

## **Exercise: SAP API Management**

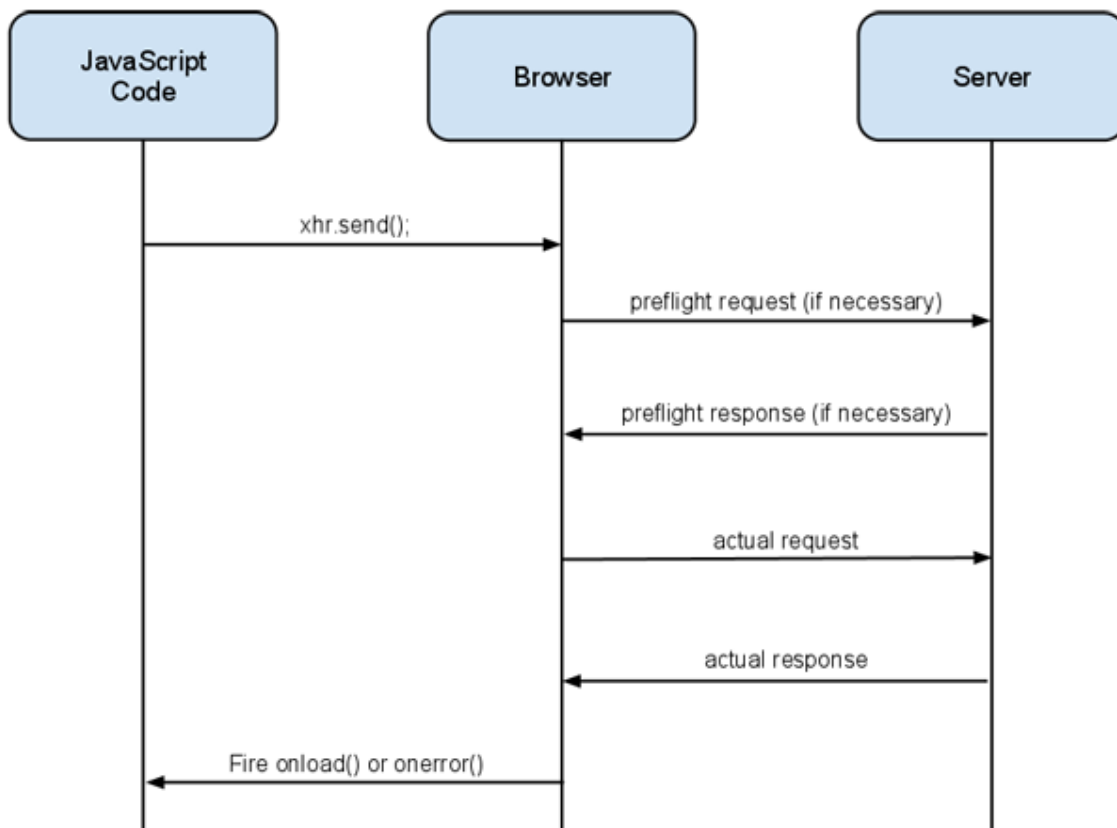
### **Unit 4.4.11 – CORS**

## SCENARIO

Cross-Origin Resource Sharing (CORS) is a W3C spec that allows cross-domain communication from the browser. By building on top of the XMLHttpRequest object, CORS allows developers to work with the same idioms as same-domain requests.

HTTP requests from JavaScript are traditionally bound by the Same Origin Policy, which means that the Ajax requests must have the same domain and port. The common ways to get around this are using techniques like JSON-P or setting up a custom proxy. By supporting CORS requests, the server can add a few special response headers that would allow the browser to access the data from a different domain.

CORS supports require coordination between both server and client. On the client side (browser side) most of the handling for CORS is automatically done by the browser on behalf of the client which is depicted below in the diagram.



Typically the preflight request is triggered by the browser with http method OPTIONS to the requested server resource. In this call, the server must return the CORS related headers. All CORS headers are prefixed with “Access-Control-“. The table below describes the CORS header which the server must return

Header Name	Description
Access-Control-Allow-Origin	This header must be included in all valid CORS responses; omitting the header will cause the CORS request to fail. The value of the header can either echo the Origin request header (as in the example above), or be a '*' to allow requests from any origin.
Access-Control-Allow-Credentials	By default, cookies are not included in CORS requests. Use this header to indicate that cookies should be included in CORS requests. The only valid value for this header is true (all lowercase). If this header is specified then * can't be used with Access-Control-Allow-Origin header it must return the domain name of client which can access the data.

	<p>This header works in conjunction with <i>withCredentials</i> property on the XMLHttpRequest2 object (this changes needs to be done on the client and is captured below)</p> <p><i>For CSRF token handling sine Gateway service also requires cookies to be passed this header must be set to true</i></p>
Access-Control-Expose-Headers	<p>The XMLHttpRequest 2 object has a <code>getResponseHeader()</code> method that returns the value of a particular response header. During a CORS request, the <code>getResponseHeader()</code> method can only access simple response headers (Cache-Control, Content-Language, Content-Type, Expires, Last-Modified, Pragma).</p> <p><i>For CSRF token handling sine Gateway service also requires client to read the custom header x-csrf-token therefore this header would be have to set to include x-csrf-token</i></p>
Access-Control-Allow-Methods	Comma-delimited list of the supported HTTP methods
Access-Control-Allow-Headers	Comma-delimited list of the supported request headers.

