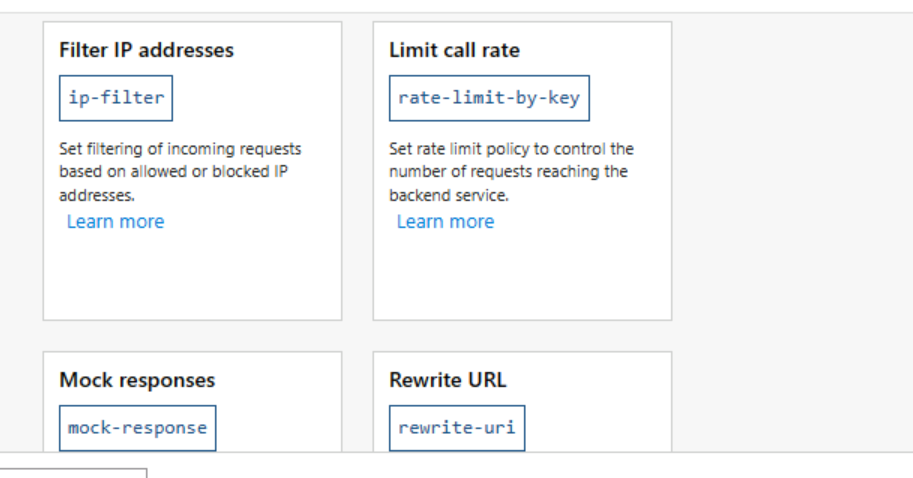
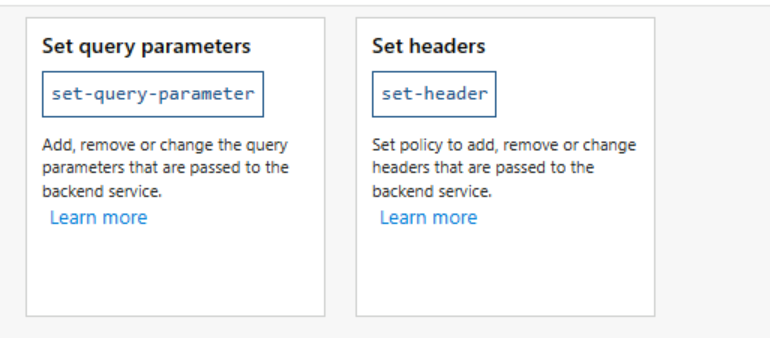
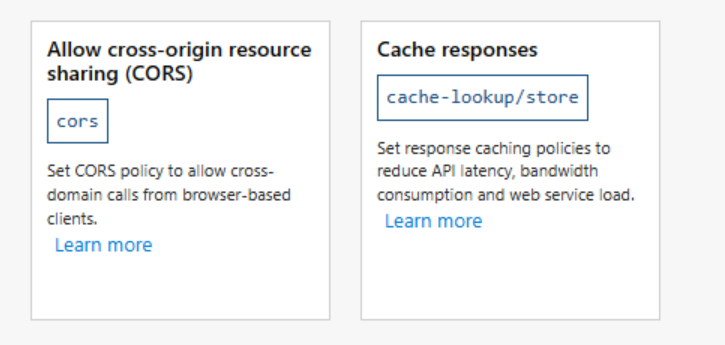
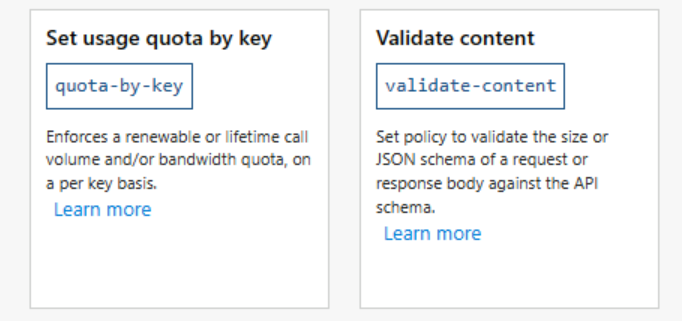


