

**Note:** A more recent version of IBM API Connect is available.  
For details, see the [IBM API Connect 10.0.2 and later product documentation](#).

# Tutorial: Generate a JSON Web Token (JWT)

Last Updated: 2021-07-14

This tutorial shows you how to define and implement a REST API definition that generates a JSON Web Token (JWT).

## About this tutorial

In this tutorial you complete the following lessons:

- 1. [Generate a JWT](#)
- 2. [Testing the REST API](#)

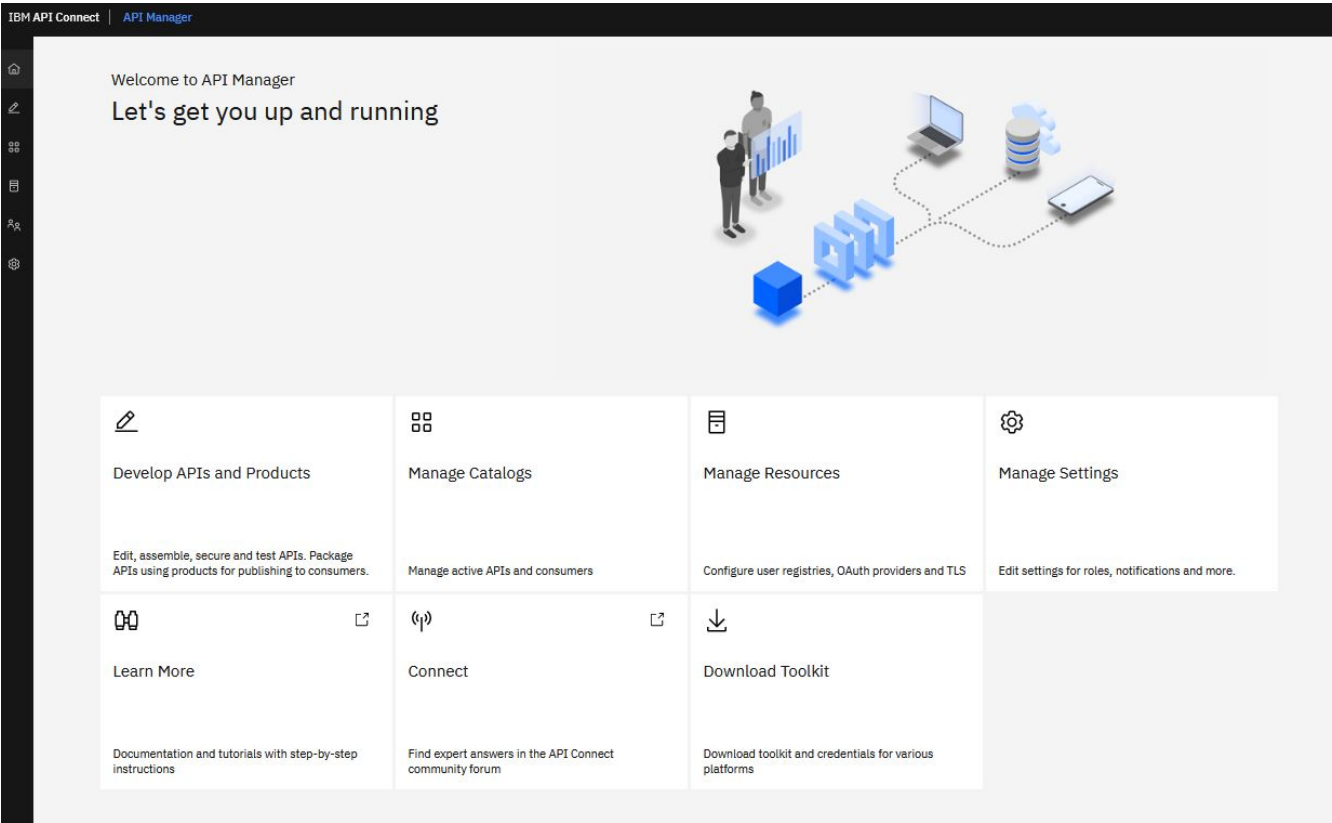
**Note:** The Sandbox catalog must be configured to use either a DataPower® Gateway (v5 compatible) or a DataPower API Gateway or both. See [Creating and configuring Catalogs](#).