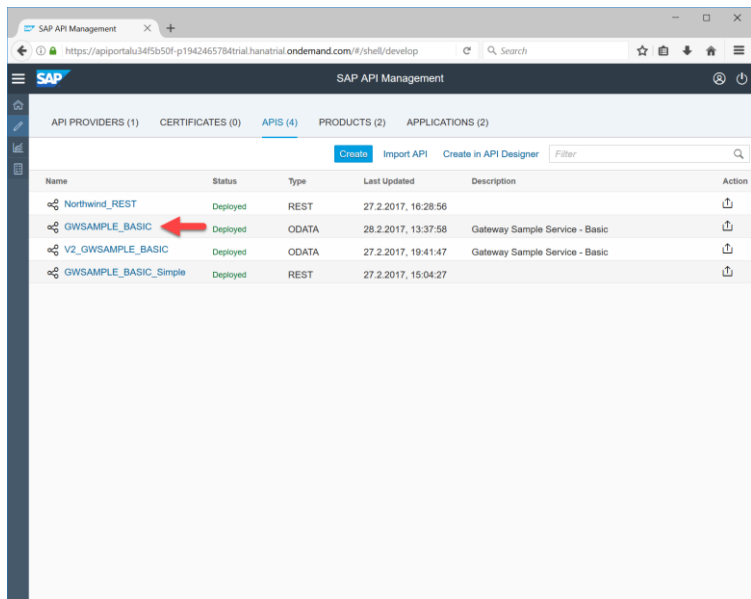
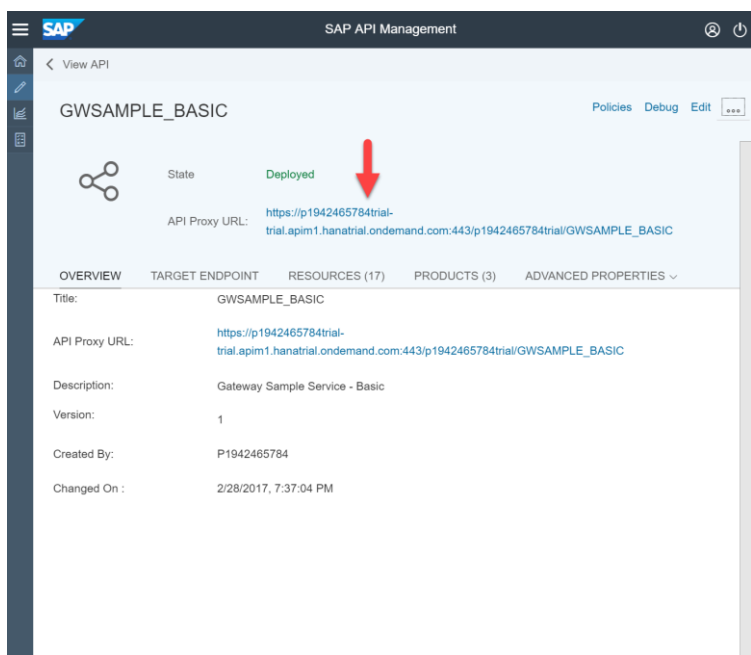
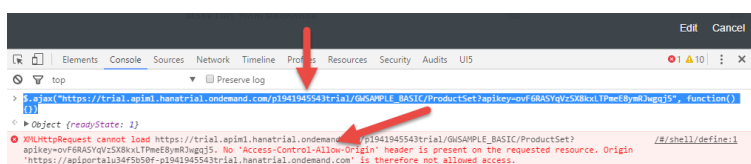
We can use SAP API Management to enable this CORS handling for the Gateway services.

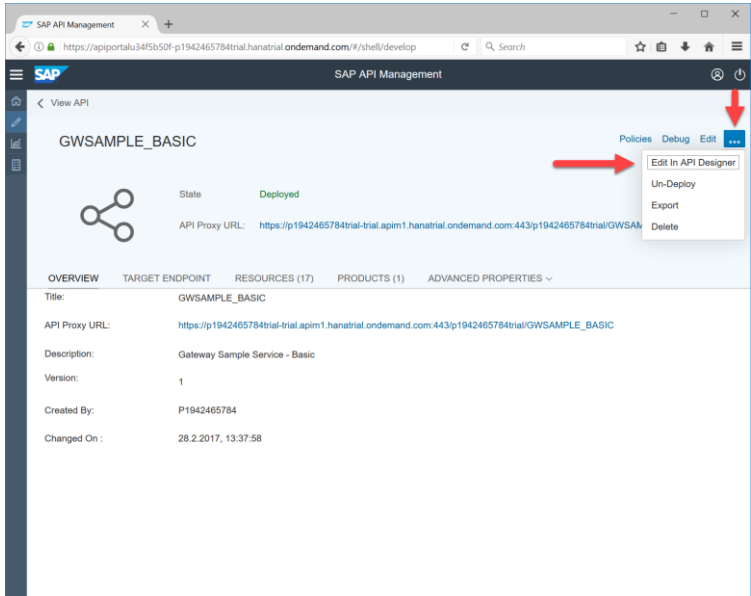
#### **CORS HANDLING ON SAP API MANAGEMENT**

The SAP Gateway services doesn't support OPTIONS http method and therefore we can use routerule to ensure that the OPTIONS call is not routed to the SAP Gateway services but then the response with CORS header is returned by the SAP API Management.

#### **Prerequisites**

- Existing API Proxy

Explanation	Screenshot
<div>PART 1</div>	
<div>1. Select the GWSAMPLE_BASIC API Proxy</div>	
<div>2. Take the API Proxy URL</div>	
<div>There are a few ways to easily tests CORS.</div> <div>A) Slightly more technical approach</div>	

Explanation	Screenshot
<p><b>Note:</b> Make sure that you open the F12 tool only when you are in the API Proxy view.</p> <ol style="list-style-type: none"> <li>Click F12 to open the Developer Tool</li> <li>Enter the command  <code>\$.ajax("https://p1942465784trial-trial.apim1.hanatrial.ondemand.com/p1942465784trial/GWSAMPLE_BASIC?apikey=VrHk2kQK9ePMIUIJKnpbuV85BALmDZUb", function({})</code></li> <li>Hit Enter</li> </ol> <p>As a result you see the Access-Control-Allow-Origin error message</p>	
<p>B) Go to the API Designer by clicking on <b>Edit in API Designer</b>.</p> <ol style="list-style-type: none"> <li>Copy and replace the contents with this code.</li> </ol> <p><b>Note:</b> The API Designer will show an error message on the top. You can ignore this message.</p> <p><b>Note:</b> Please make sure to replace the basePath with your P-User.</p>	 <pre> {   "swagger": "2.0",   "info": {     "version": "1.0.0",     "title": "",     "description": ""   },   "host": "p1942465784trial-trial.apim1.hanatrial.ondemand.com",   "basePath": "/p1942465784trial/GWSAMPLE_BASIC",   "tags": [     {       "name": "ProductSet", </pre>

