IBM App Connect Enterprise with OAuth JWT authentication support

Contents

User Defined Policy in IBM App Connect Enterprise

IBM App Connect Enterprise does not bring OAuth JWT authentication out-of-the-box. This authentication is generally done on the API Management level like IBM API Connect, APIGEE, Kong, Tyk etc. Leveraging User Defined Policy along with a subflow (developed as a common utility in a library for reusability) brings the *experimental* feature to IBM ACE.

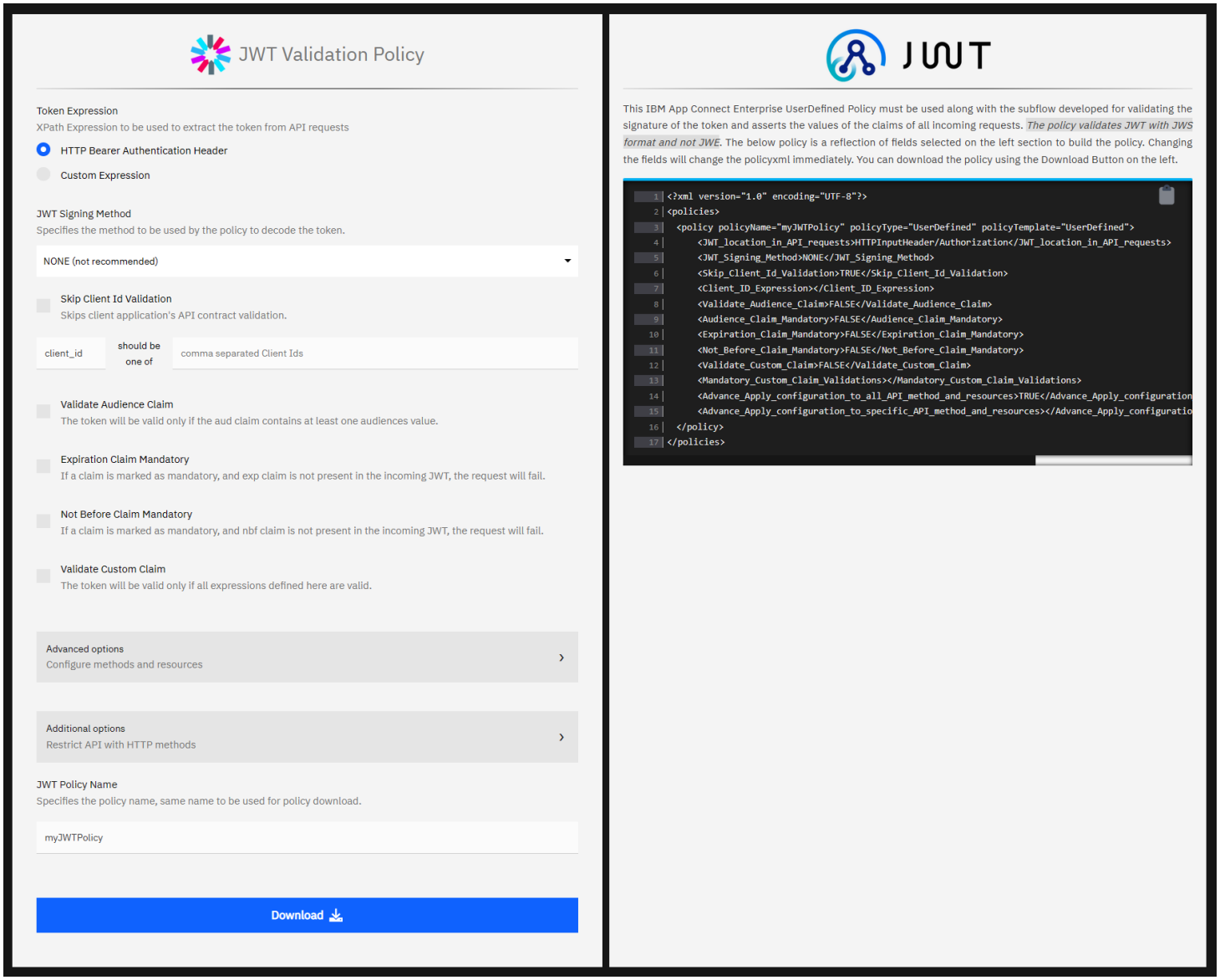
As per User Defined Policy documentation, a user defined policy has no predefined properties, so that you can define your own properties. Hence, custom fields are created which are read by the subflow for rule implementation.

