API Security: Authentication and Authorization

A common API Management use case is that an API should not be accessible to anyone, but only to authorized users. To secure your REST APIs, we recommend to use the **Keycloak OAuth** policy for user authentication. If additional user authorization (with roles) is required, we recommend to extend your setup with the **Authorization** policy.

- **Keycloak OAuth:** Use this policy to secure your API via Keycloak. This Keycloak-specific OAuth2 policy should be your first choice to secure an API in the PAS environment.
  Refer to Authentication With Keycloak OAuth for details.
- **Authorization:** Use this policy in addition to Keycloak OAuth or Basic Auth to control precisely who is allowed to access the API.
  Refer to Additional Authorization for details.

Related Pages:

- Authentication With Keycloak OAuth
- Additional Authorization
- Policies
  - Attaching Policies
  - Authorization
  - Keycloak OAuth