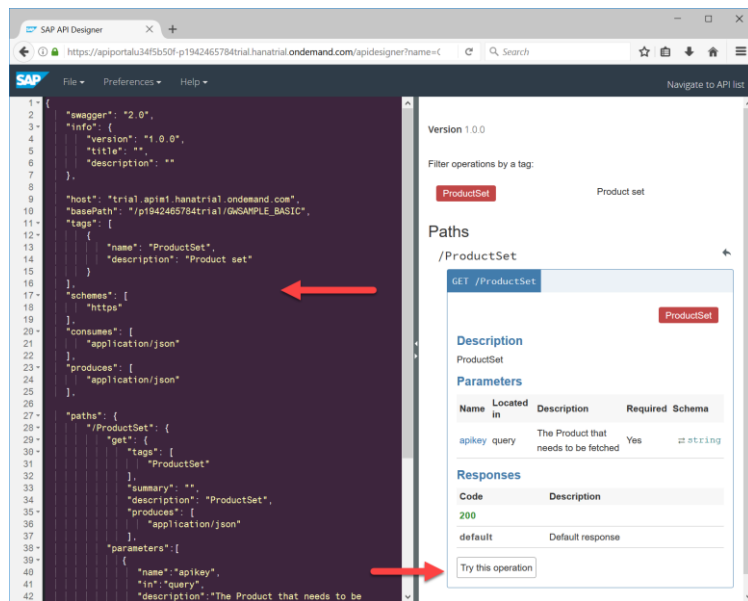
Explanation	Screenshot
	<pre>        "description": "Product set"       },     ],     "schemes": [       "https"     ],     "consumes": [       "application/json"     ],     "produces": [       "application/json"     ],     "paths": {       "/ProductSet": {         "get": {           "tags": [             "ProductSet"           ],           "summary": "",           "description": "ProductSet",           "produces": [             "application/json"           ],           "parameters": [             {               "name": "apikey",               "in": "query",               "description": "The Product that needs to be fetchd",               "required": true,               "type": "string"             }           ],           "responses": {             "default": {               "description": "Default response"             }           }         }       }     }   } }</pre>

---

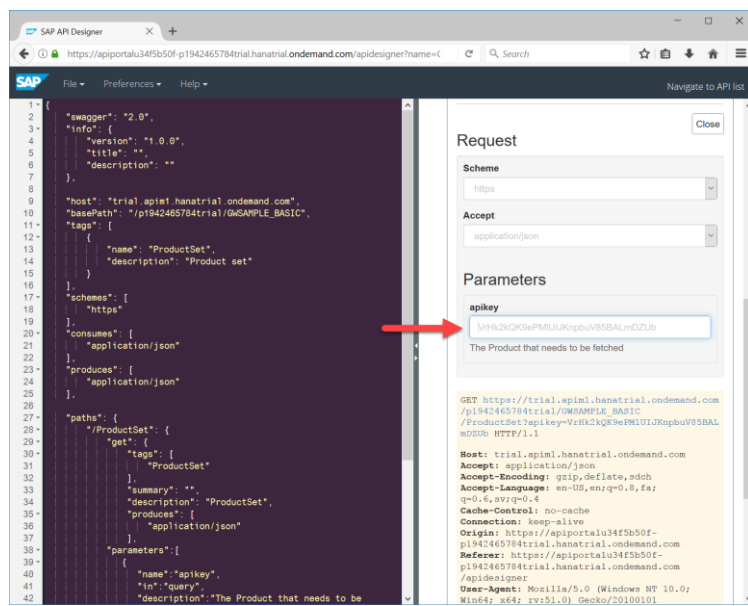
## Explanation

7. Click on Try this operation

## Screenshot



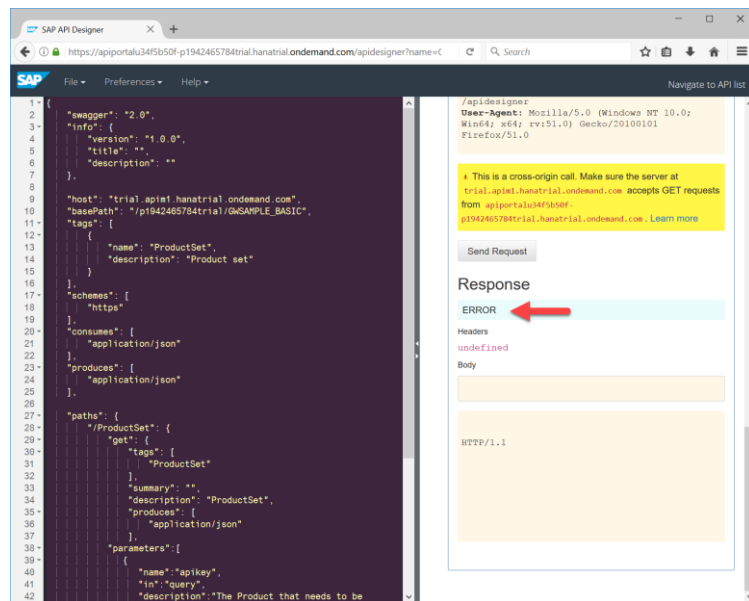
8. Enter the API Key  
9. Click on Send Request