It is easy to make humane mistakes while creating the policy xml manually (editing directly the policyxml file) however, to avoid such situation, a simple JWT policy builder Web GUI utility has been created. With this Web GUI utility, the policy is created instantly without any error since selecting values on the policy-builder form will enable only supported features and disable/hide unsupported feature. Let's have a look at the Web GUI utility.

JWT Policy Builder utility for IBM App Connect Enterprise

The below picture shows a glimpse of the Web GUI utility for User Defined Policy creation. The Web GUI is divided in two sections (i) Policy Builder Form on the left and (ii) User Policy generated view based on right.

Values selected on the Policy Builder Form will reflect live changes on the User Policy generated view. Let's understand the Policy Builder Form, its capabilities and possible values.



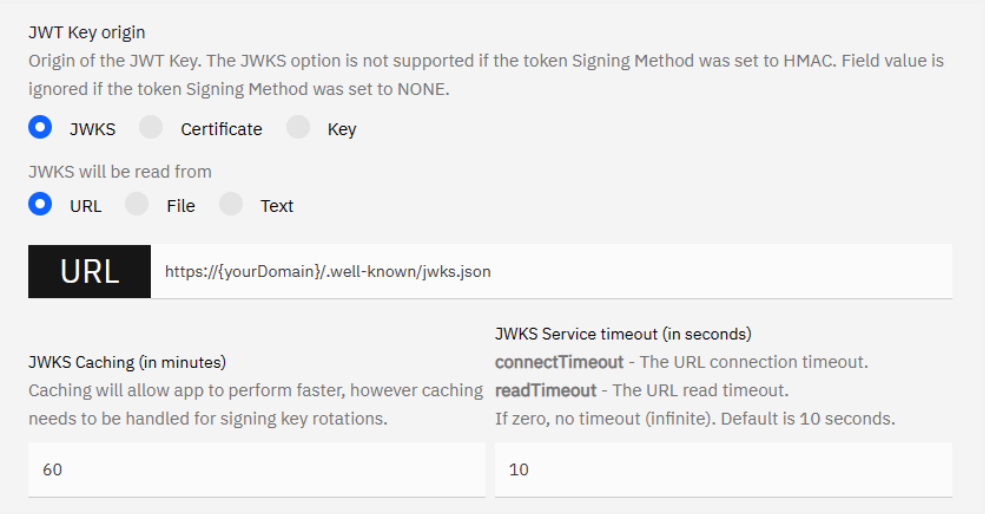
Policy Builder Form

Breaking down the Policy Builder Form to Segments.

JWT Origin
Token Expression XPath Expression to be used to extract the token from API requests (•) HTTP Bearer Authentication Header ( ) Custom Expression
Specifies from where in the request the JWT will be extracted: * HTTP Bearer Authentication Header * Custom Expression If you set this field to HTTP Bearer Authentication Header, the JWT is expected as Bearer (shown above). If you set this field to Custom Expression, provide an XPath expression that returns the token (shown below), adds a new Token Expression field in the form to provide the expression.
Token Expression XPath Expression to be used to extract the token from API requests ( ) HTTP Bearer Authentication Header (•) Custom Expression HTTPInputHeader/jwt

JWT Signing Method
JWT Signing Method Specifies the method to be used by the policy to decode the token. NONE (not recommended) RSA (256, 384, 512) PS (256, 384, 512) ED (EdDSA - Ed25519) ES (ECDSA 256, 284, 512) HMAC (256, 384, 512)
Specify the signing method expected in the incoming JWT from the Select options. The policy rejects the token if the JWT has a different signing method. Specifying the length of the key is not required.
If you select *NONE* as JWT Signing Method, the new segment *JWT Key origin* will be hidden.