## Generate a JWT

Create a REST API to generate and return a JSON Web Token (JWT).

To add and define this REST API, complete the following steps:

- 1. Log in to API Manager.
- 2. In the Welcome page, click the **Develop APIs and Products** tile.



- 3. Click **Add API**.

## Develop

APIs

Products

Add

API

Product

 What are you looking for today?


No recent items found.

4. Ensure that **OpenAPI 2.0** is selected.5. Select **New OpenAPI**. Click **Next**.

OpenAPI 2.0

OpenAPI 3.0

Create

☒ **From target service**  
 Create a REST proxy that routes all traffic to a target API or service endpoint

☒ **From existing OpenAPI service**  
 Create a REST proxy based upon an OpenAPI described target service

☒ **From existing WSDL service (SOAP proxy)**  
 Create a SOAP proxy based upon a WSDL described target service

☒ **From existing WSDL service (REST proxy)**  
 Create a REST proxy based upon a WSDL described target service

☒ **From existing GraphQL service (GraphQL proxy)**  
 Create a GraphQL proxy based on a GraphQL service

☒ **New OpenAPI**  
 Compose a new REST proxy by defining paths and operations

Import

☒ **Existing OpenAPI**  
 Use an existing definition of a REST proxy or GraphQL proxy or SOAP API

Cancel

Next

```

graph LR
    App[App] <--> APIProxy[API Proxy]
    APIProxy --- OpenAPI[OpenAPI]
  
```

6. Enter the appropriate information to create a REST API definition.

- In the **Title** field, enter JWT.
- The **Name** and **Base Path** fields auto-populate with the terms `jwt` and `/jwt` respectively.
- The **Version** field auto-populates with `1.0.0`.

>

### Info

Enter details of this API

Title

Name

Version

Base path (optional)

Description (optional)

[Cancel](#) [Next](#)

7. Click **Next**.

8. Make no changes on the **Secure** screen. Click **Next**.

## Create New OpenAPI

### Secure

Configure the security of this API

☒ Secure using Client ID

☒ CORS

[Cancel](#) [Back](#) [Next](#)