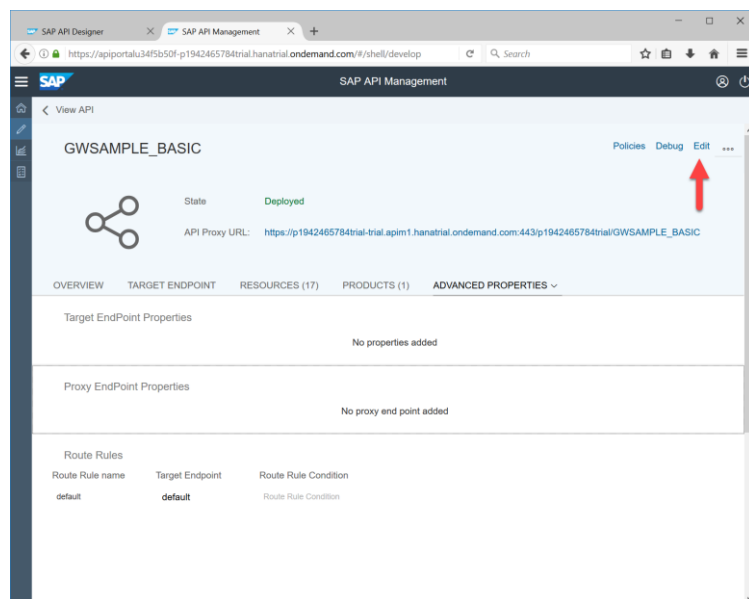
## Explanation

10. You will see an error message as again

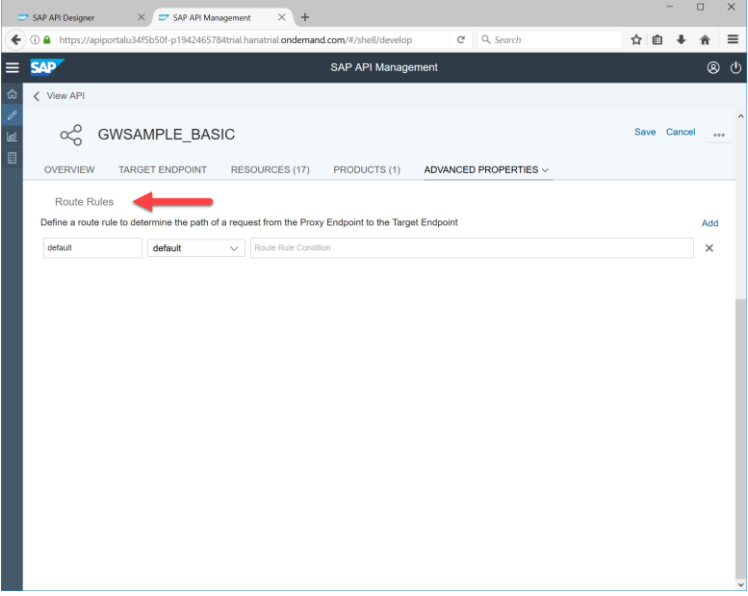
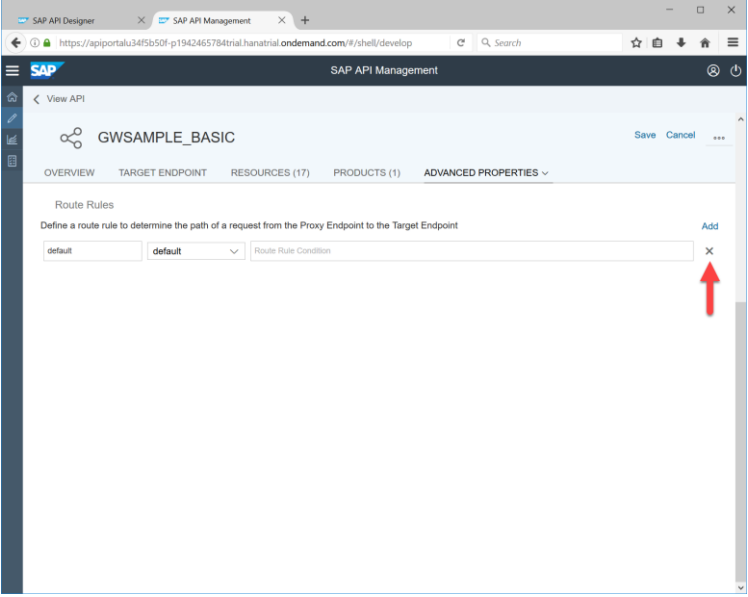
## Screenshot

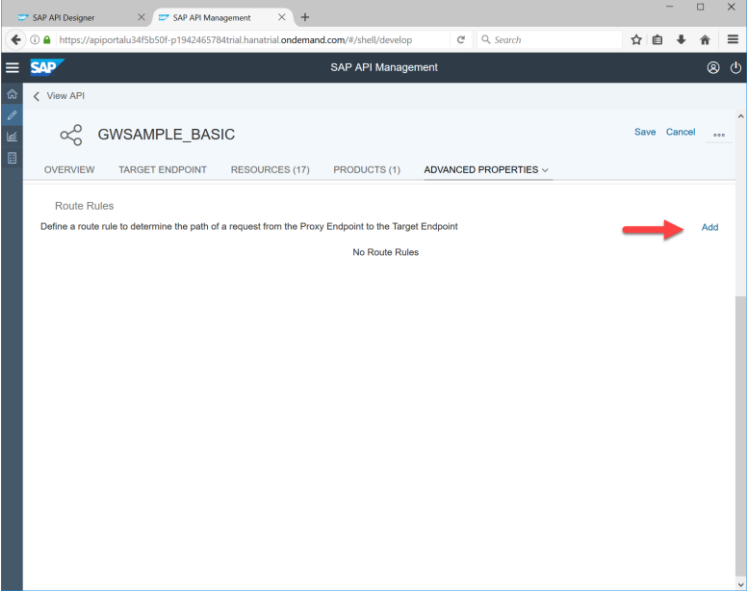
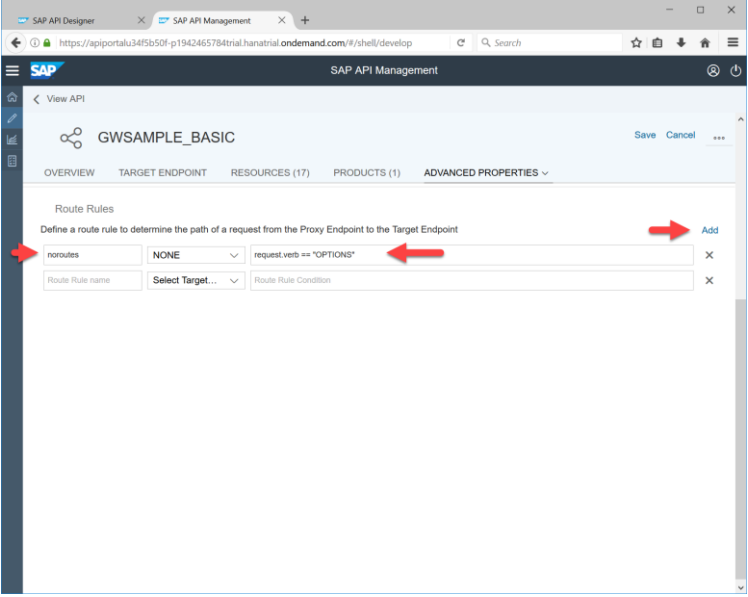


