CORS

By implementing this policy, you can enable and configure Cross Origin Resource Sharing on an API. This is a method to define access to resources outside of the originating domain. Principally, this is a security mechanism to prevent the loading of resources from unexpected domains, for instance via XSS injection attacks.

General Remarks

The CORS policy works correctly only for public APIs. If the API is private, the API Key is checked at first stage. However, the browser will not send this request during a preflight request. So the CORS request is blocked before it can reach the CORS policy.

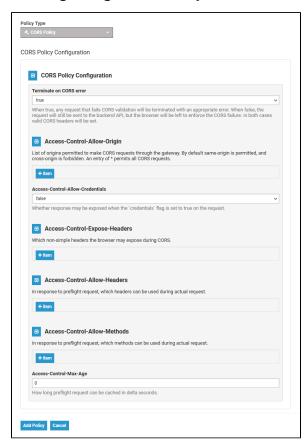
API Management sets the CORS headers in the following order:

- 1. CORS headers from the CORS policy have the highest priority.
- 2. If no CORS policy has been defined, CORS headers from the external API are used.



For detailed explanations about Cross-Origin Resource Sharing (CORS) visit the official Mozilla documentation.

Configuring the Policy



Configuration Options

Option	Туре	Description	Possible Values	Default
Terminate on CORS error	Boolean	Defines whether the API Management should terminate on a CORS validation error (true) or not (false). In both cases, valid CORS headers (see below) will be set.	true/false	true

On this Page:

- General Remarks
- Configuring the Policy
 - Configuration Options

Related Pages:

- Policies
 - Assigning Policies
 - Policy Configuration

Related Documentation:

- Official Mozilla documentation
 - Cross-Origin
 Resource Sharing
 (CORS)

Access- Control- Allow-Origin	Array of String	A list of origin URLs that are permitted to make requests. By default, same-origin is permitted, cross-origin is forbidden. By adding an item of "*", you can permit all URLs.		
Access- Control- Allow- Credentials	Boolean	Define whether the response may be exposed when the API Management receives a request with a credentials flag = true.	true/false	false
Access- Control- Expose- Headers	Array of String	A list of non-simple headers the browser may expose.		
Access- Control- Allow- Headers	Array of String	A list of headers that can be used during a request. Will be provided as a response to a preflight request.	any valid HTTP header	
Access- Control- Allow- Methods	Array of String	List of HTTP methods that can be used during the request. Will be provided as a response to a preflight request. The Access-Control-Allow-Methods must be set for all methods you want to use (e.g. POST, DELETE, PUT).	any valid HTTP method	
Access- Control-Max- Age	Integer	Value in seconds how long a browser may cache a preflight request before it expires.	delta in seconds	



Click **Add Policy** to save your changes.