JWT Key Origin

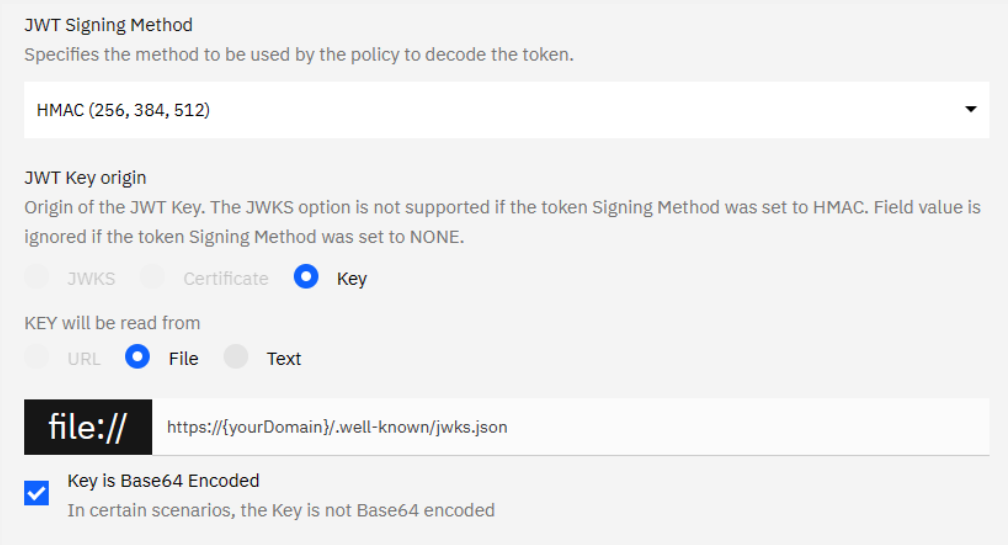


Specifies where to obtain the key for the Signature validation.

Key Origin	Source	Description
JWKS	URL	The URL to the JWKS server (recommended in most of the scenarios)
	File	The absolute path to the Certificate
	Text	Minified JWKS or JWK JSON pasted
Certificate	File	The absolute path to the .cer file
	Text	In-lined certificate (generally Base64 encoded) without ----BEGIN/END CERTIFICATE----
Key	File	The absolute path to the .pem file
	Text	In-lined Public Key (generally Base64 encoded) without ----BEGIN/END PUBLIC KEY----

If you select *NONE* as JWT Signing Method, the entire segment will be hidden.

If you select *HMAC* as JWT Signing Method, a new field will be added to mark if the Key provided is Base64 encoded or not. It will also disable *JWKS* and *Certificate* from Key Origin options and *URL* from Source options (shown below).

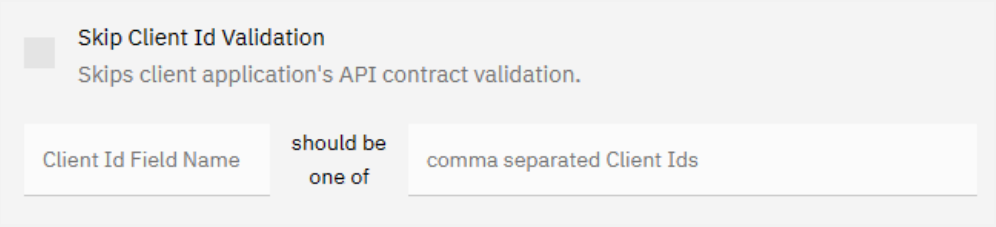


If you select JWT Signing Method apart from NONE and HMAC, and select JWKS as Key Origin and URL as Source, the JWKS Caching and JWKS Service timeout fields will be visible (otherwise hidden).

JWKS Caching (Time to Live) - This time field, in minutes, during which the policy is locally cached and considers the JWKS as valid. Caching will reduce the latency for fetching the JWKS again and again from the server. Retry mechanism is implemented to handle rotating signing keys.

JWKS Service connection timeout (seconds) - Sets the maximum time, in milliseconds, to wait for a response when authenticating the access token validation endpoint. The default value is 10 seconds.