9. You see the progress as the new API gets created. When it is done, you see a Summary. Click **Edit API**.

## Create New OpenAPI

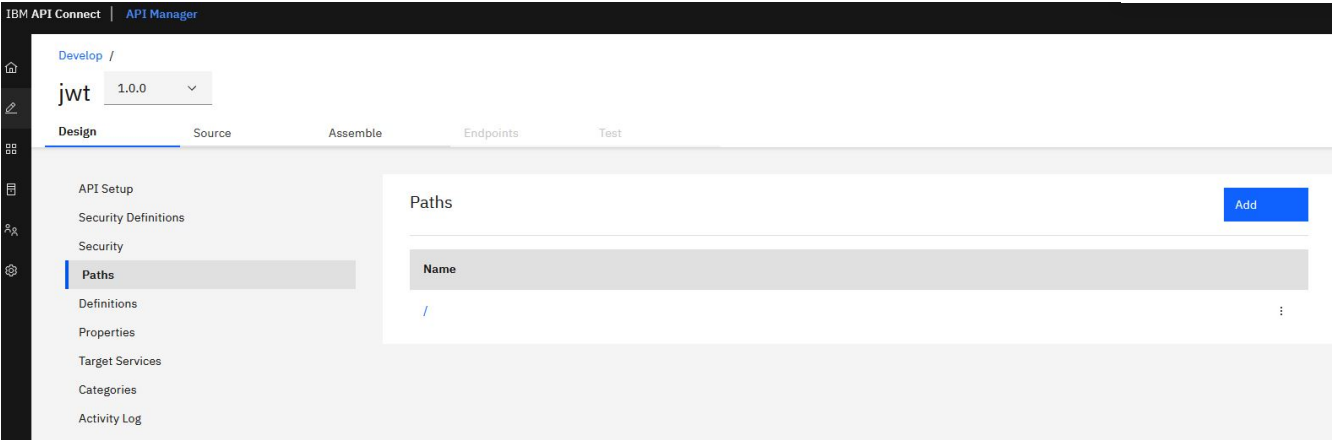
### Summary

✓ Generated OpenAPI 2.0 definition

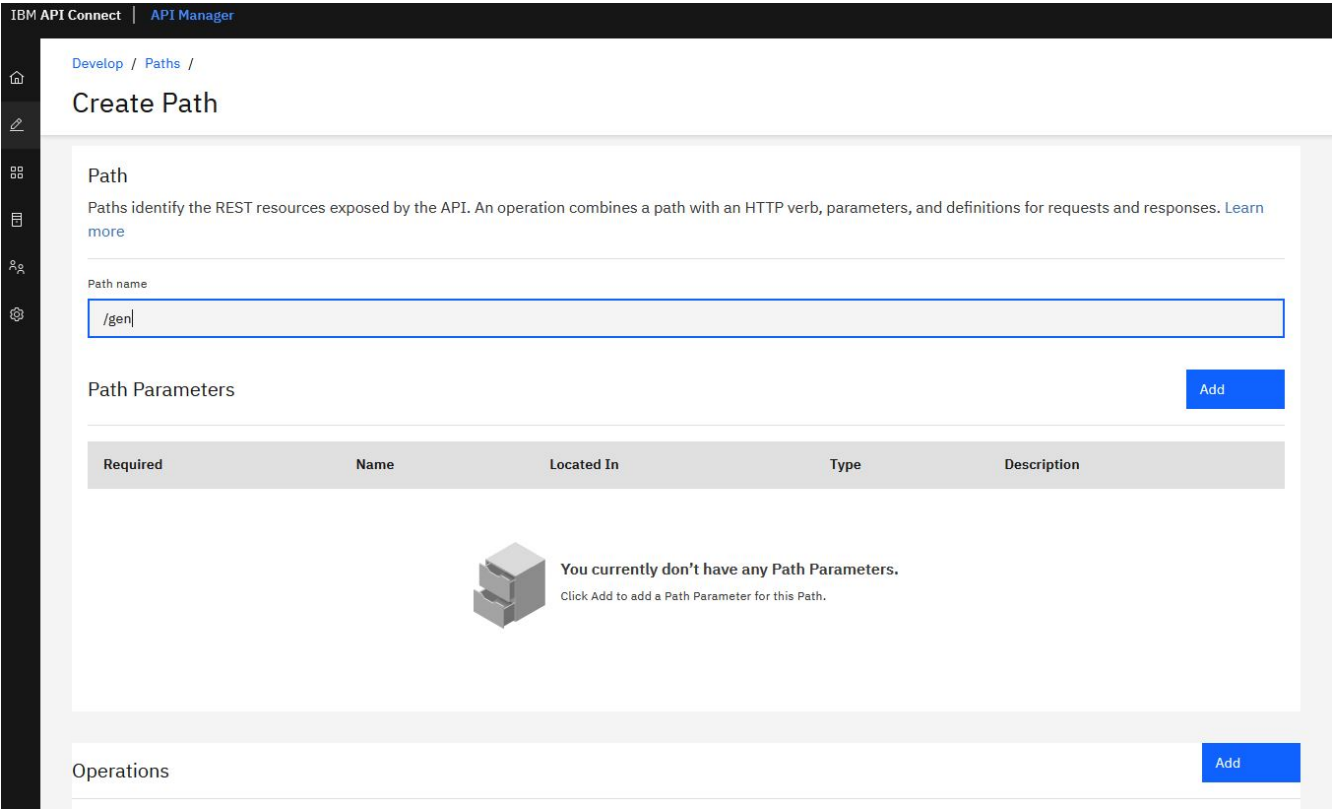
✓ Applied security

[Edit API](#)

10. In the side bar of the Design page, select **Paths** to display the **Paths** panel.



- 11. Click **Add**.
- 12. In the **Path name** field, enter **/gen**.
- 13. In the **Operations** section, click **Add**.
- 14. Select **GET** and click **Add**.