11. Go back to the API Management API Proxy and click on Edit.





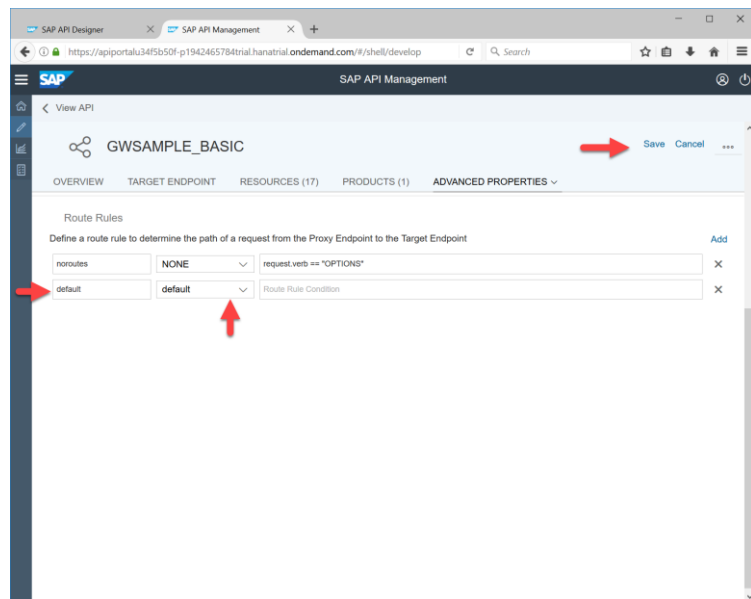
Explanation	Screenshot
12. Scroll down to Route Rules	 The screenshot shows the SAP API Management console interface. The top navigation bar includes 'SAP API Designer' and 'SAP API Management'. The main header displays 'View API' and 'GWSAMPLE_BASIC'. Below the header, there are tabs for 'OVERVIEW', 'TARGET ENDPOINT', 'RESOURCES (17)', 'PRODUCTS (1)', and 'ADVANCED PROPERTIES'. The 'Route Rules' tab is selected, and a red arrow points to the 'Route Rules' section header. The text below the header reads: 'Define a route rule to determine the path of a request from the Proxy Endpoint to the Target Endpoint'. There is an 'Add' button on the right. Below this, there is a table with columns for 'default', 'default', and 'Route Rule Condition'. A red arrow points to the 'Route Rule Condition' column header.
13. Click on the X to remove the current route rule	 The screenshot shows the same SAP API Management console interface as the previous one. The 'Route Rules' tab is selected. A red arrow points to the 'X' icon next to the 'Route Rule Condition' column header, indicating the action to remove the current route rule.

Explanation	Screenshot
14. Click on Add to add a new Route rule	 The screenshot shows the SAP API Management console interface. At the top, there's a navigation bar with 'SAP API Designer' and 'SAP API Management' tabs. Below that, the URL bar shows a development endpoint. The main header indicates 'View API' for 'GWSAMPLE_BASIC'. There are tabs for 'OVERVIEW', 'TARGET ENDPOINT', 'RESOURCES (17)', 'PRODUCTS (1)', and 'ADVANCED PROPERTIES'. The 'Route Rules' section is active, displaying the instruction 'Define a route rule to determine the path of a request from the Proxy Endpoint to the Target Endpoint' and 'No Route Rules'. A red arrow points to the 'Add' button in the top right corner of this section.
15. Enter the name noroutes and Route Rule Condition: request.verb == "OPTIONS" 16. Click on Add again	 This screenshot shows the same SAP API Management console but with a new route rule added. The rule is named 'noroutes' and has the condition 'request.verb == "OPTIONS"'. The 'Add' button is again highlighted with a red arrow. Red arrows also point to the 'Route Rule name' and 'Route Rule Condition' input fields. The table below the rule shows columns for 'Route Rule name' and 'Route Rule Condition'.