Skip Client ID Validation



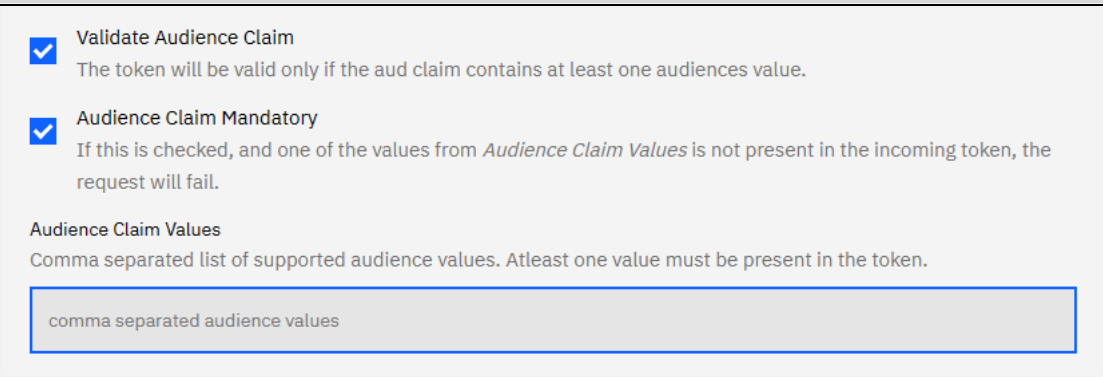
If you check this field, the policy does not verify that the client ID extracted from the JWT matches a valid client application of the API.

By default, *Skip Client Id Validation* is unchecked i.e., Client Id validation will be enforced.

Client ID Expression (the field below the check box) must be provided to enforce this policy criteria. Provide the *Client Id Field Name* from where the Client Id to be fetched (default value is set to *client_id* as specified in the Oauth 2.0 token exchange draft). The authorized Client Ids must be mentioned in the next field (multiple values can be written as comma separated values).

Check the *Skip Client Id Validation* field to stop client Id validation, this disables/hides the Client ID Expression field.

Validate Audience Claim

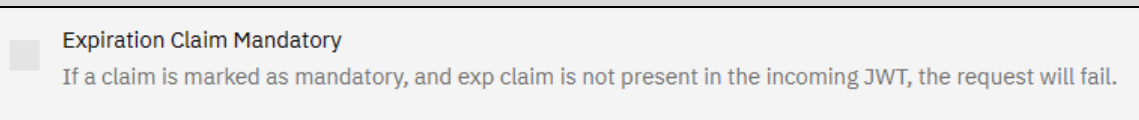


Validate Audience Claim check indicates that the policy should check for at least one audience to be present in the token however, the audience value is not validated.

You can set *Audience Claim Mandatory* if you want to validate the value mention in the *Audience Claim Expression* (multiple values can be written as comma separated values). At least one audience value must match with the token's audience claim.

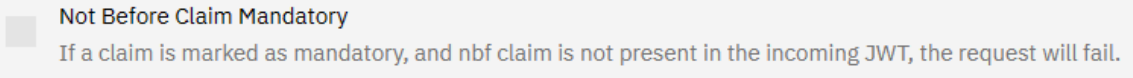
Validate Audience Claim is unchecked by default and hence, *Audience Claim Mandatory* and *Audience Claim Expression are disabled/hidden*. Checking *Validate Audience Claim* field will enable *Audience Claim Mandatory* and *Audience Claim Expression*.

Validate Audience Claim



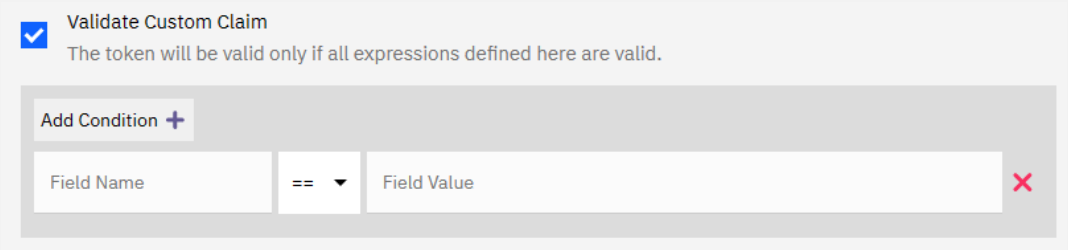
Indicates that the policy should check for the validity of the expiration claim. You can set this claim as "Mandatory" by selecting Expiration Claim Mandatory.

