AUTHORIZATION

On this Page:

- Configuration Options
  - Basic Configuration

Related Pages:

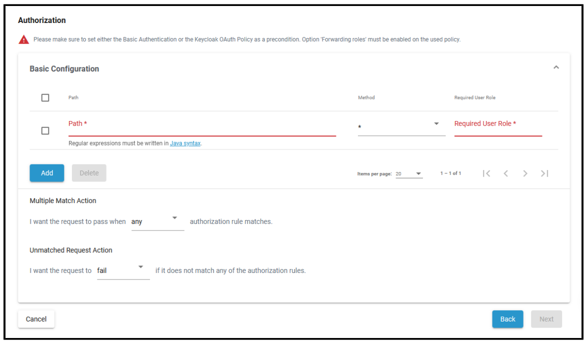
- Policies
  - Attaching Policies

The **Authorization Policy** allows to add a list of fine-grained authorization rules. Use this policy to control precisely who is allowed to access the API.

> This policy must be configured **after** one of the standard authentication policies like the Basic Authentication policy or the Keycloak OAuth policy.
> An authentication policy is responsible for extracting the authenticated user's roles - and this is data, that is required for the Authorization policy to do its work. Refer to Additional Authorization for more details.

The configuration of this policy consists of a number of rules that are applied to any inbound request to the API. Each rule consists of a regular expression pattern, an HTTP verb and the role that an authenticated user must possess in order for access to be granted. It is also possible to apply the rules for all requests by using a wildcard regular expression.

Configuration Options



Authorization

Please make sure to set either the Basic Authentication or the Keycloak OAuth Policy as a precondition. Option 'Forwarding roles' must be enabled on the used policy.

Basic Configuration

	Path	Method	Required User Role
☐	Path *	*	Required User Role *

Regular expressions must be written in Java syntax.

Items per page: 20 1 – 1 of 1

Multiple Match Action

I want the request to pass when any authorization rule matches.

Unmatched Request Action

I want the request to fail if it does not match any of the authorization rules.

Basic Configuration

Option	Description	Possible Values	Default
Path	The pattern must match the request resource path you would like the policy to be applicable to. The input of a path is mandatory. Regular expressions must be written in **Java syntax**.	a string	-
Method	The HTTP method has to match the request you would like the policy to be applicable to.	• * • GET • POST • PUT • DELETE • OPTIONS • PATCH • HEAD • TRACE • CONNECT	*
Required User Role	This role must be assigned to the user if this pattern should match the request. The input of a user role is mandatory.	a string	-
Click **Add** to create more rows in the table. Click **Delete** to remove selected rows.			
Multiple Match Action	Use this option to determine when the request should pass.	• any • at least one	any

Unmatched Request Action	Use this option to determine the action when a request does not match.	• fail • pass	fail