- 15. Click **Save**.
- 16. Click **/gen** in the list of available paths.



- 17. Click **GET** in the list of **Operations**.
- 18. Scroll down. In the **Parameters** section, click **Add**.
  - a. Select **REQUIRED**.
  - b. Enter **iss-claim** in the **NAME** field.
  - c. Select **header** in the **LOCATED IN** field.

- d. Select string in the **TYPE** field.
- e. Enter Enter https://myidp.ibm.com to match in the **DESCRIPTION** field.

Parameters Add

Required	Name	Located In	Type	DESCRIPTION	Delete
<input checked="" type="checkbox"/>	iss-claim	header	string	Enter https://myidp.ibm.com	

19. Click **Add** to add a second parameter.
- a. Select **REQUIRED**.
  - b. Enter aud-claim in the **NAME** field.
  - c. Select header in the **LOCATED IN** field.
  - d. Select string in the **TYPE** field.
  - e. Enter Enter ClientID1 to match in the **DESCRIPTION** field.

Parameters Add

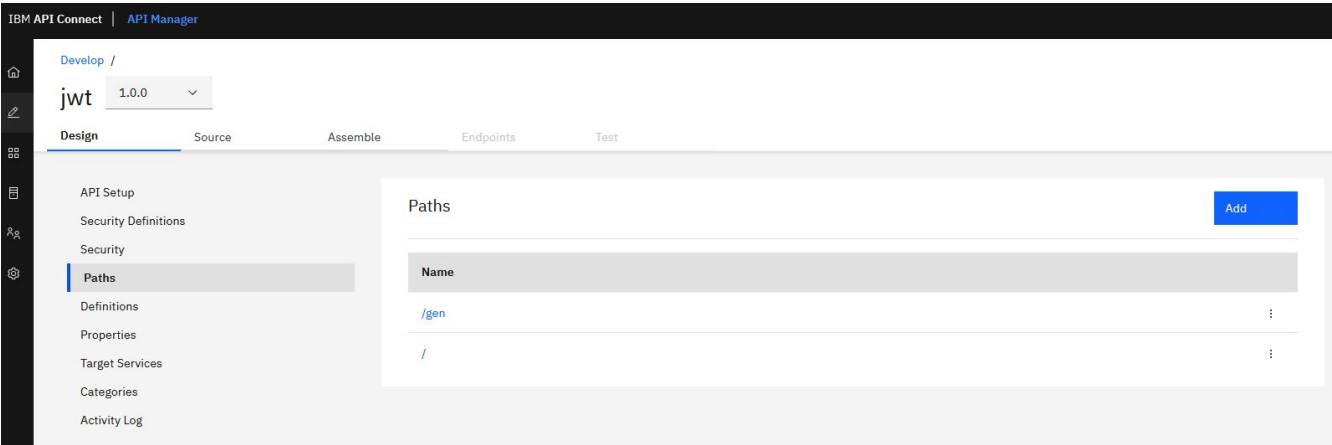
Required	Name	Located In	Type	DESCRIPTION	Delete
<input checked="" type="checkbox"/>	iss-claim	header	string	Enter https://myidp.ibm.com	
<input checked="" type="checkbox"/>	aud-claim	header	string	Enter ClientID1	