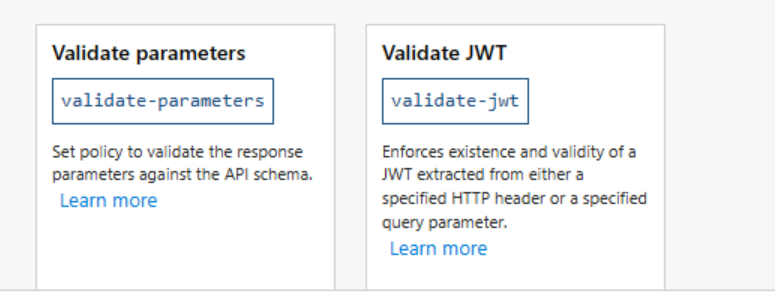
Add inbound policy



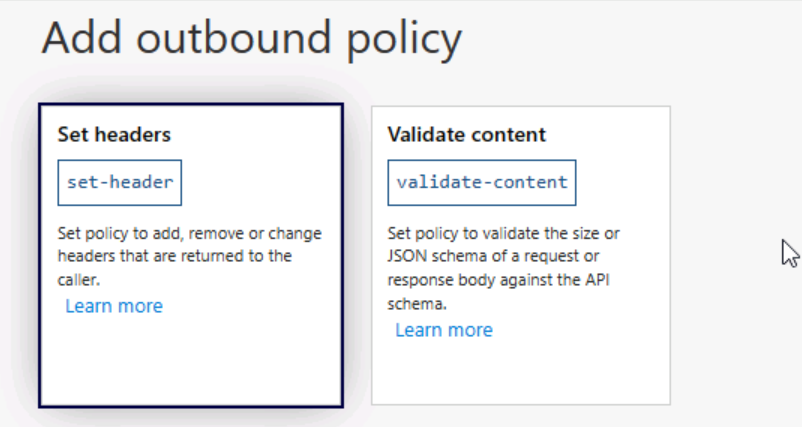


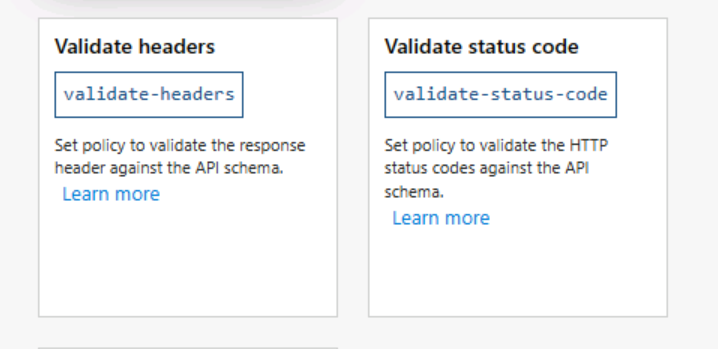


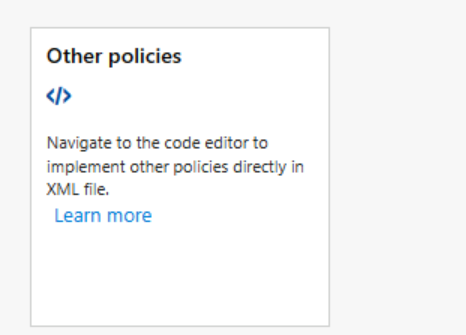




Outbound Policy







Header name

Ocp-Apim-Subscription-Key

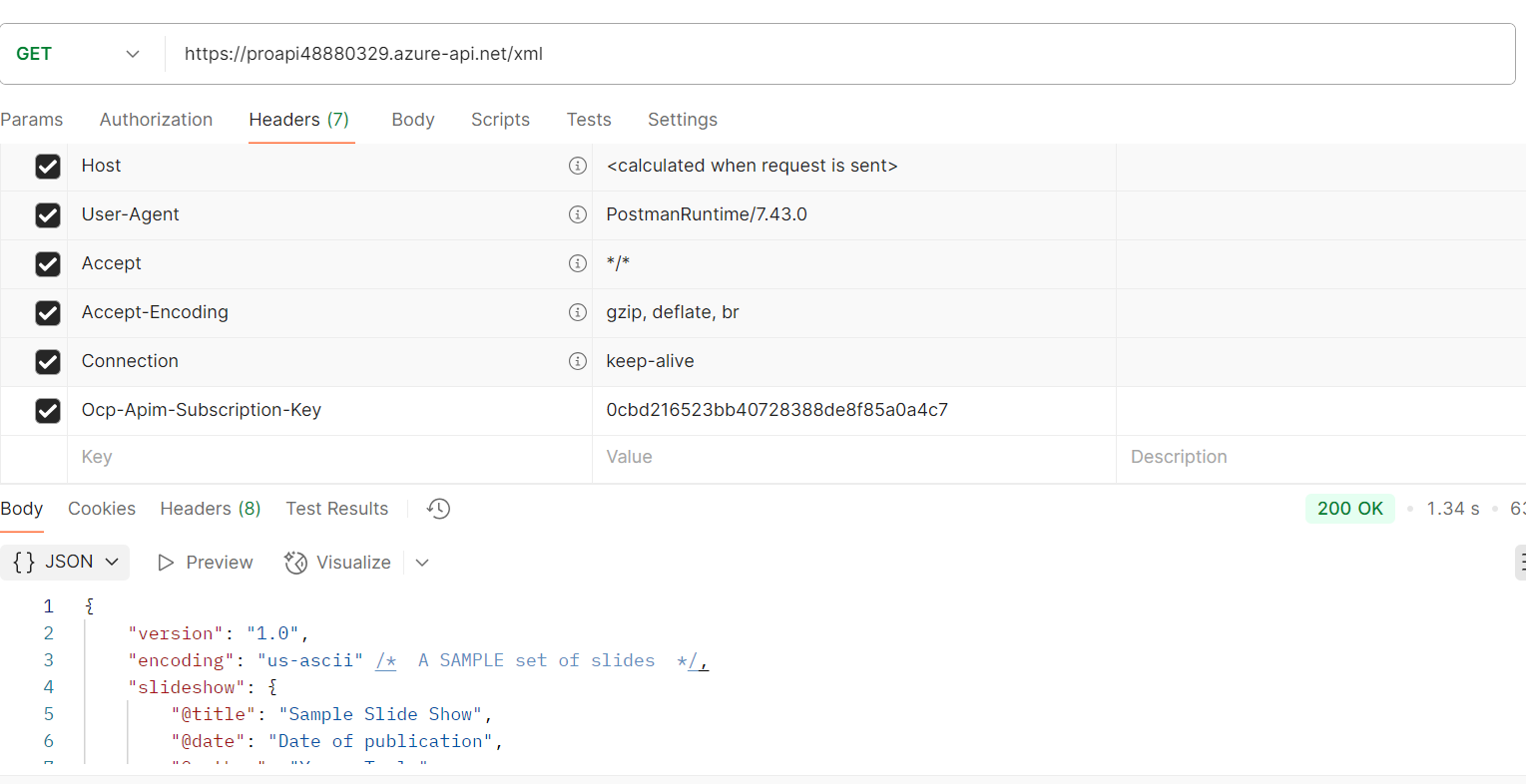
Query parameter name

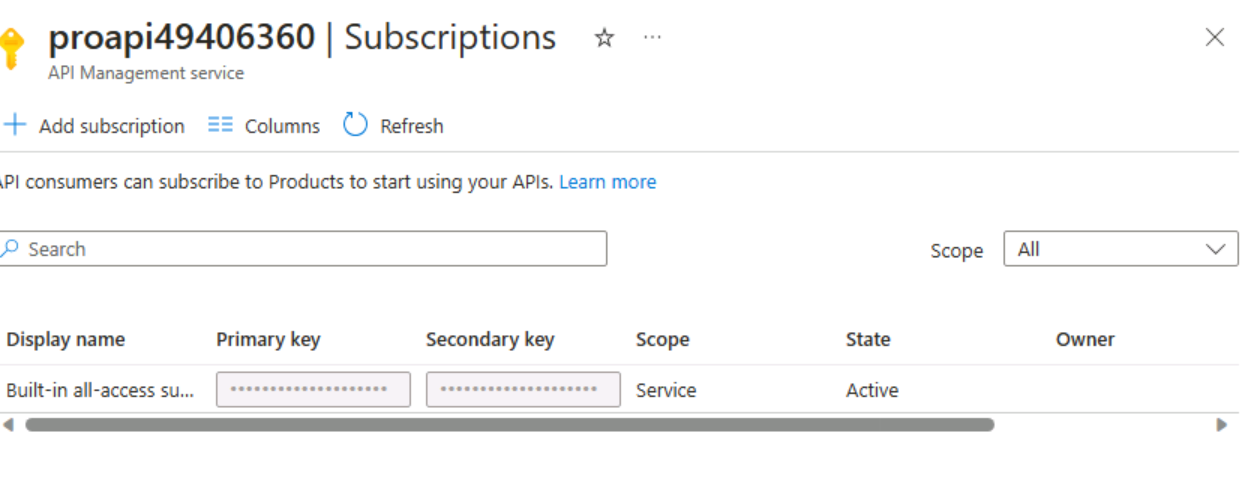
subscription-key

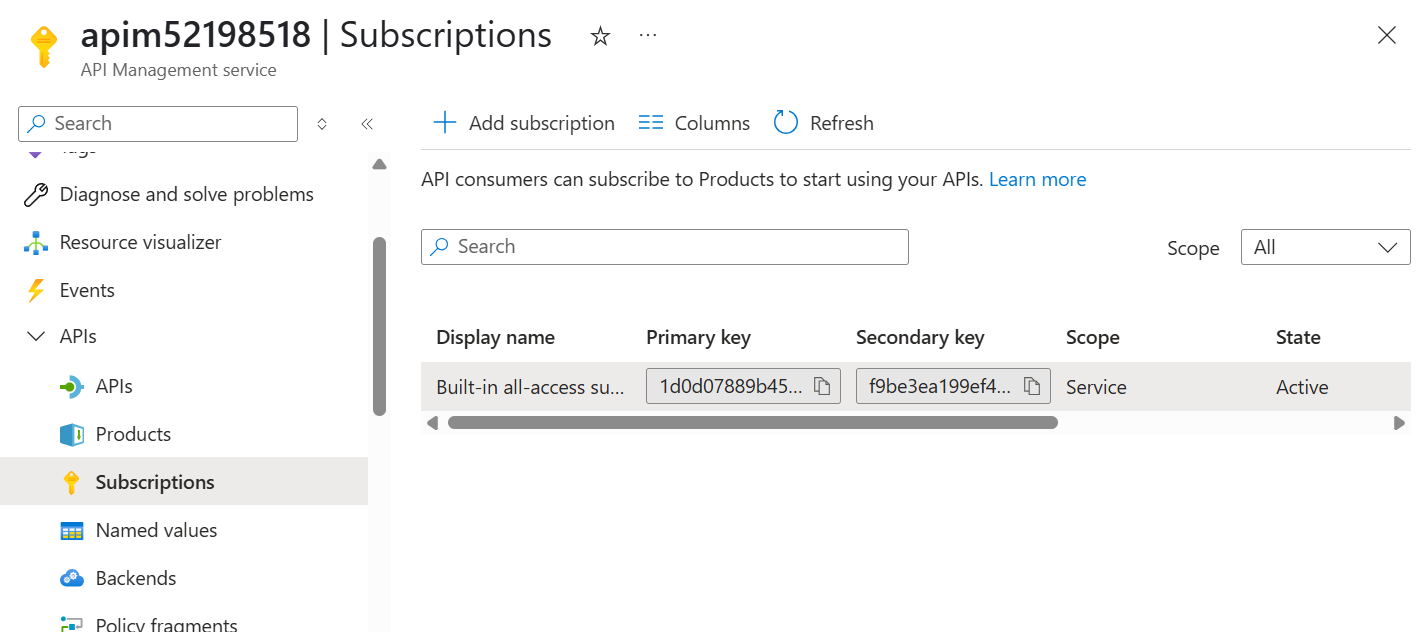
"Ocp-Apim-Subscription-Key": "0cbd216523bb40728388de8f85a0a4c7",

