

# WSO2 API Manager 3.2.0 Developer Fundamentals

API Visibility and Access Control



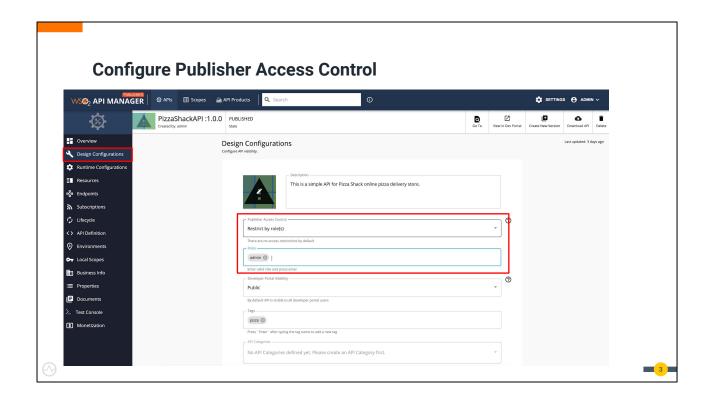


#### **Publisher Access Control**

- Visibility settings prevent certain user roles from viewing and modifying APIs created by another user role.
- By default, APIs created in the API Publisher Portal are visible to any user who logs in to the Publisher Portal.
- This feature allows API creators to restrict API view and modify actions to a set of users, based on their roles

Link - Publisher Access Control





- Log in to API Publisher and open an API by selecting it.
- Go to Design Configurations
- Select Publisher Access Control as Restricted by Role(s) from the dropdown list.
- Enter the roles list for which the API should be visible.

## **API Visibility in Developer Portal**

- By default, the APIs created and published via the API Publisher Portal are visible to anyone (even anonymous users) who visit the Developer Portal.
- API Publishers can control this by selecting which users can view their APIs.

Control API Visibility in Developer Portal





## **API Visibility in Developer Portal**

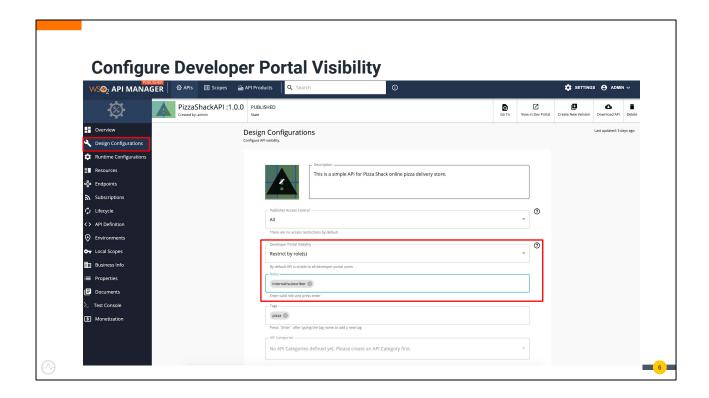
API visibility can be one of the following options:

Visibility	Visible to
Public	<ul> <li>All users who are registered</li> <li>Anonymous users</li> <li>Can be advertised in multiple stores (central and non-WSO2 store)</li> </ul>
Restricted by roles	<ul><li>It's tenant domain</li><li>Only to the user roles that have been specified</li></ul>
Visible to my domain*	<ul><li>All users registered to the API's tenant domain</li><li>Not applicable when there is only one tenant</li></ul>

<sup>\*</sup> This option will not be visible if there is only one tenant







- Log in to API Publisher and open an API by selecting it.
- Go to Design Configurations
- Select necessary option from the **Developer Portal Visibility** dropdown list.
- If Restrict by role(s) is selected, enter the roles list for which the API should be visible.

### How visibility levels work for users in different roles

- The API Creator and Publisher users with the same access controlled roles can see all APIs in their tenant store even if you restrict access to them.
- Anonymous users can only see APIs that have the visibility set as Public.
- Registered users can see,
  - Public APIs of all tenant domains.
  - All APIs in the registered user's tenant domain as long as the API is not restricted to a role that the user is assigned to.

#### **API Visibility**



