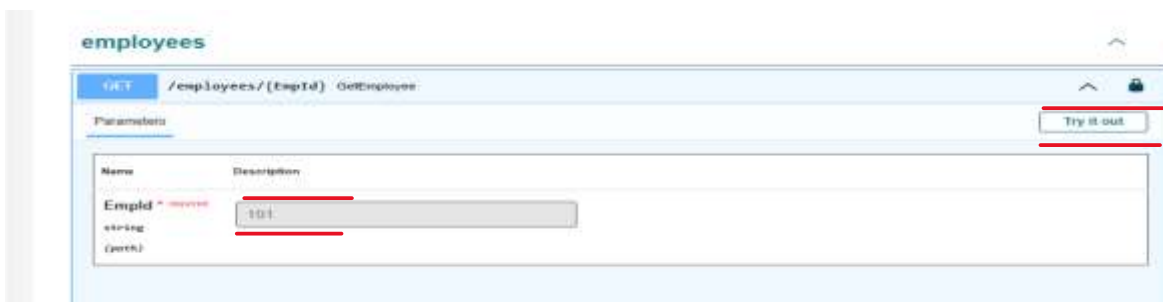
(Here for Employee API also we are using the same authentication source which we have configured previously to authenticate the users of developer portal)

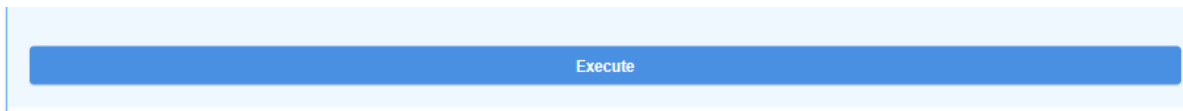


Step 24: Expand the operation.



Step 25: Click on Try it out and pass the EmpId. Now click on Execute bar.





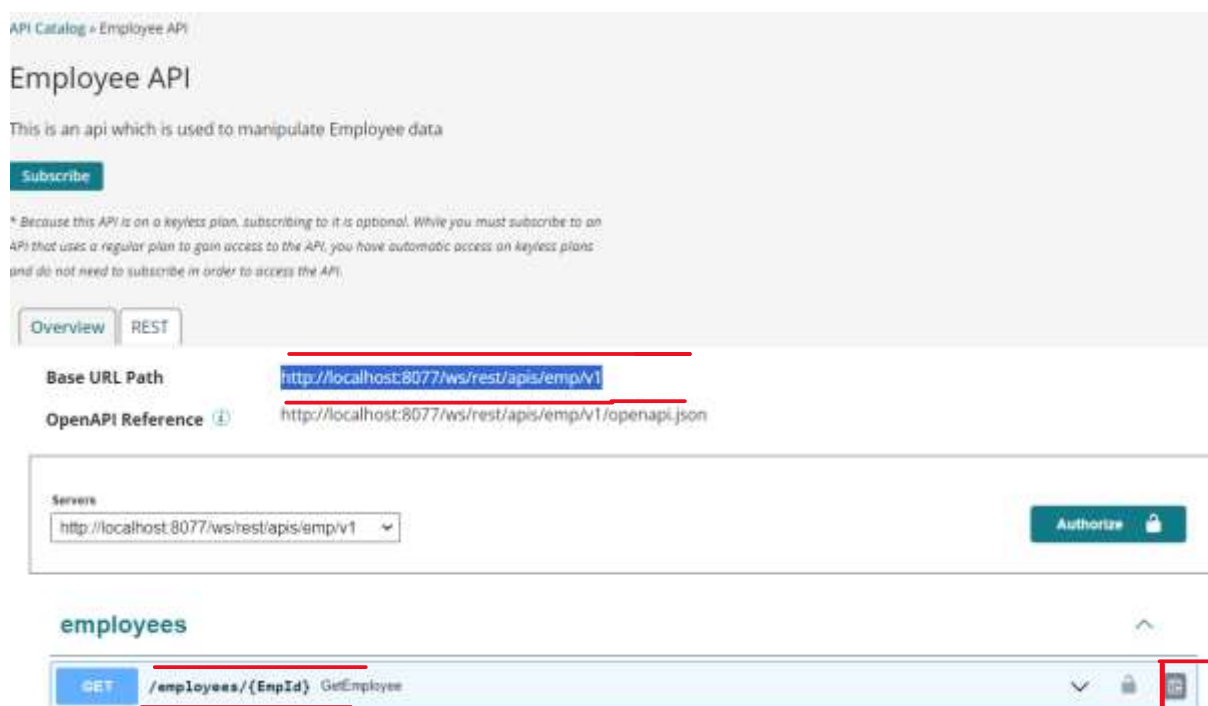
Step 26: we can see the response with status code as 200.