{ "headers": { "Accept": "\*/\*", "Accept-Encoding": "gzip,deflate,br", "Accept-Language": "en-US,en;q=0.9", "Cache-Control": "no-cache, no-store", "Client-Ip": "20.241.180.81:19649", "Disguised-Host": "httpapi48880329-deczadbtbvdrejak.eastus-01.azurewebsites.net", "Host": "httpapi48880329-deczadbtbvdrejak.eastus-01.azurewebsites.net", "Max-Forwards": "8", "Ocp-Apim-Subscription-Key": "0cbd216523bb40728388de8f85a0a4c7", "Referer": "https://apimanagement.hosting.portal.azure.net/", "Sec-Ch-Ua": "\"Not\_A Brand\";v=\"8\",\"Chromium\";v=\"120\",\"Microsoft Edge\";v=\"120\"", "Sec-Ch-Ua-Mobile": "?0", "Sec-Ch-Ua-Platform": "\"Windows\"", "Sec-Fetch-Dest": "empty", "Sec-Fetch-Mode": "cors", "Sec-Fetch-Site": "cross-site", "Source": "azure-api-mgmt", "Was-Default-Hostname": "httpapi48880329-deczadbtbvdrejak.eastus-01.azurewebsites.net", "X-Appservice-Proto": "https", "X-Arr-Log-Id": "910bf527-1e09-485f-b0c9-f78047f3961f", "X-Arr-Ssl": "2048|256|CN=Microsoft Azure RSA TLS Issuing CA 08, O=Microsoft Corporation, C=US|CN=\*.azurewebsites.net, O=Microsoft Corporation, L=Redmond, S=WA, C=US", "X-Client-Ip": "20.241.180.81", "X-Client-Port": "19649", "X-Forwarded-Tlsversion": "1.2", "X-Original-Url": "/headers", "X-Site-Deployment-Id": "httpapi48880329", "X-Waws-Unencoded-Url": "/headers" } }

<https://proapi48880329.azure-api.net/xml?subscription-key=0cbd216523bb40728388de8f85a0a4c7>

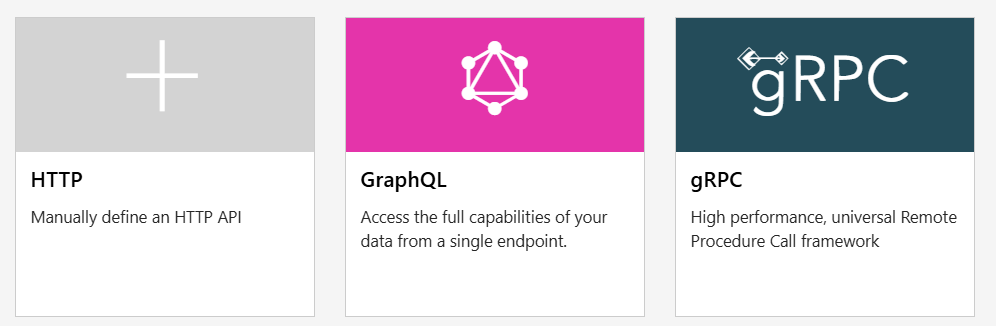


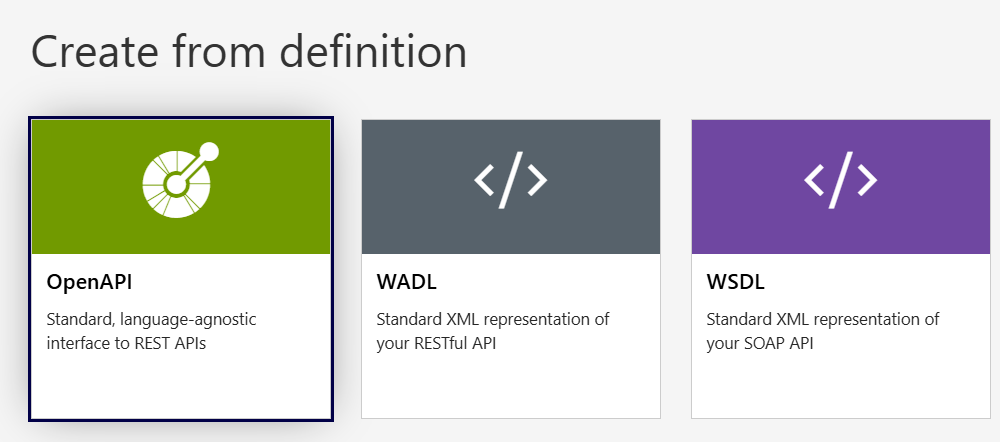


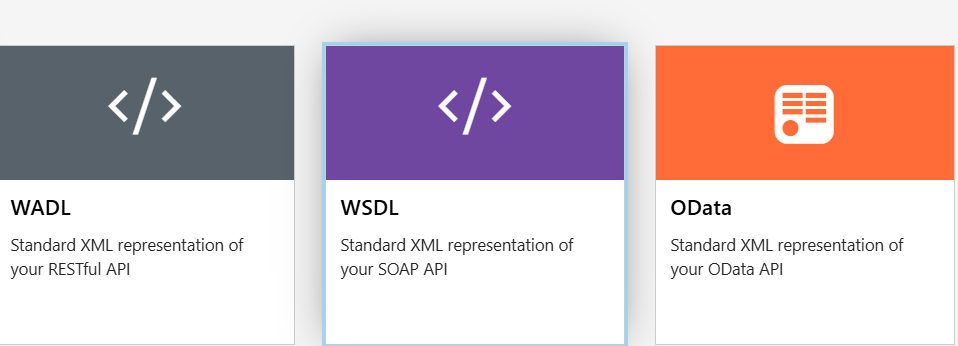


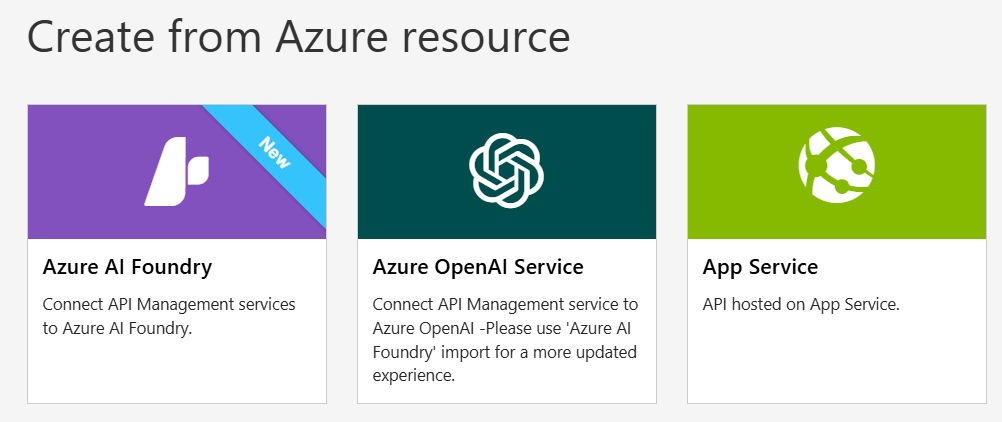
1d0d07889b4540d497695c4228bdb1b0

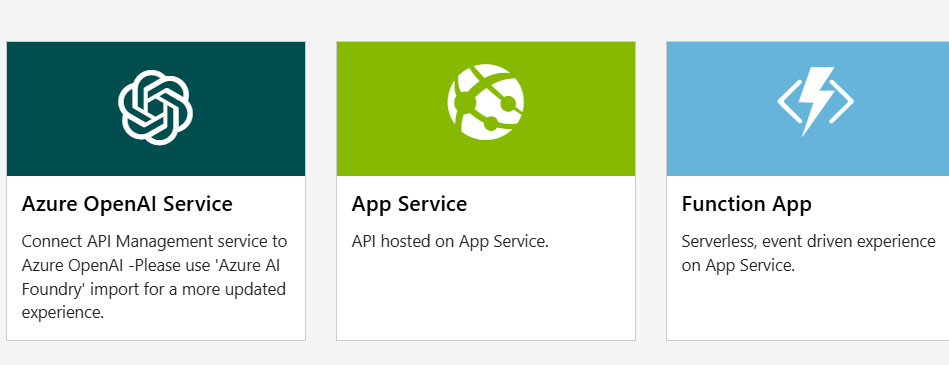
|  |  |
| --- | --- |
| **Web service URL** text box | Enter the URL for the web app that you copied earlier in this lab. **Note**: Make sure that the URL starts with the https:// prefix  Web service url is the url of azure app service web app.  <https://httpapi51968293-bthwase2dqdxg8cr.eastus-01.azurewebsites.net/> |