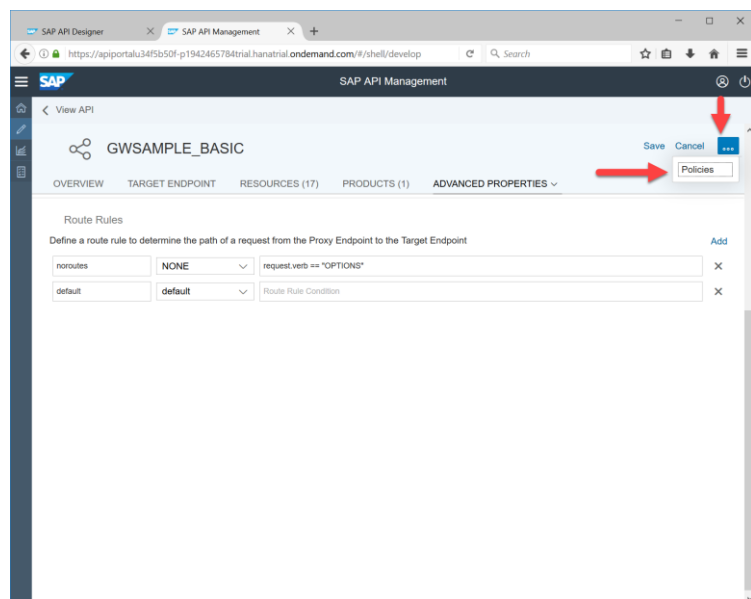
## Explanation

17. Add another Route rule name "default"
18. Switch the Target Endpoint to "default"
19. and click on Save

## Screenshot

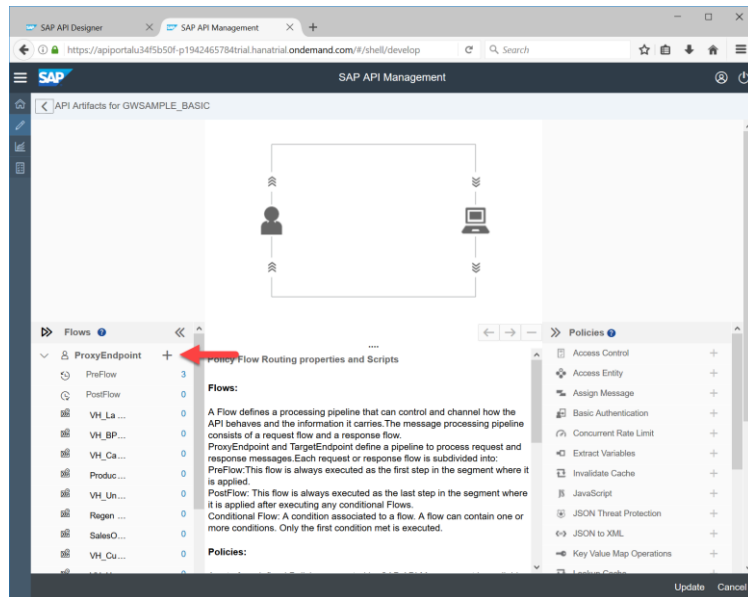


20. Click on Policies

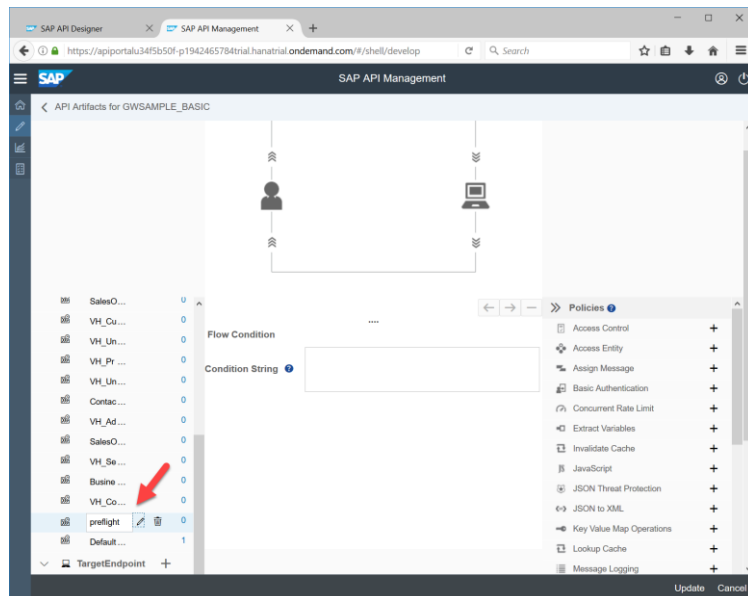


**Explanation**

21. Click on the + sign next to the ProxyEndpoint

**Screenshot**

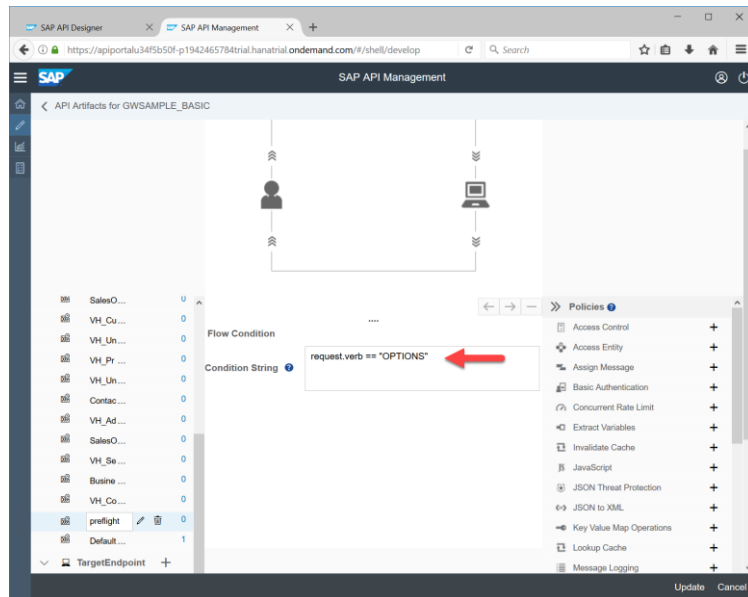
22. Scroll down and enter the name preflight