20. In the **Response** section, change the description of the pre-supplied 200 status code to 200 OK.

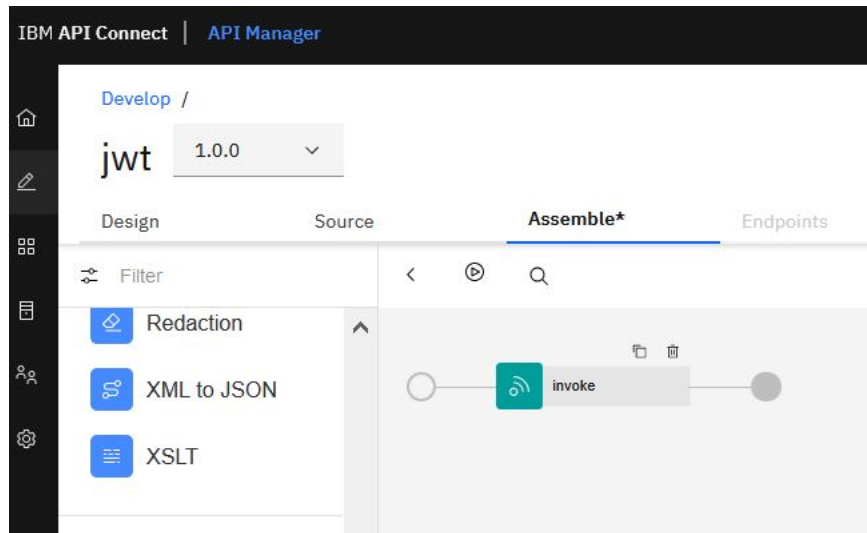
Response Add

Status Code	Schema	Description	Delete
200	string	200 OK	

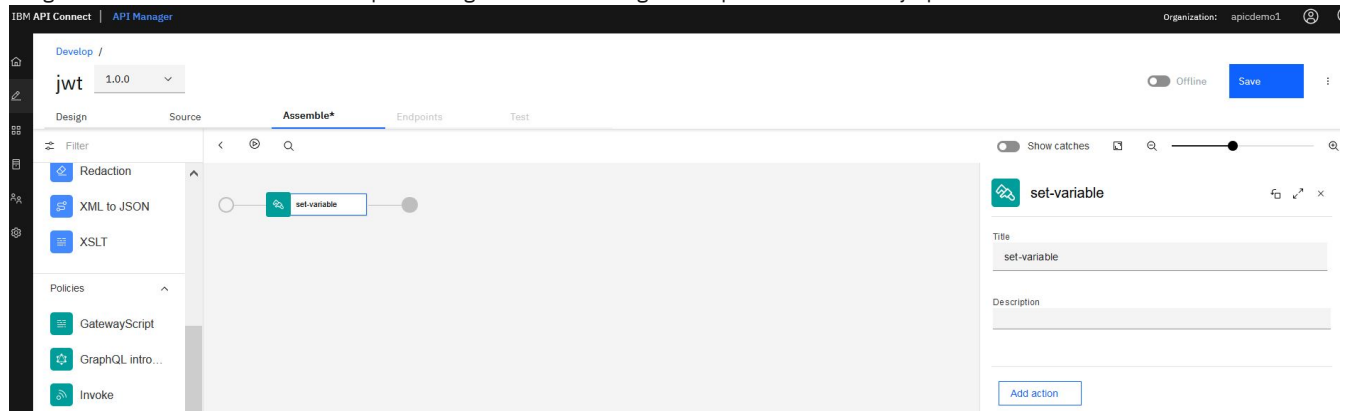
21. Click **Save**.
22. Click **Assemble**.