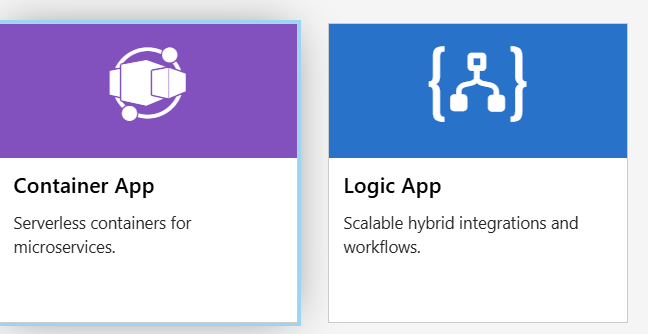




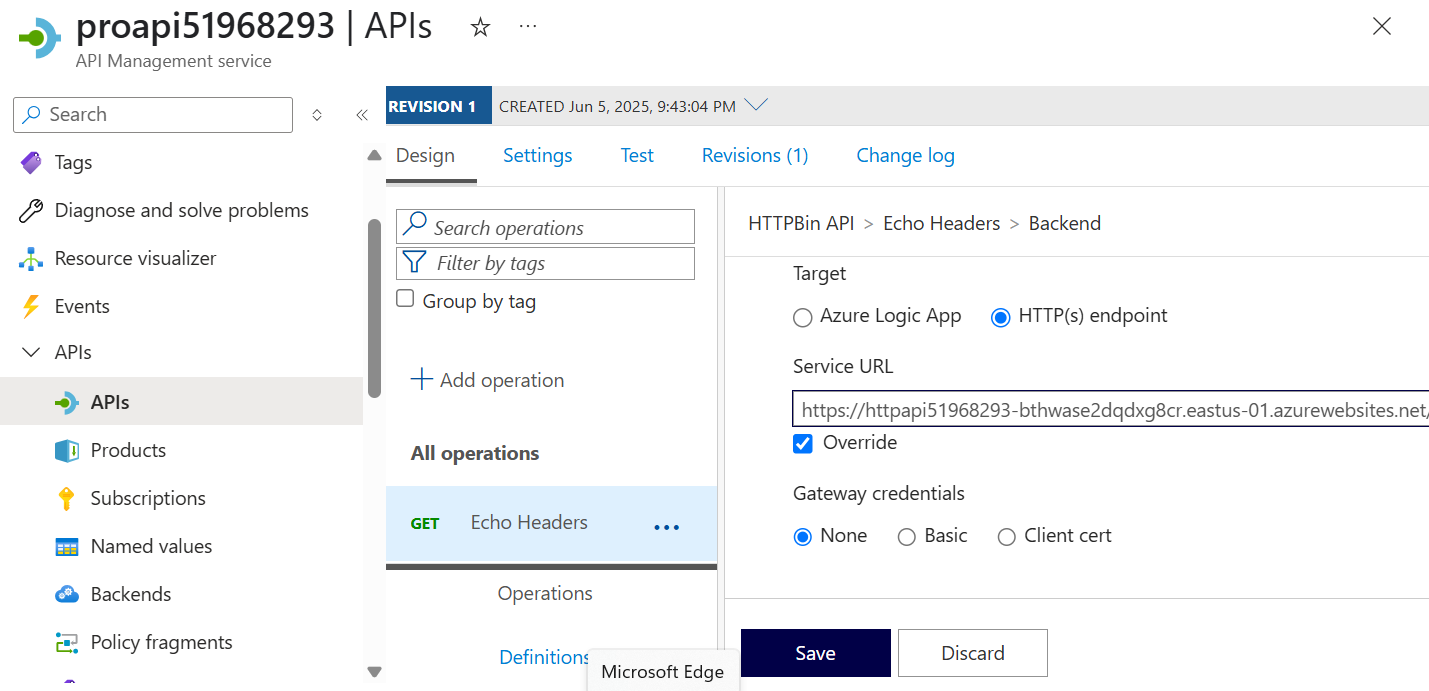


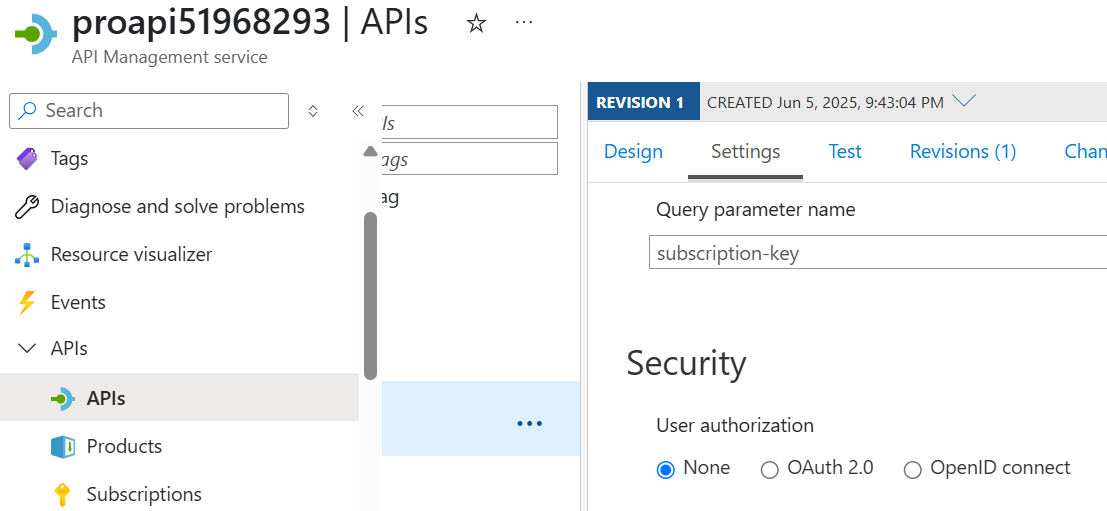






|  |  |
| --- | --- |
| **Access Type** | Select **Public** |
| **Registry server URL** | https://index.docker.io |
| **Image and tag** text box | enter kennethreitz/httpbin:latest |





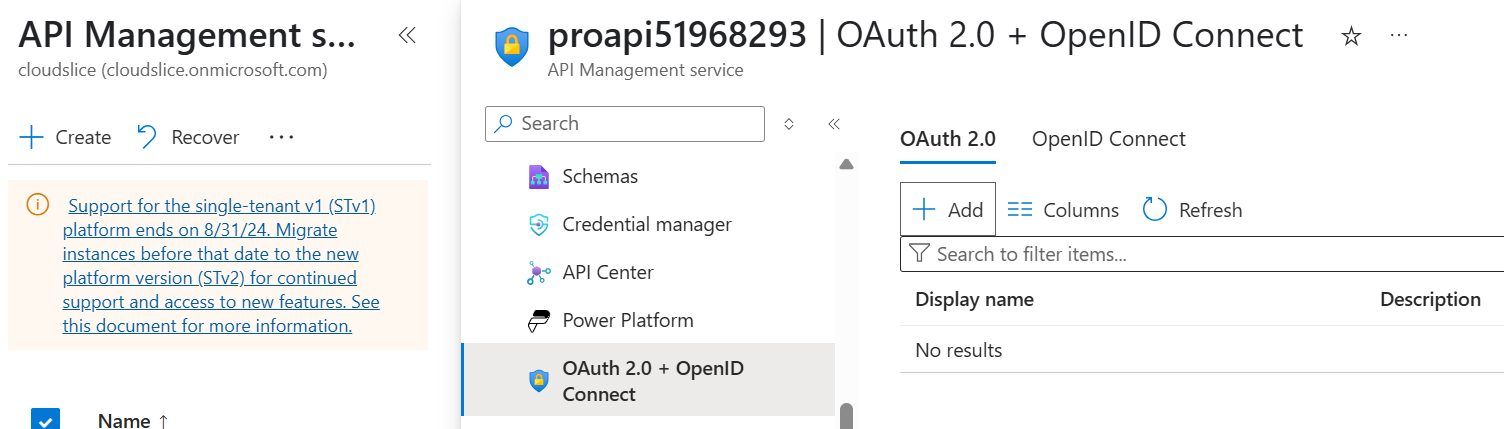
In [Azure API Management](https://www.google.com/search?sca_esv=ee5c04314dac669e&cs=0&q=Azure+API+Management&sa=X&ved=2ahUKEwiJjbW729qNAxUcUGcHHQPIMVMQxccNegQIBBAB&mstk=AUtExfAMRcgZHj3o3NCodlHcjk1G_R2jWLpdSLxqA7O9LLYzuHO7ggl6lD3P4LnjEgiBEV6WE5J1ftKGSFl5nMi9UirDFmGllYQO1kEcEM-Pwbqk8GCfbsXncmKyl2Y5L4XLqfA&csui=3), the inbound process refers to actions taken on a request before it's sent to the backend service, while the outbound process refers to actions taken on a response before it's sent back to the client. These processes are managed through policies configured within the API Management instance.