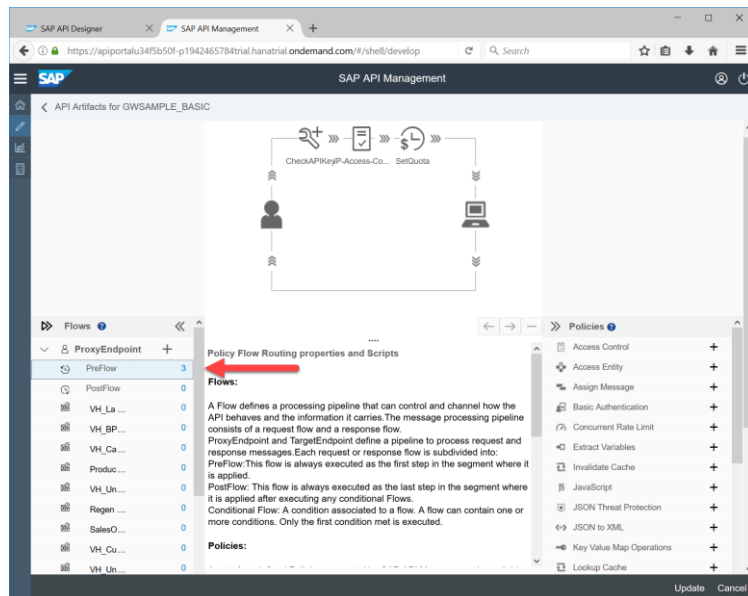
## Explanation

23. Enter the Condition string:  
request.verb == "OPTIONS"

## Screenshot



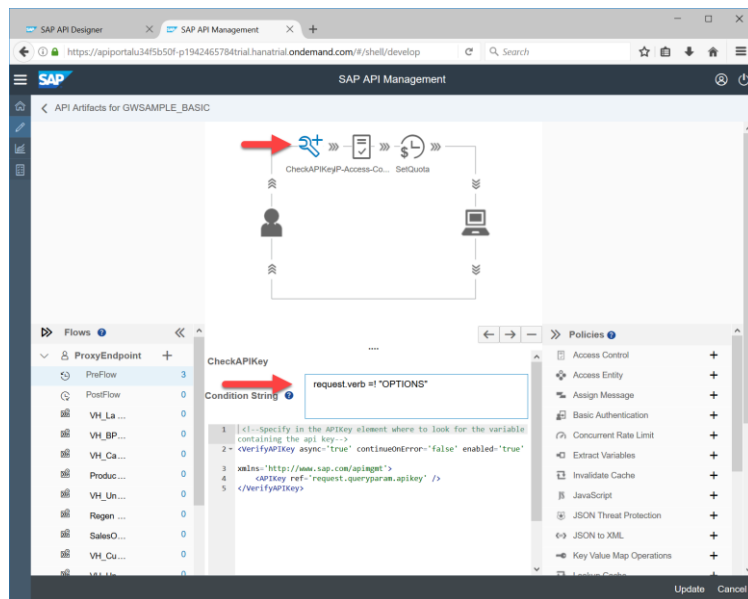
24. Select the PreFlow on the left hand side:



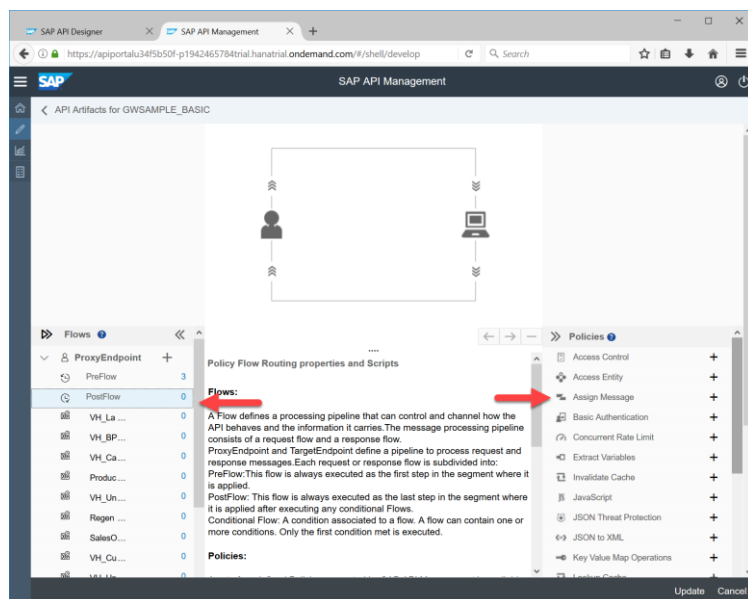
## Explanation

25. Select the Check API Key Policy and add the Condition: request.verb != "OPTIONS"

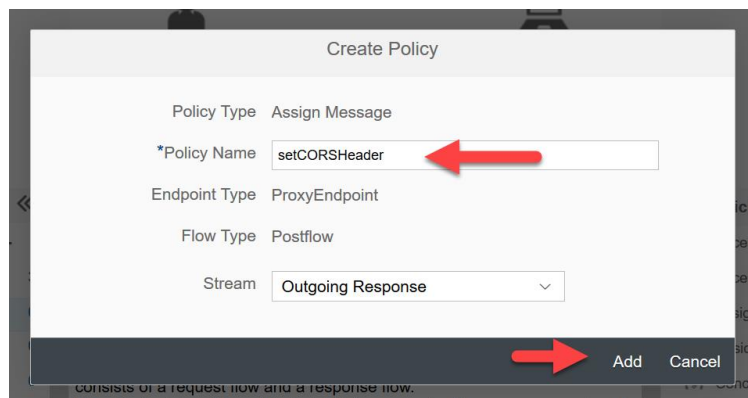
## Screenshot




26. Scroll up and select PostFlow from ProxyEndpoint  
27. Click on the + Sign next to the AssignMessage Policy on the right