Validate Not Before Claim



Indicates that the policy should check for the validity of the Not Before claim. You can set this claim as "Mandatory" by selecting Not Before Claim Mandatory

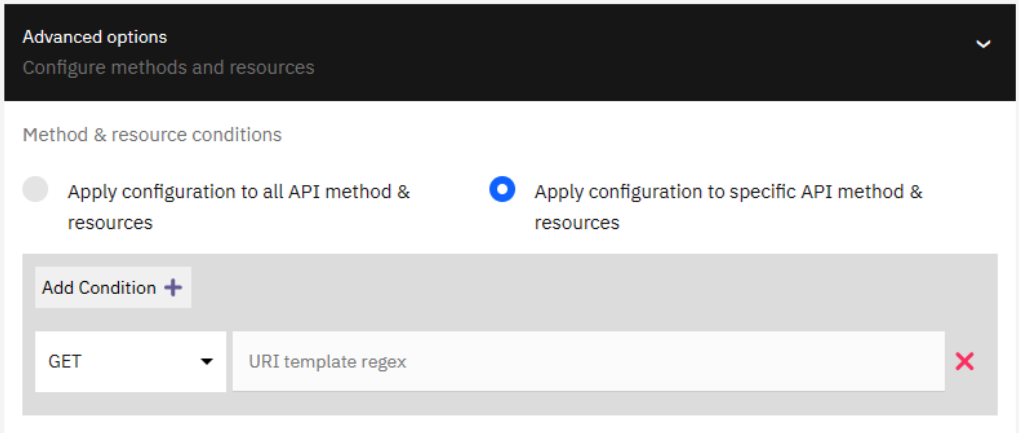
Validate Custom Claim



Enables the usage of custom validations in the policy. The JWT will be valid only if all the conditional expressions are fulfilled. Conditional operators supported are: equal (==), not equal (!=), greater than (>), less than (<), greater than or equal (>=), less than or equal (<=), in (IN an array – value must be supplied as comma separated), notin (NOT IN an array – value must be supplied as comma separated)

Conditions can be added or removed using + or ✕ buttons respectively. By default, *Validate Custom Claim* is unchecked. Conditions can be added only if *Validate Custom Claim* is checked.

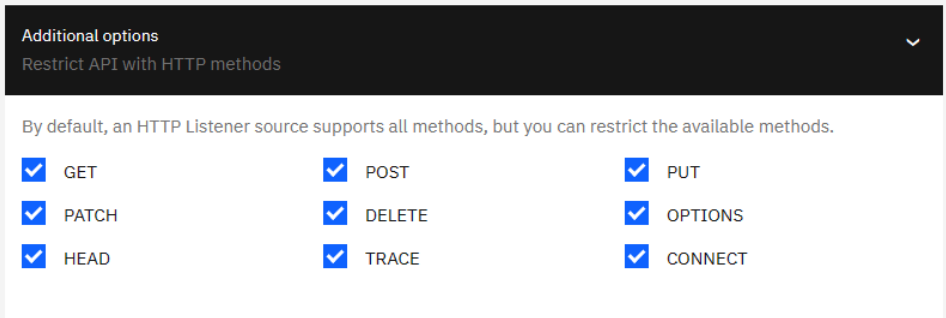
Advanced Options



This segment allows to specifically filter-in any URI that matches with the URI regular expression for applying the JWT policy. If the regular expression and HTTP Method doesn't match with the incoming HTTP(S) request, then the JWT policy will not be applicable.

Conditions can be added or removed using + or ✕ buttons respectively. By default, *Apply configuration to all API methods & resources* is selected. If *Apply configuration to specific API method & resources* is selected, then the condition expression segment is displayed, otherwise, disabled and hidden.

Additional Options



This segment allows to restrict any unwanted HTTP method invoking the API. By default, all methods are allowed. Uncheck the methods you want to restrict. If an API consumer invokes the API with invalid HTTP method, HTTP 405 Method Not Allowed will be replied along with the original request payload (if any).

Policy Name and Download

JWT Policy Name

Specifies the policy name, same name to be used for policy download.

myJWTPolicy

Download

Mention the policy name for the policy generated. The same policy name will be used to save the policyxml file when downloaded.

