Configuring an API

If you have created an API, you must configure it before you can publish the API to the API Developer Portal. Refer to API Settings for an overview of the available options in the API details view.

API Tab "Settings"

In tab **Settings** of the API details page you can provide the backend API implementation. You can configure the following options here:

- Implementation
- API Type
- Visibility
- Plans and Approval Requirement
- Feature in API Developer Portal

Defining the API Endpoint

In section **Implementation**, you need to enter the URL that the API Management will use to proxy a request made for this API.

If you import your API from the PAS Administration, the API endpoint /location is automatically set.

Choosing the API Type

In API Management, you can create two different types of APIs: Public APIs and private APIs. Refer to API Types: Public vs. Private for a detailed overview on the differences between the two types. During API configuration, you should make a considered decision about the API type: It is not recommended to change the API type once the API has been published.

Depending on the chosen type, the content below the **Public API** toggle button changes (in addition, see Defining the Visibility and Attaching Plans):

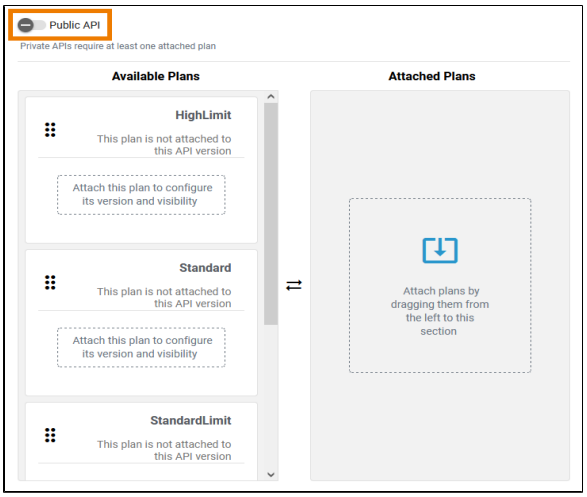
On this Page:

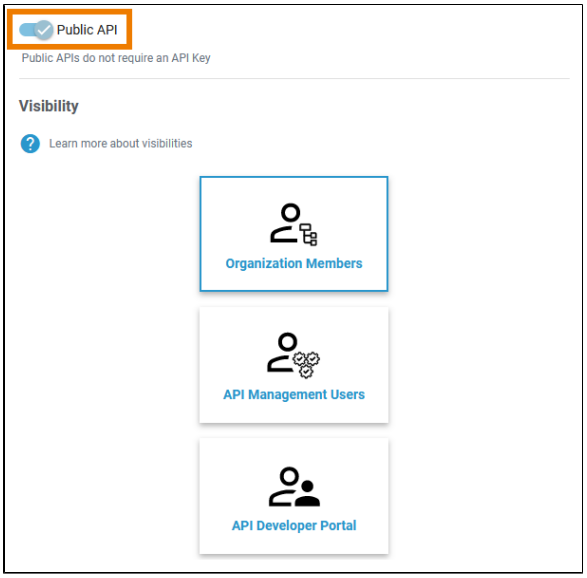
Related Pages:

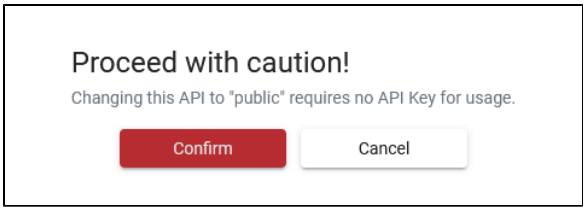
- APIs
  - API Settings
  - Importing APIs
  - Publishing an API

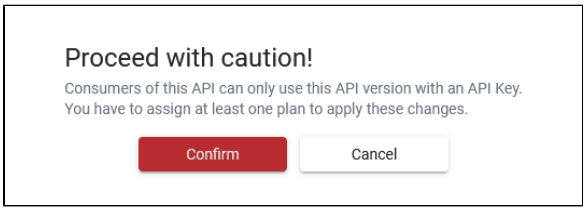
Related Documentation:

- OpenAPI Specification
- WSDL Specification

	By **default**, newly created or imported APIs are created as **private APIs**. A private API cannot be consumed by everyone: They require an API Key in order to be called. To consume a private API, a client and a contract must be created. Compared to a public API, private APIs require more complex configuration.

	Enable the toggle button to change the type to **public**. A public API can be consumed by everyone (assuming no additional security policy has been set). It is also very easy to consume a public API: You just need to know its public endpoint. Clients do not need to register for a public API: Neither a client nor a contract are necessary. Compared to a private API, a public API requires less configuration.