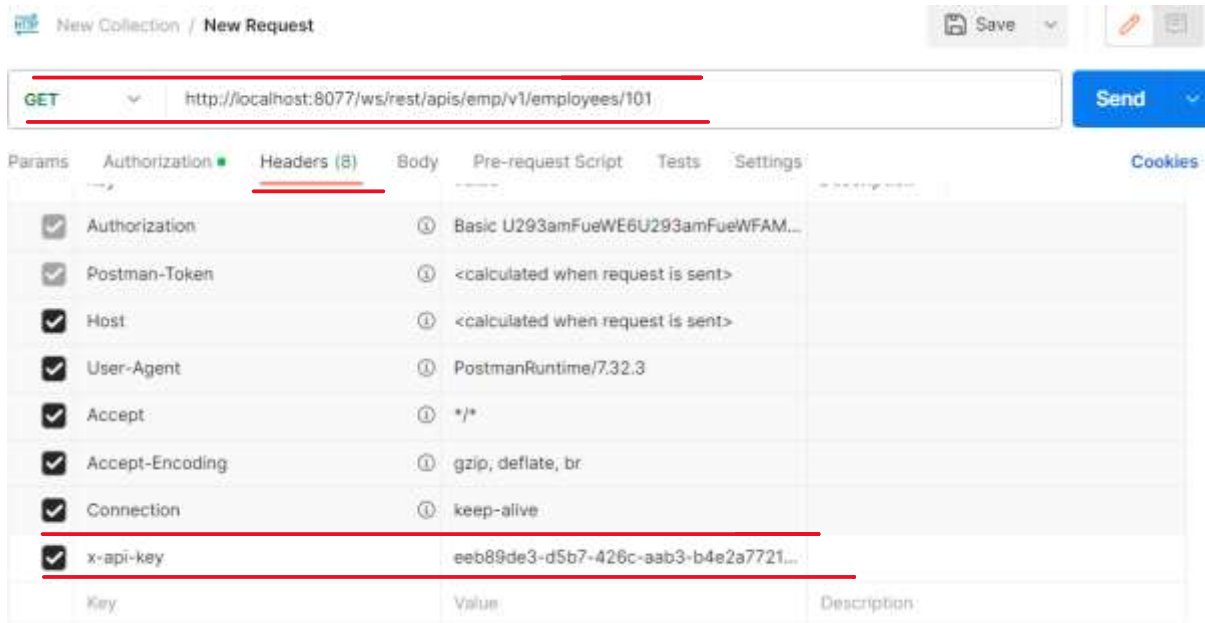
Step 27: To test in postman

Copy Base URL path and resource path. Concatenate to form the complete endpoint

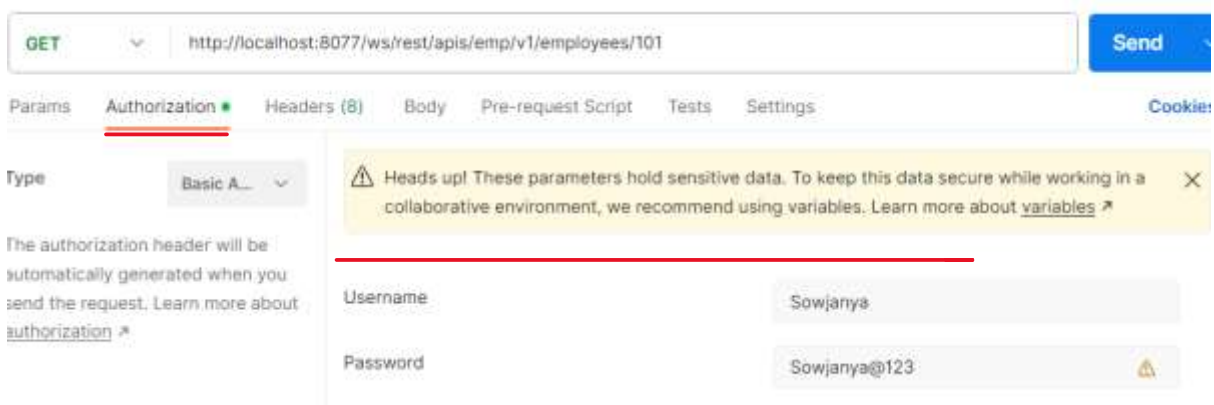
`http://localhost:8077/ws/rest/apis/emp/v1/employees/ {EmpId}`