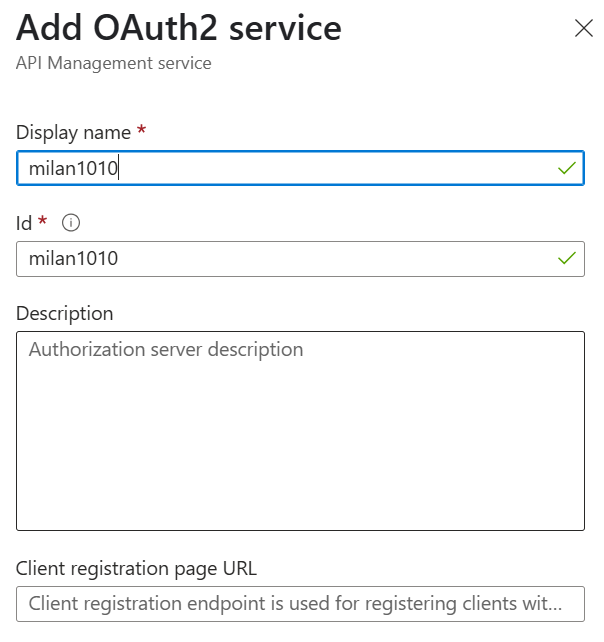
Inbound Processing:

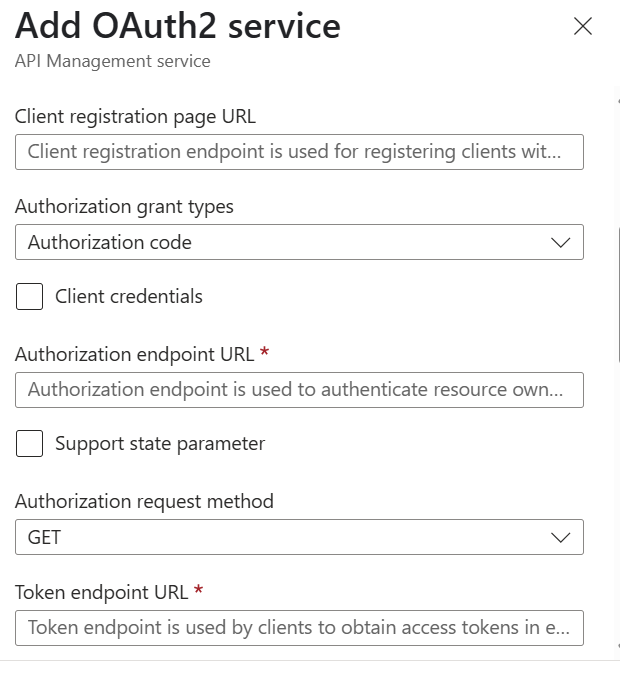
* **Purpose:** To modify or validate incoming requests before forwarding them to the backend service.
* **Examples:**
  + Adding or modifying request headers.
  + Validating API keys or tokens.
  + Enforcing rate limits or quotas.
  + Applying transformation policies (e.g., converting XML to JSON).
* **Policies:** Policies are applied within the "Inbound" section of the API's design.

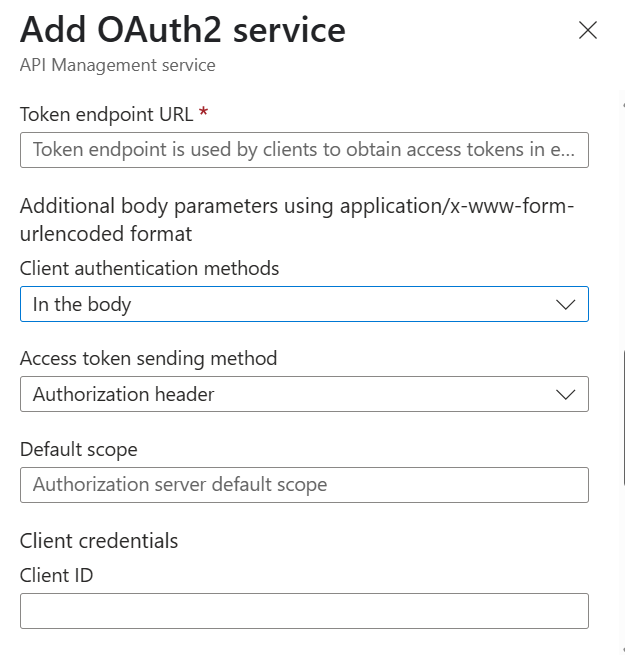
Outbound Processing:

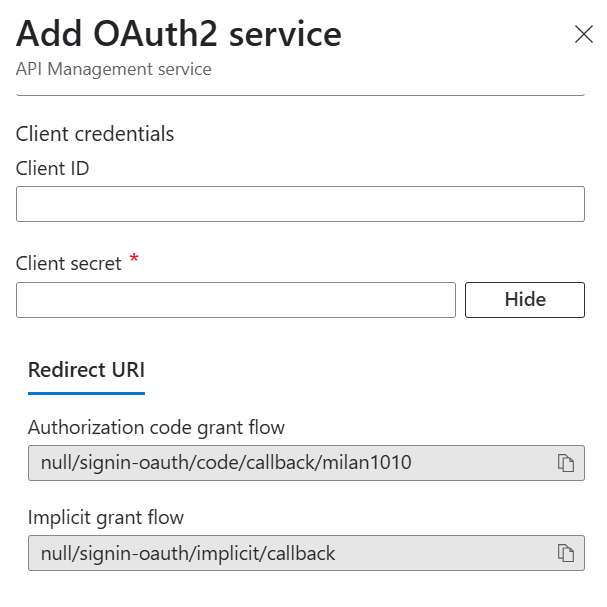
* **Purpose:** To modify or transform the response from the backend service before sending it back to the client.
* **Examples:**
  + Adding or modifying response headers.
  + Applying transformation policies (e.g., converting JSON to XML).
  + Caching responses.
  + Handling errors.

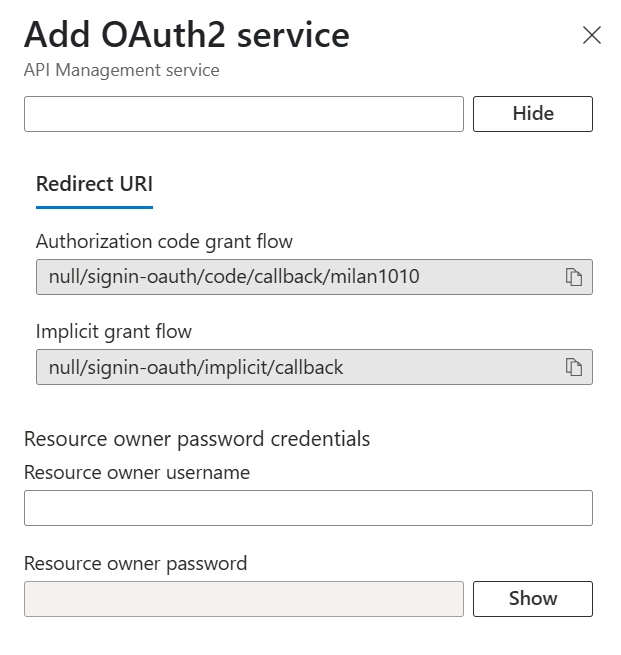


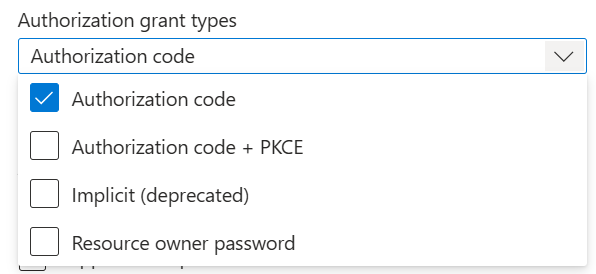


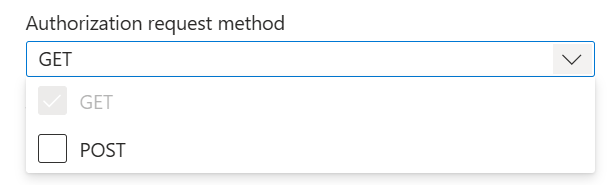












In client authentication, "in a body" and "Body" both refer to the transmission of authentication credentials in the request body, not the header. "Basic" authentication is a separate method where credentials are sent in the Authorization header, often base64 encoded.