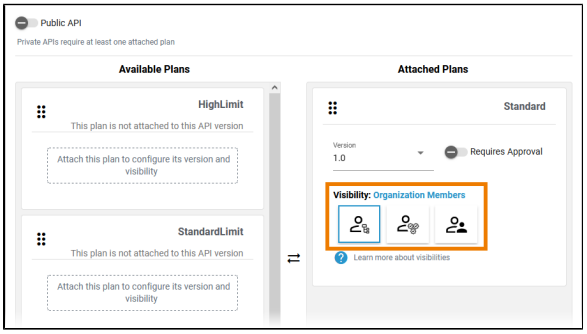


If you change the type of the API, you must confirm your choice in a separate pop-up. Read the information carefully before you change the type.

> ⚠ It is not recommended to change the API type once the API has been published.

Defining the Visibility

For detailed information about the visibility concept, refer to The Concepts of API Management.

	If you have enabled the option **Public API**, you can define the desired visibility for your API below.
	If you have chosen to make your API **private**, you need to attach at least one plan to section **Attached Plans** first. See Attaching Plans. The visibility is then defined for each plan separately.

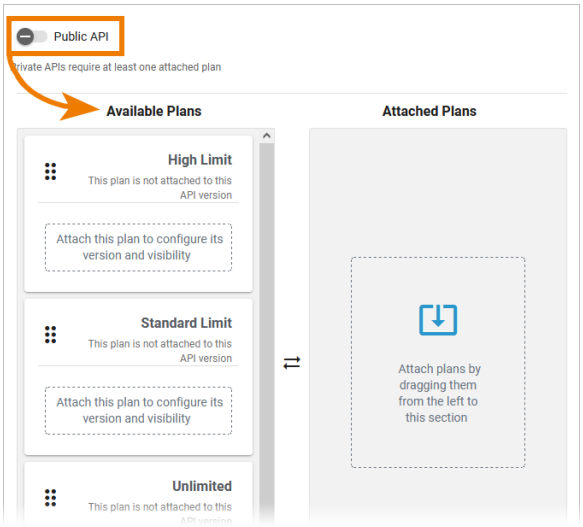
The handling is the same for both API types: Click on the option you want to apply.

Visibility	Description
Organization Members (default)	• All members of the organization. • The PAS user must be listed in one of the Identity Management groups **API-Management-Users**, **API-Management-Administrators** or **API-Management-Developer-Portal-Users** .
API Management Users	• Any PAS user listed in Identity Management groups **API-Management-Users** or **API-Management-Administrators** .

API Developer Portal Visitors	• Any PAS user listed in Identity Management group **API-Management-Developer-Portal-Users** and any user who visits the API Developer Portal, whether logged in or not.

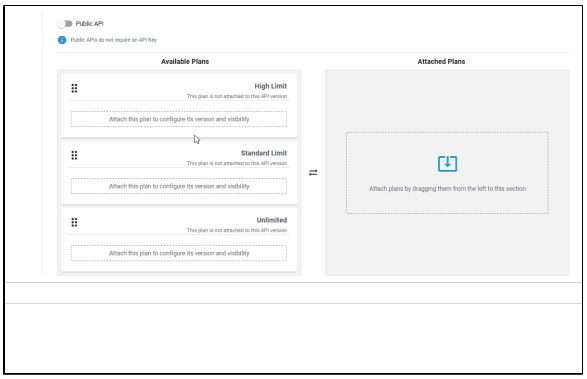
> In API Management, a user can see all APIs for which he has explicit permissions (roles **Viewer** and **Editor**). The permissions are assigned in the corresponding organizations, refer to Administrating Organization Members > Applicable Roles.
> In addition, a user can be assigned the profile **api_management_admin** in the user management (refer to Administration Guide) which makes him a "superadmin" who can basically see and do everything in API Management (refer to Administration for details).

Attaching Plans



If option **Public API** is disabled, you need to attach at least one plan to the API.

All plans that are available in the corresponding organization are displayed below.



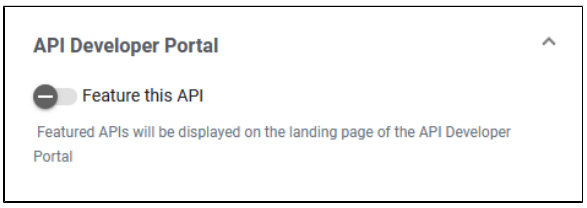
> Click on the image to run through the animated version once. Click again to repeat.

To attach a plan, drag them from section **Available Plans** to section **Attached Plans**.