23. Hover the mouse over the existing **Proxy** or **Invoke** action and click the trash can icon to delete it.



24. Drag the **Set Variable** action onto the processing flow line. A configuration panel automatically opens.



25. Click **Add action** field.

26. Enter **hs256-key** in the **Set** field.

27. Select **string** in the **Type** field.

28. Enter a JWK in the **Value** field. Here is an example. `{ "alg": "HS256", "kty": "oct", "use": "sig", "k": "o5yErLaE-dbgVpSw65Rq570A9dHyaF66Q_Et5azPa-XUjbyP0w9iRWhR4kru09aFfQLXeIODIN4uhjE1YKXt8n76jt0Pjkd2pqk4t9abRF6tnL19GV4pflfL6uvVKkP4we0h39tqHt4TmkBgF2P-gFhgssZpjwq6l82fz3dUhQ2nkzoLA_CnyDGLZLd7SZ1yv73uzfE20t813zmig8KTMEMWVcWSDvy61F06vs_6LURcq_IEEevUiubBxG5S2aYHt95Siz0Qub0MN1T_X8F76wH7_A37GpKKJGqeaINWmHkgWdE8QWDQ", "kid": "hs256-key" }`

Action \*

Set, Add, or Clear a runtime variable.

Set

Set

The name of the variable to be set.

hs256-key

Type \*

The type of the value to set. This can be any, string, number or boolean.

string

Value

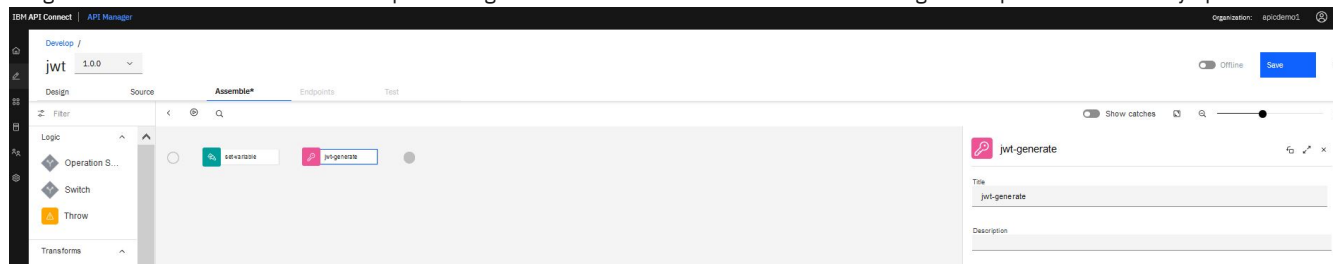
The value that the variable will be set to.

{ "alg": "HS256", "kty": "oct", "use": "sig", "k": "o5yErLaE-dbgVpSw65

29. Close the property panel. Click **Save**.

Cookie Preferences

30. Drag the **Generate JWT** action onto the processing flow line after the **set-variable** icon. A configuration panel automatically opens.



31. Enter `request.headers.iss-claim` in the **Issuer Claim** field.  
 32. Enter `request.headers.aud-claim` in the **Audience Claim** field.  
 33. Enter `hs256-key` in the **Sign JWK variable name** field.  
 34. Select **HS256** in the **Cryptographic Algorithm** field.

**Issuer Claim**  
Runtime variable from which the issuer (iss) claim string can be retrieved. This claim represents the Principal that issued the JWT.

`request.headers.iss-claim`

**Subject Claim**  
Runtime variable from which the Subject (sub) claim string can be retrieved.

**Audience Claim**  
Runtime variable from which the Audience (aud) claim string can be retrieved. Multiple variables are set via a comma-separated string.

`request.headers.aud-claim`

**Validity Period**  
The length of time (in seconds), that is added to the current date and time, in which the JWT is considered valid.