"In a body" or "Body" authentication refers to passing authentication information (like username/password or client ID/secret) directly within the HTTP request body, as parameters in the payload.

[Basic authentication](https://www.google.com/search?sca_esv=ee5c04314dac669e&cs=0&q=Basic+authentication&sa=X&ved=2ahUKEwjr6s3V39qNAxXaR2wGHfRGL6gQxccNegQIExAB&mstk=AUtExfD7ezr7fY9Liccyv7a3sWxSs1AR41C85iNYulDGqqDkyZzgjSAW_z055tW-0nSY7pL__991QB-mD2-AkpQSwTcE9QxA8pWU-cSq3zRV1lDOA-eIWZBhUXyQK9TSJcPd9ZE&csui=3), on the other hand, sends the credentials as part of the [Authorization header](https://www.google.com/search?sca_esv=ee5c04314dac669e&cs=0&q=Authorization+header&sa=X&ved=2ahUKEwjr6s3V39qNAxXaR2wGHfRGL6gQxccNegQIExAC&mstk=AUtExfD7ezr7fY9Liccyv7a3sWxSs1AR41C85iNYulDGqqDkyZzgjSAW_z055tW-0nSY7pL__991QB-mD2-AkpQSwTcE9QxA8pWU-cSq3zRV1lDOA-eIWZBhUXyQK9TSJcPd9ZE&csui=3).

basic authentication.

Authorization: Basic YWJkMTIzNDU2Nzg5QDEyMy4xMjMuMTIzMTIz

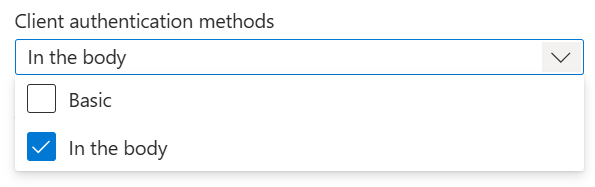
body authentication.