User Policy generated view

User Policy generated view

JWT

This IBM App Connect Enterprise UserDefined Policy must be used along with the subflow developed for validating the signature of the token and asserts the values of the claims of all incoming requests. *The policy validates JWT with JWS format and not JWE*. The below policy is a reflection of fields selected on the left section to build the policy. Changing the fields will change the policyxml immediately. You can download the policy using the Download Button on the left.

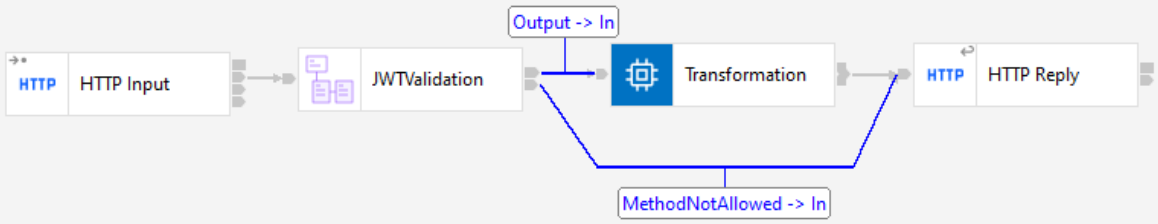
```
<?xml version="1.0" encoding="UTF-8"?>
<policies>
  <policy policyName="myJWTPolicy" policyType="UserDefined" policyTemplate="UserDefined">
      <JWT_location_in_API_requests>HTTPInputHeader/Authorization</JWT_location_in_API_requests>
      <JWT_Signing_Method>RSA</JWT_Signing_Method>
      <JWT_Key_origin>JWKS</JWT_Key_origin>
      <JWKS_URL_or_Key>https://{yourDomain}/.well-known/jwks.json</JWKS_URL_or_Key>
      <JWKS_Caching_TTL>60</JWKS_Caching_TTL>
      <JWKS_Service_connection_timeout>10</JWKS_Service_connection_timeout>
      <Skip_Client_Id_Validation>TRUE</Skip_Client_Id_Validation>
      <Client_ID_Expression></Client_ID_Expression>
      <Validate_Audience_Claim>FALSE</Validate_Audience_Claim>
      <Audience_Claim_Mandatory>FALSE</Audience_Claim_Mandatory>
      <Expiration_Claim_Mandatory>FALSE</Expiration_Claim_Mandatory>
      <Not_Before_Claim_Mandatory>FALSE</Not_Before_Claim_Mandatory>
      <Validate_Custom_Claim>FALSE</Validate_Custom_Claim>
      <Mandatory_Custom_Claim_Validations></Mandatory_Custom_Claim_Validations>
      <Advance_Apply_configuration_to_all_API_method_and_resources>TRUE</Advance_Apply_configuration
      <Advance_Apply_configuration_to_specific_API_method_and_resources></Advance_Apply_configuratio
  </policy>
</policies>
```

This segment shows the policy generated based on the values selected in the Policy Builder Form. You can copy-to-clipboard the policy generated or use the download button below the Policy Builder form to download the policy.

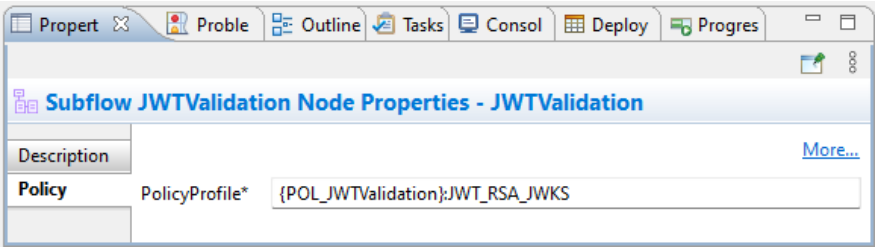
JWT Policy usage in IBM App Connect Enterprise

Let us design a simple application which will be JWT protected. The message flow (shown below) uses the JWTValidation sublow. The only configuration for this subflow is the JWT policy that was developed using the Web GUI utility.