Once a plan is attached, you can configure the following options:

Option	Description
Version	Use the drop-down to select the version of the plan you want to use.
Requires Approval	Enable this option if a user should be able to use the plan only after granted approval.
Visibility	Click one of the options to define the desired visibility for this plan. This affects the view in the API Management itself as well as in the API Developer Portal. See Defining the Visibility for an overview on the available visibility options. For detailed information about the visibility concept, refer to The Concepts of API Management.

Feature in API Developer Portal

	In section **API Developer Portal** you can determine if you want to display the API on the landing page of the API Developer Portal. Enable option **Feature this API** to show this API directly on the portals's first page. This setting is valid for all versions of the API.

API Tab "Documentation"

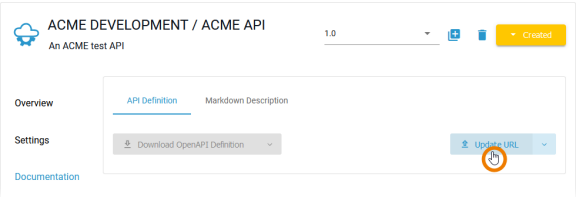
If the API is to be offered to a larger group of users, good documentation is helpful for further usage. An API definition file allows consumers to better understand how to use your API. If you want to test your API directly from API Management, it is necessary to have an API definition.

> PAS 24.1 **The OpenAPI definition is adapted, when the API is published:**
>
> - The API's name, version number and markdown description are taken over in the code displayed in the definition editor.
> - Adding or removing policies enriches the OpenAPI definition.
> (This also applies to the whole policy chain, even if the definition editor in the API details will only show API-related policy code.)

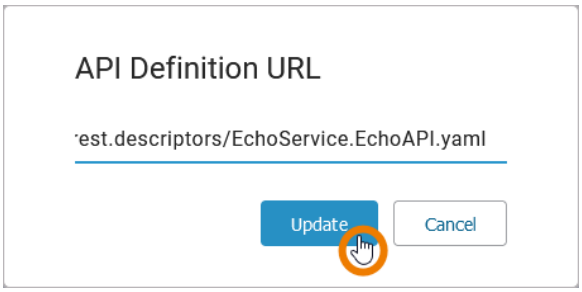
Adding API Definition

If you have imported the API from the PAS Administration, the API definition is populated automatically. Alternatively, you can load a definition from a URL, or upload a definition file. API definition files must be valid JSON or YAML files following the OpenAPI specification or valid WDSL files according to the WSDL specification.

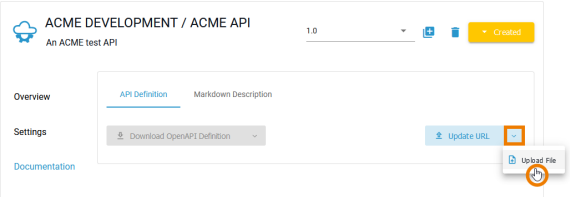
If you want to load the API definition from a URL source, click **Update URL**:



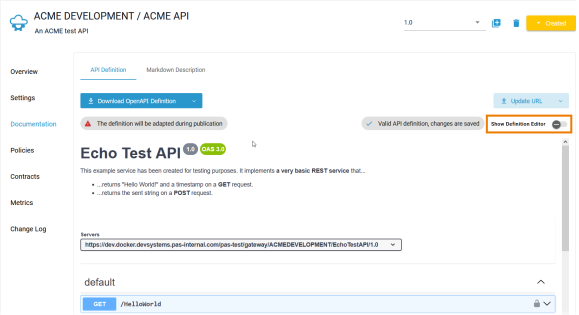
Enter the URL to your definition source:



If you want to upload a definition file instead, click the arrow to access the additional option **Upload File**:



If your definition is saved, the content is shown below. In addition, option **Show Definition Editor** is displayed:



The definition editor allows you to adapt **some** content of the displayed definition, but changes on the policy logic will be overwritten during reload of the editor or publication of the API. For detailed information about the definition editor refer to API Settings > API Definition.

API Tab "Policies"

A policy is a rule or a set of rules API Management uses to manage access to your APIs. Policies are applied to all API requests and represent a unit of work applied at runtime to the request by API Management. Policies are applied through a policy chain: when a request to an API is made, API Management creates a chain of policies to be applied to that request. The policy chain is applied to the request in a fixed order: Client policies are applied first, then policies added to plans, and finally policies added to the API itself (refer to Policies > Policy Chain for details).

> Refer to chapter **Policies** for an overview of the standard policies supplied with **Scheer PAS** *API Management*. Page Attaching Policies explains how to attach and configure a policy.