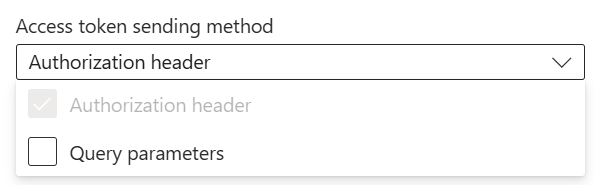
POST /login HTTP/1.1

Content-Type: application/x-www-form-urlencoded

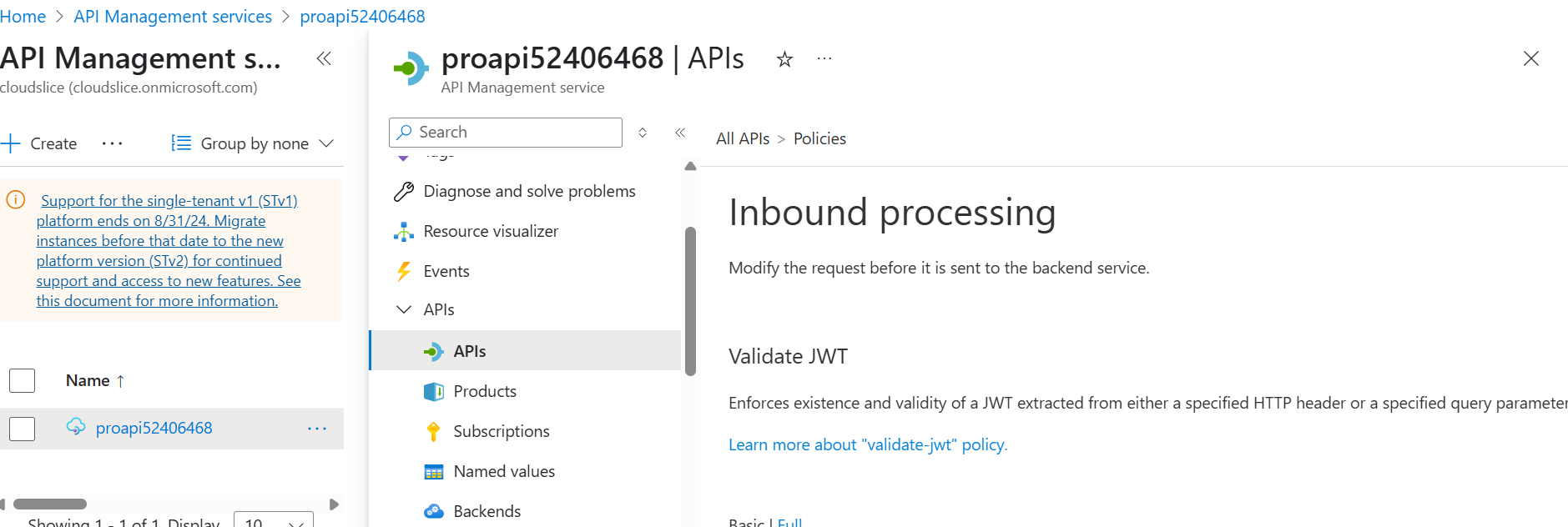
Content-Length: 36

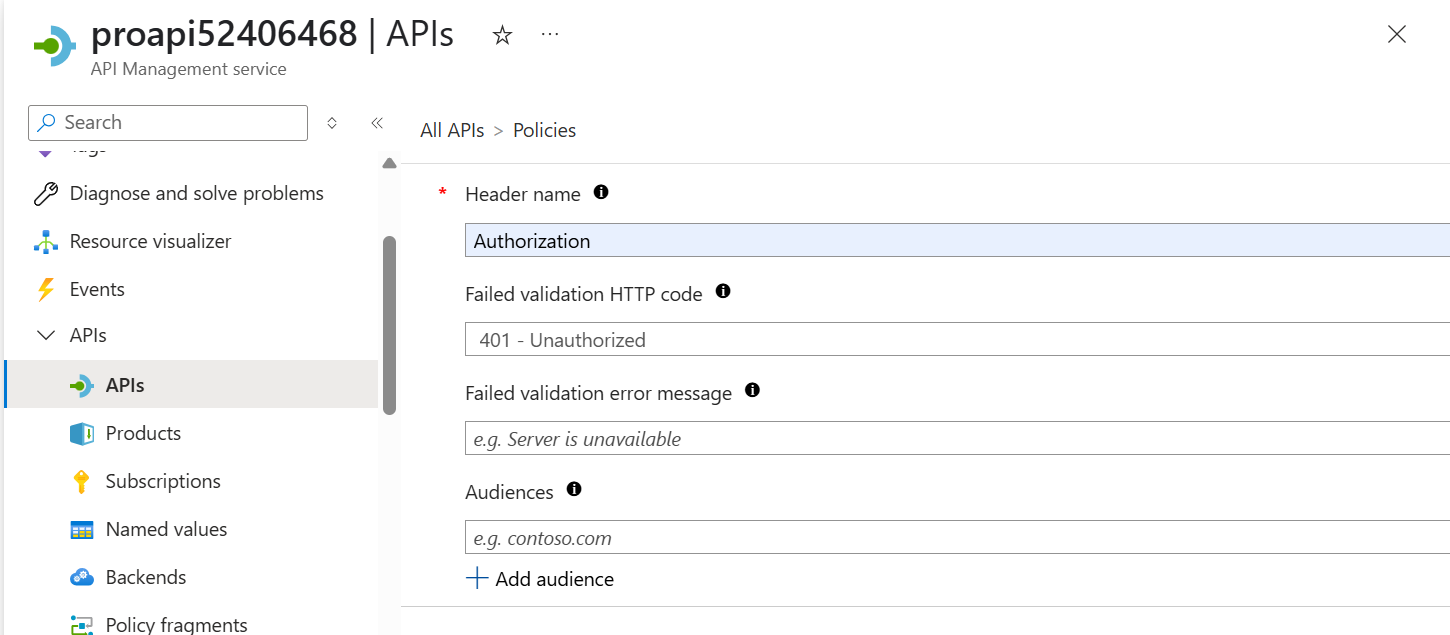
username=testuser&password=testpassword

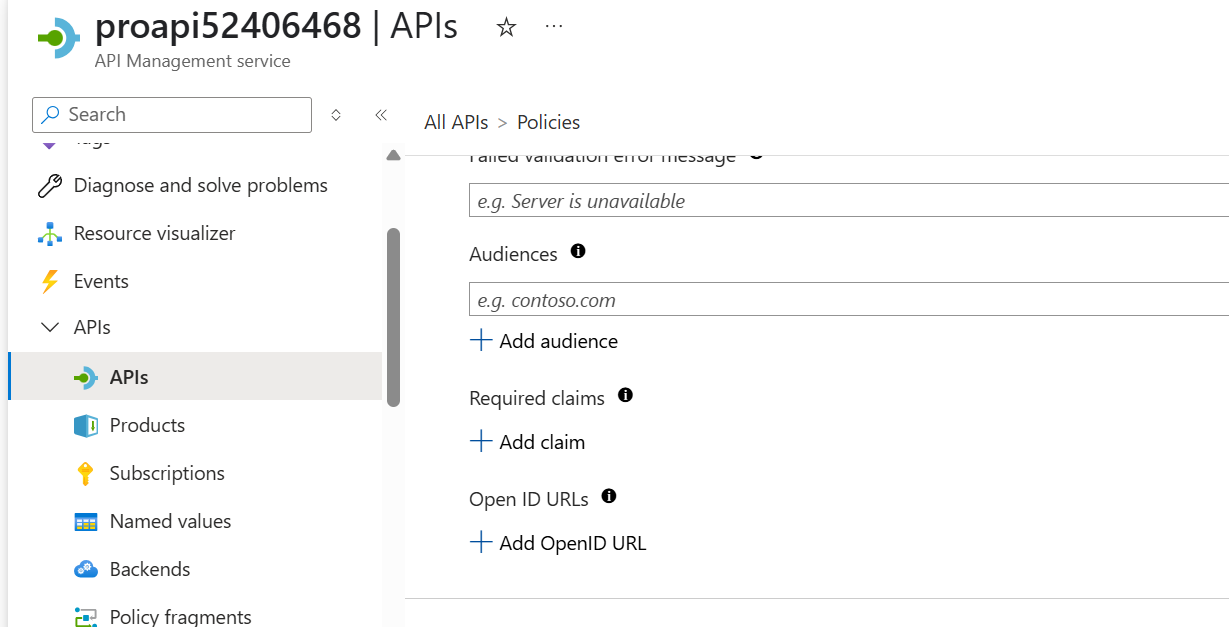




<https://medium.com/identity-beyond-borders/choose-the-right-oauth2-flow-for-your-application-3c87af1c8512>







<!--

    - Policies are applied in the order they appear.

    - Position <base/> inside a section to inherit policies from the outer scope.

    - Comments within policies are not preserved.

-->

<!-- Add policies as children to the <inbound>, <outbound>, <backend>, and <on-error> elements -->

<policies>

    <!-- Throttle, authorize, validate, cache, or transform the requests -->

    <inbound>

        <base />

        <validate-jwt header-name="Authorization" failed-validation-httpcode="401" failed-validation-error-message="Server is unavailable" require-scheme="Bearer">

            <audiences>

                <audience>api://0ffd5df6-6509-4515-b152-cdb0ae823694</audience>

            </audiences>

            <issuers>

                <issuer>https://sts.windows.net/8eb87a6e-8055-4135-b69d-f19c799ec045</issuer>

            </issuers>

        </validate-jwt>

    </inbound>

    <!-- Control if and how the requests are forwarded to services  -->

    <backend>

        <base />

    </backend>

    <!-- Customize the responses -->

    <outbound>

        <base />

    </outbound>

    <!-- Handle exceptions and customize error responses  -->

    <on-error>

        <base />

    </on-error>

</policies>

{

"typ": "JWT",

"alg": "RS256",

"x5t": "CNv0OI3RwqlHFEVnaoMAshCH2XE",

"kid": "CNv0OI3RwqlHFEVnaoMAshCH2XE"

}

<validate-jwt header-name="Authorization" failed-validation-httpcode="401" failed-validation-error-message="Unauthorized. Access token is missing or invalid.">

<openid-config url="https://login.microsoftonline.com/{aad-tenant}/v2.0/.well-known/openid-configuration" />

<audiences>

<audience>{audience-value - (ex:api://guid)}</audience>

</audiences>

<issuers>

<issuer>{issuer-value - (ex: https://sts.windows.net/{tenant id}/)}</issuer>

</issuers>

<required-claims>

<claim name="aud">

<value>{backend-app-client-id}</value>

</claim>

</required-claims>

</validate-jwt>

<validate-jwt header-name="Authorization" failed-validation-httpcode="401" failed-validation-error-message="Unauthorized. Access token is missing or invalid." require-expiration-time="true" require-scheme="Bearer" clock-skew="300">

<openid-config url="https://login.microsoftonline.com/{tenant-id}/v2.0/.well-known/openid-configuration" />

<audiences>

<audience>api://your-api-client-id</audience>

</audiences>

<issuers>

<issuer>https://sts.windows.net/{tenant-id}/</issuer>

</issuers>

</validate-jwt>

<https://login.microsoftonline.com/8eb87a6e-8055-4135-b69d-f19c799ec045/v2.0/.well-known/openid-configuration>

<!--

    - Policies are applied in the order they appear.

    - Position <base/> inside a section to inherit policies from the outer scope.

    - Comments within policies are not preserved.

-->

<!-- Add policies as children to the <inbound>, <outbound>, <backend>, and <on-error> elements -->

<policies>

    <!-- Throttle, authorize, validate, cache, or transform the requests -->

    <inbound>

        <base />

        <validate-jwt header-name="Authorization" failed-validation-httpcode="401" failed-validation-error-message="Server is unavailable">

            <openid-config url="https://login.microsoftonline.com/8eb87a6e-8055-4135-b69d-f19c799ec045/v2.0/.well-known/openid-configuration" />

            <audiences>

                <audience>api://0dd78c4e-e475-4b60-adaf-e500286087d7</audience>

            </audiences>

            <issuers>

                <issuer>https://sts.windows.net/8eb87a6e-8055-4135-b69d-f19c799ec045/</issuer>

            </issuers>

        </validate-jwt>

    </inbound>

    <!-- Control if and how the requests are forwarded to services  -->

    <backend>

        <base />

    </backend>

    <!-- Customize the responses -->

    <outbound>

        <base />

    </outbound>

    <!-- Handle exceptions and customize error responses  -->

    <on-error>

        <base />

    </on-error>

</policies>

{ "typ": "JWT", "alg": "RS256", "x5t": "CNv0OI3RwqlHFEVnaoMAshCH2XE", "kid": "CNv0OI3RwqlHFEVnaoMAshCH2XE" }.{ "aud": "api://0dd78c4e-e475-4b60-adaf-e500286087d7", "iss": "https://sts.windows.net/8eb87a6e-8055-4135-b69d-f19c799ec045/", "iat": 1750586350, "nbf": 1750586350, "exp": 1750590250, "aio": "k2RgYPDdFNRptyu6aWWo7Unb89/0AA==", "appid": "0dd78c4e-e475-4b60-adaf-e500286087d7", "appidacr": "1", "idp": "https://sts.windows.net/8eb87a6e-8055-4135-b69d-f19c799ec045/", "oid": "5c22ba2e-a217-4529-9ed4-cad9f58d0cd2", "rh": "1.ASkAbnq4jlWANUG2nfGceZ7ARU6M1w115GBLra\_lAChgh9fOAQApAA.", "sub": "5c22ba2e-a217-4529-9ed4-cad9f58d0cd2", "tid": "8eb87a6e-8055-4135-b69d-f19c799ec045", "uti": "6Jxt5zB-P0ug5VooRxqLAA", "ver": "1.0", "xms\_ftd": "3MC0rS4UxaOH6OVQVlcxxaakWeMzlMN11hmPIk1F--wBdXNub3J0aC1kc21z" }.[Signature]

{

"args": {},

"headers": {

"Accept": "\*/\*",

"Accept-Encoding": "gzip,deflate,br,zstd",

"Accept-Language": "en-US,en;q=0.9",

"Authorization": "Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6IkNOdjBPSTNSd3FsSEZFVm5hb01Bc2hDSDJYRSIsImtpZCI6IkNOdjBPSTNSd3FsSEZFVm5hb01Bc2hDSDJYRSJ9..eOn1RS34Obwd3FGHylamrfci5ZY0WUncWRuTj7P6L5Cwx9eGSqUwCAfNfXKEqRdWxuzV0r1qZm20owouPIWLf1wy\_friIDI1Quoc5o4Y\_YRgkqz1sKUeZIqnD2w1znWYI3vTUrgRi3s0VQQ\_FzMQDIIK18qgDK\_7AprD98Iz5xiB3HK2Ke0nOiVyWW-qEGi2swR4Z9ltvEho4olwHbJXsA9W7Or6fF0WeAVrlBLlBciBwrCm9Uet-zULV6M5cku4Bl4QQjzus\_EomeiarWkR4\_6h\_Vq\_VBN\_27APzlETMGngNj\_r0yDp1V2YWnD02ERNEUEpSyucmr9CcD83bp\_89w",