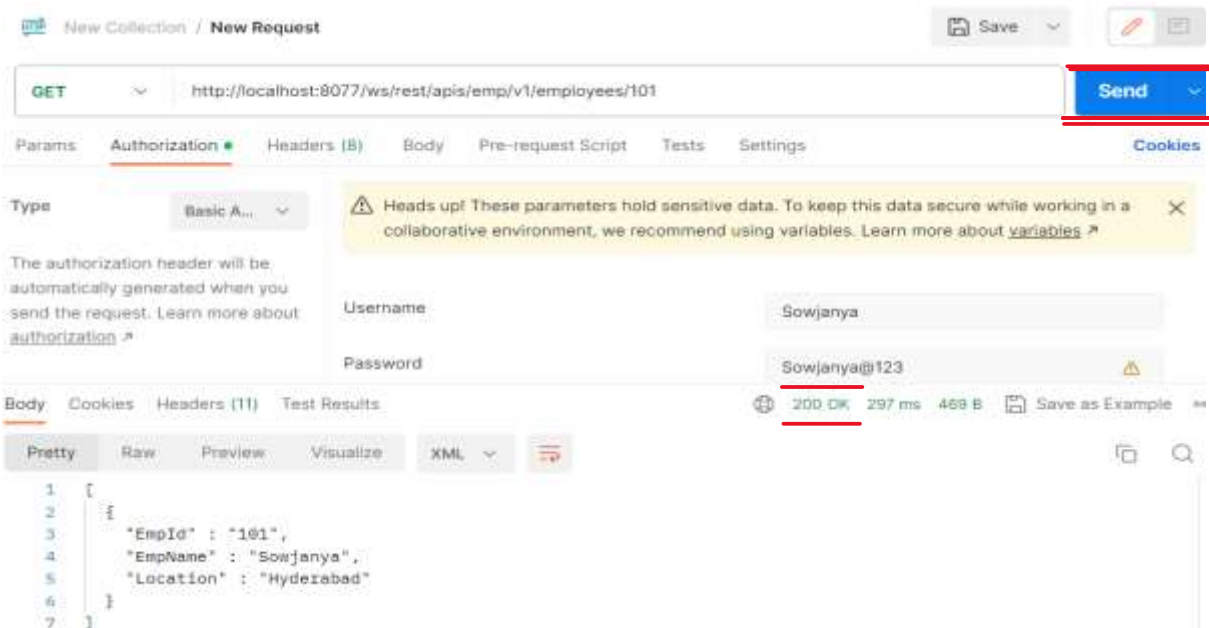
Step 28: Open postman app. Paste the endpoint and give value for Uri parameter (ex:101). Create a custom header as x-api-key and give the value (api-key) which we copied in step 21.



Step 29: click on Authorization. Choose Type as Basic auth and give the valid username & password.



Step 30: Now click on send. We can see the response with status code as 200 OK



The screenshot shows the Postman interface for a new request. The URL is `http://localhost:8077/ws/rest/apis/emp/v1/employees/101`. The request method is GET. The Authorization tab is selected, showing Basic Auth with Username `Sowjanya` and Password `Sowjanya@123`. The response status is `200 OK`. The response body is a JSON object:

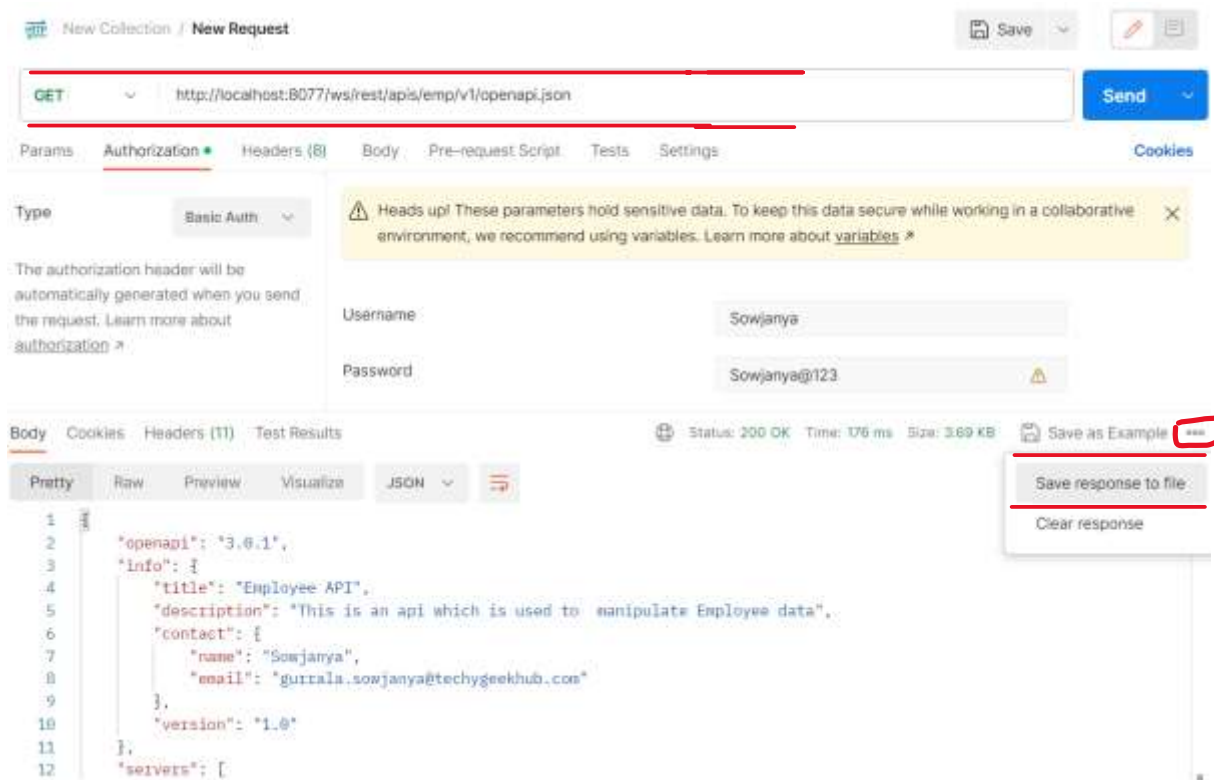
```
1 {
2   "EmpId": "101",
3   "EmpName": "Sowjanya",
4   "Location": "Hyderabad"
5 }
6 ]
7 ]
```

Step 31: To get the swagger specification file of this API

Copy the **Open API Reference** (see step 22) & paste it in postman.

Configure the Authorization and Headers tab as mentioned in step 28 & Step 29.

Click on send. We can see the Specification file which is generated. Click on save response to file to save.



The screenshot shows the Postman interface for a new request. The URL is `http://localhost:8077/ws/rest/apis/emp/v1/openapi.json`. The request method is GET. The Authorization tab is selected, showing Basic Auth with Username `Sowjanya` and Password `Sowjanya@123`. The response status is `200 OK`. The response body is a JSON object representing the OpenAPI specification:

```
1 {
2   "openapi": "3.0.1",
3   "info": {
4     "title": "Employee API",
5     "description": "This is an api which is used to manipulate Employee data",
6     "contact": {
7       "name": "Sowjanya",
8       "email": "gurrala.sowjanya@techygeekhub.com"
9     },
10    "version": "1.0"
11  };
12  "servers": [
```

The 'Save as Example' dropdown menu is open, and the 'Save response to file' option is highlighted.

©TGH Software Solutions Pvt. Ltd.

References:

- <https://help.boomi.com/>
- https://help.boomi.com/docs/Atomsphere/API%20Management/Topics/c-api-Getting_Started_f06ad982-c0d9-4c67-ab0f-7a19db534868
- https://help.boomi.com/docs/Atomsphere/API%20Management/Topics/api-Developer_Portal_8d00d936-4358-41f5-94eb-0b950d892e74



TGH

Making Integrations Simpler



TGH Software Solutions Pvt. Ltd.

www.techygeekhub.com

At TGH, we specialize in driving digital transformation through seamless Integration Technologies.

Operating as an INTEGRATION FACTORY, we serve as a one-stop shop for all your integration needs. Our expert team is well-versed in enterprise software and legacy system integration, along with leading iPaaS technologies like Boomi, MuleSoft, Workato, OIC, and more.

We're committed to enhancing business processes and solving problems through our integration expertise.



Email address

connect@techygeekhub.com



Phone number

+ 011-40071137
+ 91-8810610395



Our offices

Noida Office

iThum
Plot No -40, Tower A,
Office No: 712,
Sector-62, Noida,
Uttar Pradesh, 201301

Hyderabad Office

Plot no: 6/3, 5th Floor,
Techno Pearl Building,
HUDA Techno Enclave,
HITEC City, Hyderabad,
Telangana 500081