Application using JWTValidation



JWTValidation subflow configuration



JWT validation manual testing using valid and tampered tokens

Testing with Valid token - SUCCESSFUL

Send Request

```
POST http://localhost:7800/myjwtvalidator HTTP/1.1
Content-Type: application/json
Authorization: Bearer {{RSA256}}

{
    "firstName": "Dipanjan",
    "lastName": "Das"
}
```

```
1  HTTP/1.1 200 OK
2  Content-Type: application/json;charset=utf-8
3  Server: ACEISD10_HTTP
4  Date: Mon, 08 May 2023 17:14:51 GMT
5  Content-Length: 27
6  Connection: close
7
8  {
9    "fullName": "Dipanjan Das"
10 }
```

Testing with Invalid token - FAILED

Send Request

```
POST http://localhost:7800/myjwtvalidator HTTP/1.1
Content-Type: application/json
Authorization: Bearer {{RSA256Tampered}}

{
    "firstName": "Dipanjan",
    "lastName": "Das"
}
```

```
1  HTTP/1.1 500 Internal Server Error
2  Content-Type: application/json;charset=utf-8
3  X-Original-HTTP-Status-Code: 500
4  Server: ACEISD10_HTTP
5  Date: Mon, 08 May 2023 17:17:47 GMT
6  Content-Length: 855
7  Connection: close
8
9  {
10   "error": {
11     "code": 500,
12     "status": "Internal Server Error",
13     "detail": "BIP2230E: Error detected whilst processing a message in node 'com.dev.t
   est.MyMessageFlow.JWTValidation.JWTValidation'. \nBIP4367E: The method 'evaluate' in J
   ava node 'JWTValidation.JWTValidation' has thrown the following exception: <com.ibm.br
   oker.plugin.MbUserException class:com.dev.jwt.JWTValidation method:evaluate() source:
   key: message: Unable to resolve message: Source: Key:  >. \nBIP4394E: Java exception:
   'com.ibm.broker.plugin.MbUserException'; thrown from class name: 'com.dev.jwt.JWTValid
   ation', method name: 'evaluate()', file: 'JWTValidation.java', line: '262'; trace tex
   t: 'java.security.GeneralSecurityException: Signature check failed.';  resource bundl
   e: ''; key: ''; inserts(optional): '{8}', '{9}', '{10}', '{11}', '{12}', '{13}', '{1
   4}', '{15}', '{16}', '{17}' "
14   }
15 }
```

[WT validation automation testing (93 test cases)]

Workspace: **Dipanjan's Workspace** | Projects | API Tests | JWT_Testing | Environments | Mock Servers | Monitors | Flows | Collections | Apis | Integrations | Settings | Help | Invite | Upgrade | Sign In

JWT_Testing / Test Validation

Save | Share | Run | Comments | Documentation | Cookies | Code | Settings

JWT_Testing - Run results

Running JWT_Testing

Stop Agent | Schedule Run | Run Again | Automate Run | Share Run | Export Results

Iterations	Environment	Iterations	Duration	Avg. Resp. Time
Random	none	93	1m 28s	2245 ms

All Tests | Passed (93) | Failed (0) | Skipped (0) | **View Summary**

Iteration 1

GET validation
http://localhost:8080/getvalidation

Pass | Res. Time is well < 200ms | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 2

GET validation
http://localhost:8080/getvalidation

Pass | Res. Time is well < 200ms | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 3

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 4

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 5

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 6

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 7

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 8

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 9

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 10

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 11

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 12

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 13

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 14

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 15

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 16

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 17

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 18

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 19

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 20

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 21

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 22

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 23

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 24

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 25

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 26

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 27

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 28

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 29

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 30

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 31

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 32

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 33

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 34

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 35

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 36

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 37

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 38

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 39

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 40

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 41

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 42

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 43

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 44

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 45

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 46

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 47

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 48

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 49

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 50

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 51

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 52

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 53

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 54

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 55

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 56

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 57

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 58

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 59

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 60

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 61

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 62

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 63

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 64

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 65

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 66

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 67

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 68

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 69

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 70

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 71

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 72

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 73

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 74

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 75

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 76

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 77

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 78

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 79

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 80

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 81

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 82

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 83

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 84

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 85

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 86

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 87

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 88

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 89

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 90

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 91

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 92

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB

Iteration 93

POST validation
http://localhost:8080/postvalidation

Pass | Test - Valid JWT Signature & JWT_EXAM_JWKS policy | 200 OK | application/text | text/plain | 1 ms | 1.00KB | 200 | Internal Server Error | 0 ms | 0.00 KB