"Cache-Control": "no-cache, no-store",

"Client-Ip": "20.85.159.237:6401",

"Disguised-Host": "httpapi52407643-dzatg0fvgnd0fuc2.eastus-01.azurewebsites.net",

"Host": "httpapi52407643-dzatg0fvgnd0fuc2.eastus-01.azurewebsites.net",

"Max-Forwards": "9",

"Ocp-Apim-Subscription-Key": "a7d6cb9aba65421e8fce1697e52fda97",

"Referer": "https://apimanagement.hosting.portal.azure.net/",

"Sec-Ch-Ua": "\"Google Chrome\";v=\"137\",\"Chromium\";v=\"137\",\"Not/A)Brand\";v=\"24\"",

"Sec-Ch-Ua-Mobile": "?0",

"Sec-Ch-Ua-Platform": "\"Windows\"",

"Sec-Fetch-Dest": "empty",

"Sec-Fetch-Mode": "cors",

"Sec-Fetch-Site": "cross-site",

"Was-Default-Hostname": "httpapi52407643-dzatg0fvgnd0fuc2.eastus-01.azurewebsites.net",

"X-Appservice-Proto": "https",

"X-Arr-Log-Id": "03883105-8088-41e8-85f4-a256e8ed5452",

"X-Arr-Ssl": "2048|256|CN=Microsoft Azure RSA TLS Issuing CA 08, O=Microsoft Corporation, C=US|CN=\*.azurewebsites.net, O=Microsoft Corporation, L=Redmond, S=WA, C=US",

"X-Client-Ip": "20.85.159.237",

"X-Client-Port": "6401",

"X-Forwarded-Tlsversion": "1.2",

"X-Original-Url": "/get",

"X-Site-Deployment-Id": "httpapi52407643",

"X-Waws-Unencoded-Url": "/get"

},

"origin": "103.83.145.74,20.121.82.216:64960,20.121.82.216, 20.85.159.237:6401",

"url": "https://httpapi52407643-dzatg0fvgnd0fuc2.eastus-01.azurewebsites.net/get"

}

SendTrace

Header

{

"typ": "JWT",

"alg": "RS256",

"x5t": "CNv0OI3RwqlHFEVnaoMAshCH2XE",

"kid": "CNv0OI3RwqlHFEVnaoMAshCH2XE"

}

Payload

{

"aud": "api://0dd78c4e-e475-4b60-adaf-e500286087d7",

"iss": "https://sts.windows.net/8eb87a6e-8055-4135-b69d-f19c799ec045/",

"iat": 1750586641,

"nbf": 1750586641,

"exp": 1750590541,

"aio": "k2RgYPhSWx4y8Ut50P7MmKY5i++pAAA=",

"appid": "0dd78c4e-e475-4b60-adaf-e500286087d7",

"appidacr": "1",

"idp": "https://sts.windows.net/8eb87a6e-8055-4135-b69d-f19c799ec045/",

"oid": "5c22ba2e-a217-4529-9ed4-cad9f58d0cd2",

"rh": "1.ASkAbnq4jlWANUG2nfGceZ7ARU6M1w115GBLra\_lAChgh9fOAQApAA.",

"sub": "5c22ba2e-a217-4529-9ed4-cad9f58d0cd2",

"tid": "8eb87a6e-8055-4135-b69d-f19c799ec045",

"uti": "4obxGy0JTU6v4uNbnkuUAA",

"ver": "1.0",

"xms\_ftd": "dFOUtKktBKBTnci5L4bSb-zRYEy3Ia2mlH6AUTa5y4oBdXNlYXN0LWRzbXM"

}

Header

{

"e": "AQAB",

"kty": "RSA",

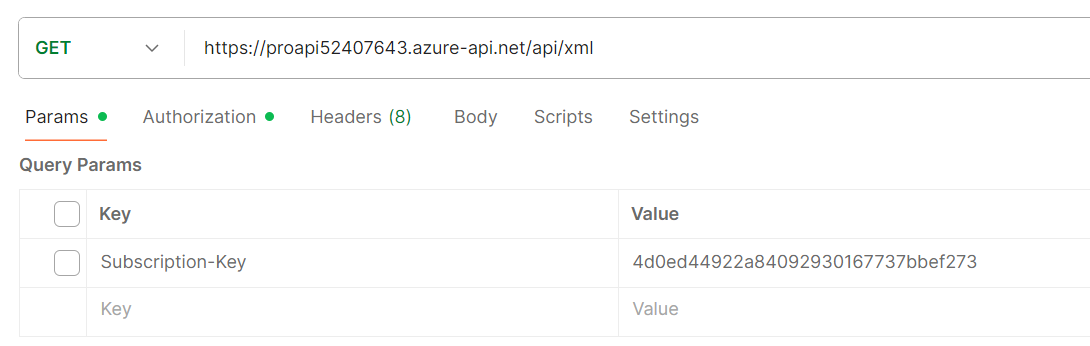
"n": "hz6fUSCSAuiyQz6L1nQj4za8kItevJzxhVbecMigTIl9pXZSHZa3gzMgtapnb1q96CG5qvR78dH6ZvTKL8MzN4VfGgZhvLEv5LJKeo0tGgBIS65wxIiJYj9ExEDqFkw9RdhW1nN8IN9eO76PbC-fdEPtDekA2BaITY2DARISKN4Ke0RLBEWNrKeEjjOzrygS2e3Q9NVzE51ZGGQAGHau7atHy8M\_qA1nnd2dMUgUMnEYIMzDBTSKz17G6itJOdanGvG3wXvdpndKffnDppaPkyWbnybdMI4IP7q6WsCqnt3Gtg-baG6GDqZQQEBp9C9gLAFv4ORTRlpD3w0gCMh7xw"

}

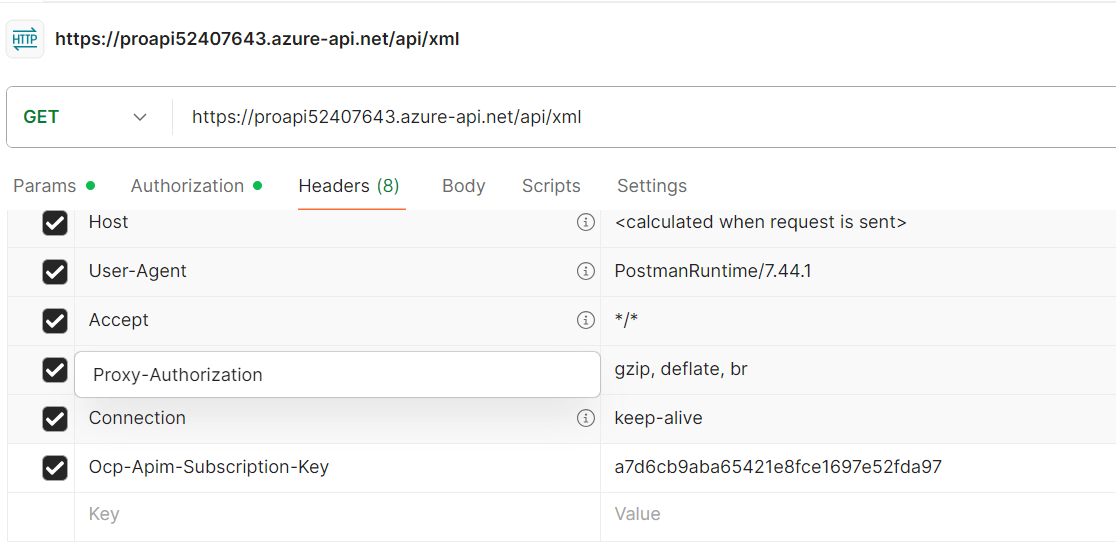
**3. Check Your App Registration**

Ensure your app is registered to support v2.0:

* Go to **Azure Portal > App registrations > Your App**
* Under **Authentication**, ensure ID tokens and Access tokens are enabled
* Check the **manifest**, make sure "accessTokenAcceptedVersion": 2



Subscription-Key - 4d0ed44922a84092930167737bbef273



Ocp-Apim-Subscription-Key - a7d6cb9aba65421e8fce1697e52fda97