`3600`

**Private Claims**  
Runtime variable from which a valid set of JSON claims can be retrieved.

**Sign JWK variable name**  
Runtime variable containing the JWK to use to sign the JWT.

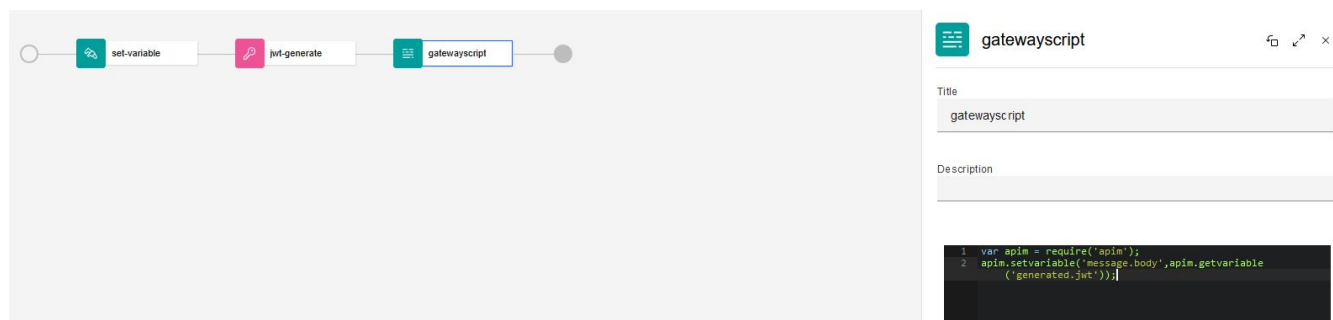
`hs256-key`

**Cryptographic Algorithm**  
Select a cryptographic algorithm.

`HS256`

35. Close the property panel. Click **Save**.  
 36. Drag the **GatewayScript** action onto the processing flow line after the Generate JWT icon. A configuration panel automatically opens.  
 37. Enter the following code:

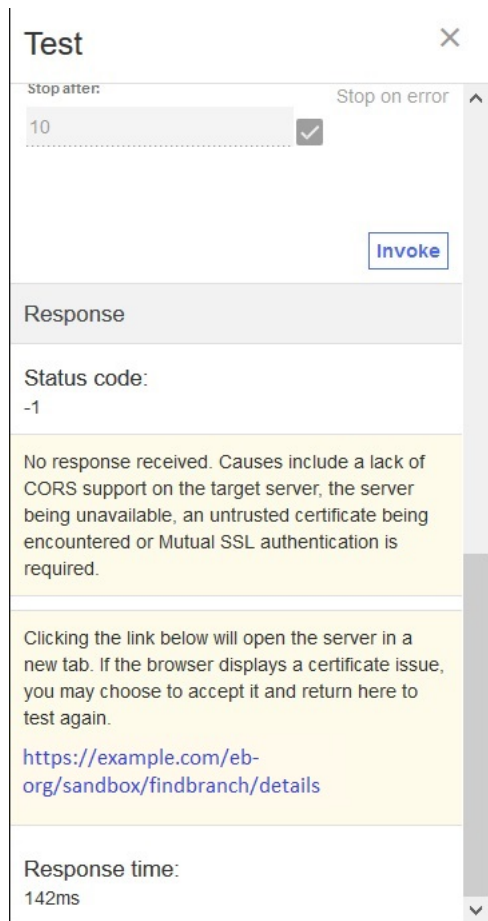
```
var apim = require('apim');
apim.setvariable('message.body', apim.getvariable('generated.jwt'));
```



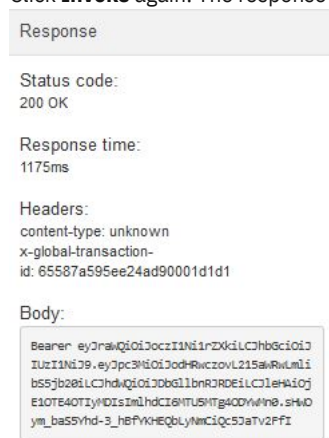
38. Close the property panel. Click **Save**.