28. Enter the name setCORSHeader,  
29. Select the Stream: Outgoing Response and  
30. Click on Add

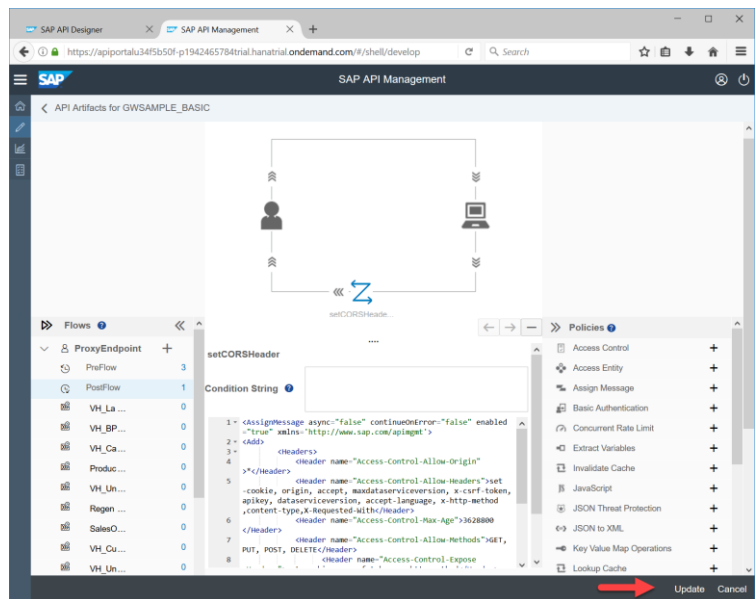


Explanation	Screenshot
31. Replace / add the following code	<pre> &lt;AssignMessage async="false" continueOnError="false" enabled="true" xmlns='http://www.sap.com/apimgmt'&gt; &lt;Add&gt;   &lt;Headers&gt;     &lt;Header name="Access-Control-Allow-Origin"&gt;*&lt;/Header&gt;     &lt;Header name="Access-Control-Allow-Headers"&gt;set- cookie, origin, accept, maxdataserviceversion, x-csrf-token, apikey, dataserviceversion, accept-language, x-http- method,content-type,X-Requested-With&lt;/Header&gt;     &lt;Header name="Access-Control-Max- Age"&gt;3628800&lt;/Header&gt;     &lt;Header name="Access-Control-Allow-Methods"&gt;GET, PUT, POST, DELETE&lt;/Header&gt;     &lt;Header name="Access-Control-Expose- Headers"&gt;set-cookie, x-csrf-token, x-http-method&lt;/Header&gt;    &lt;/Headers&gt; &lt;/Add&gt; &lt;IgnoreUnresolvedVariables&gt;&gt;false&lt;/IgnoreUnresolvedVariable s&gt; &lt;AssignTo createNew="false" type="response"&gt;response&lt;/AssignTo&gt; &lt;/AssignMessage&gt; </pre> 

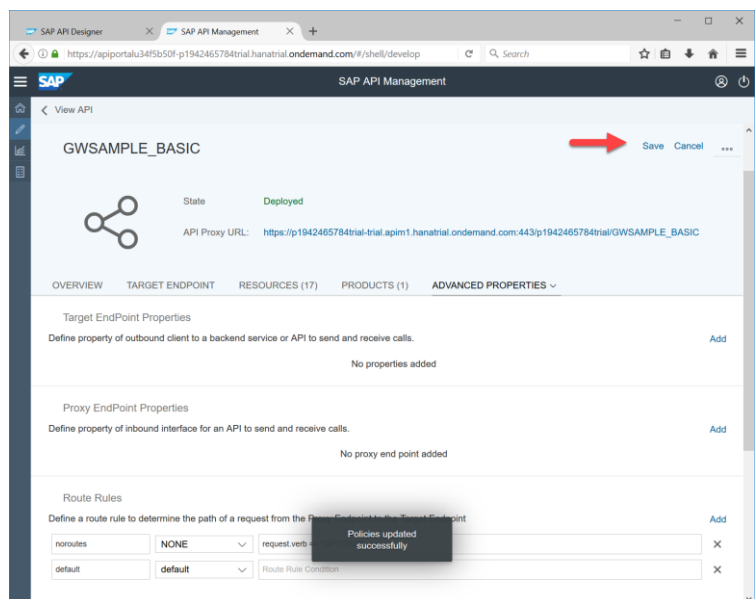
## Explanation

32. Click on Update

## Screenshot

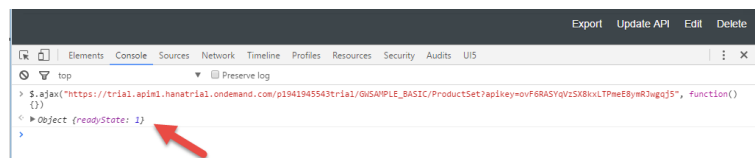


33. Click on Save



Click F12 to open the Developer tool again and run the command  
`$.ajax("https://p1942465784trial.apim1.hanatrial.ondemand.com/p1942465784trial/GWSAMPLE_BASIC?apikey=VrHk2kQK9ePMIUIJKnpbuV85BALmDZUb", function({})`

34. This time you do not get an error message

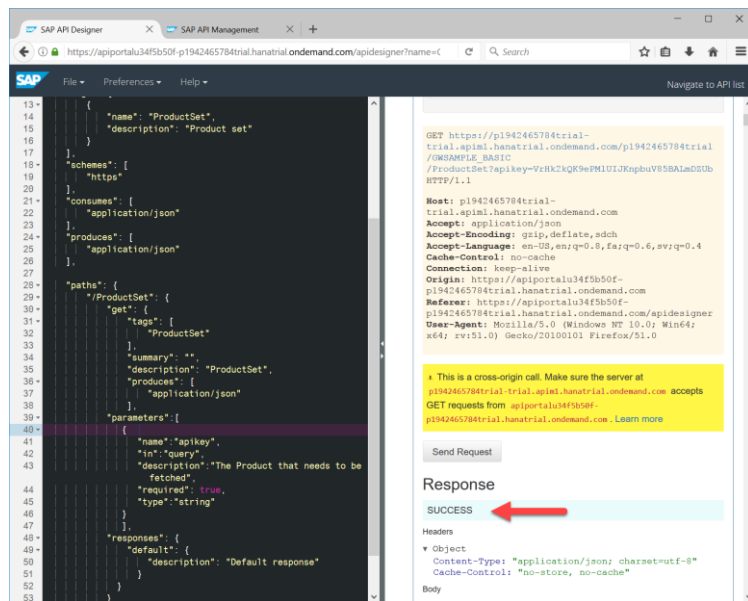




## Explanation

35. Go back to the API Designer and click on Send Request again
36. Now you get a Success message back

## Screenshot





© 2016 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. Please see <http://www.sap.com/corporate-en/legal/copyright/index.epx#trademark> for additional trademark information and notices. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors.

National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP SE or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP SE or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platform directions and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.