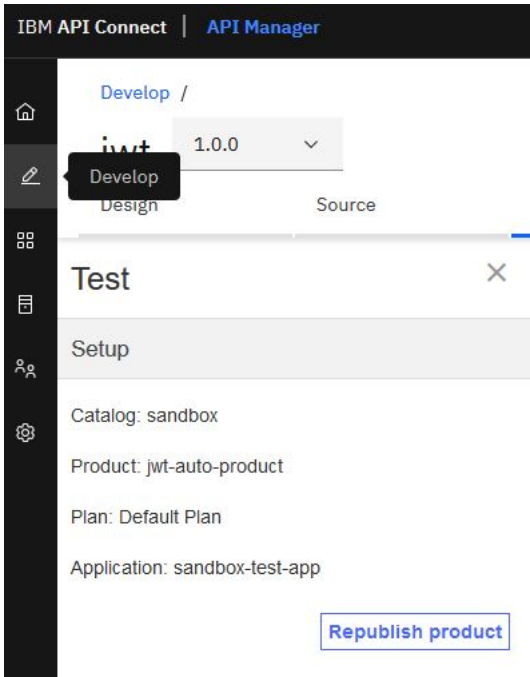
7. Click **Invoke** again. The response contains the generated JWT.




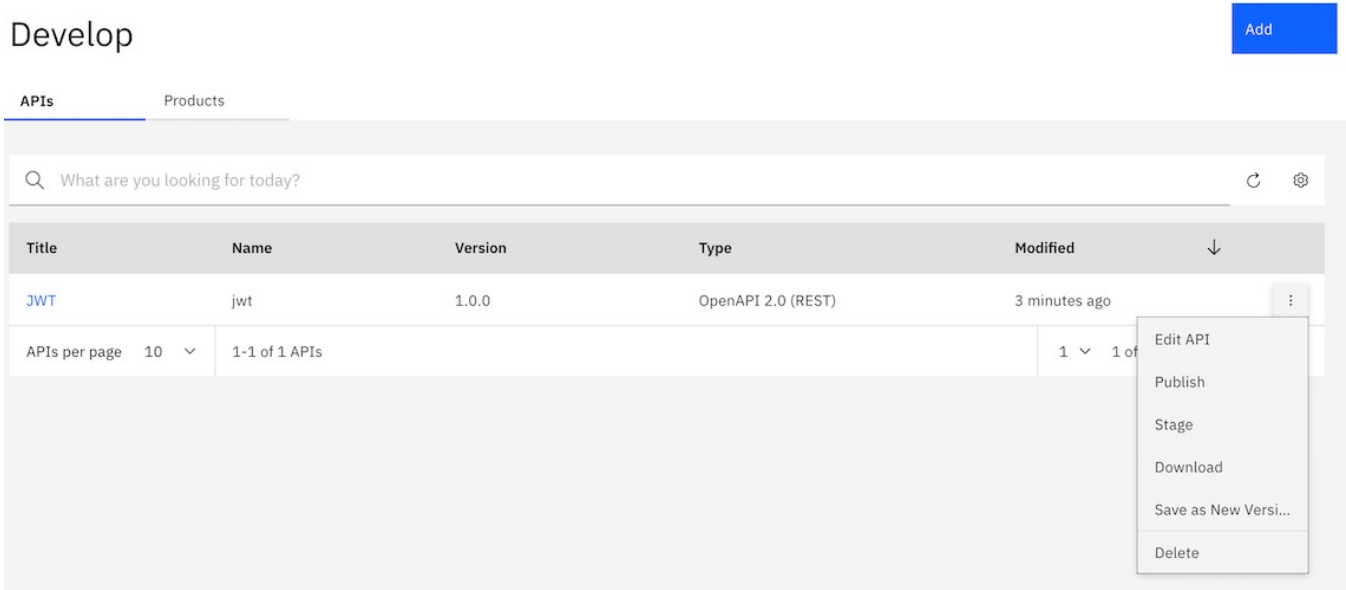
## Manage your API definition

Now that your new API works correctly, you can manage this API. To see your immediate options, take the following steps.

1. Click the **Develop** icon  on the navigation bar.



2. Click the **Options** icon  alongside the JWT API.



3. Select **Download**.

## What you did in this tutorial

In this tutorial, you completed the following activities:

- Created a new API definition that generates a JSON Web Token (JWT).
- Tested the new API.

**Parent topic:**

→ [API Manager tutorials](#)