Configuring an API

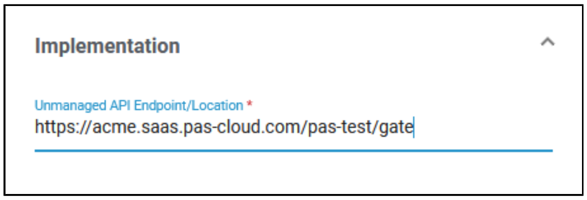
If you have created an API, you must configure it before you can publish the API to the API Developer Portal. Refer to API Settings for an overview of the available options in the API details view.

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

 Implementation Unmanaged API Endpoint/Location * https://acme.saas.pas-cloud.com/pas-test/gate	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):

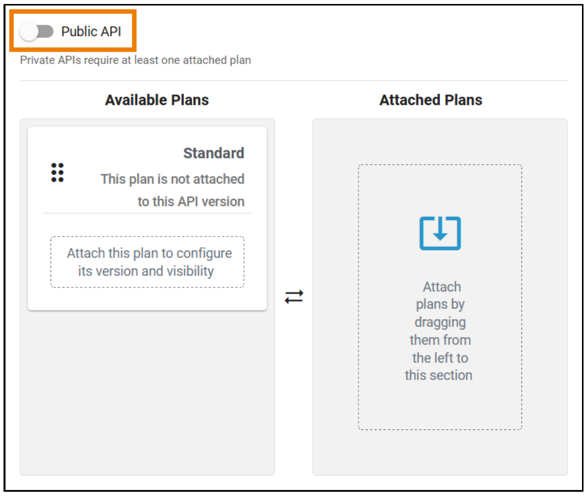
On this Page:

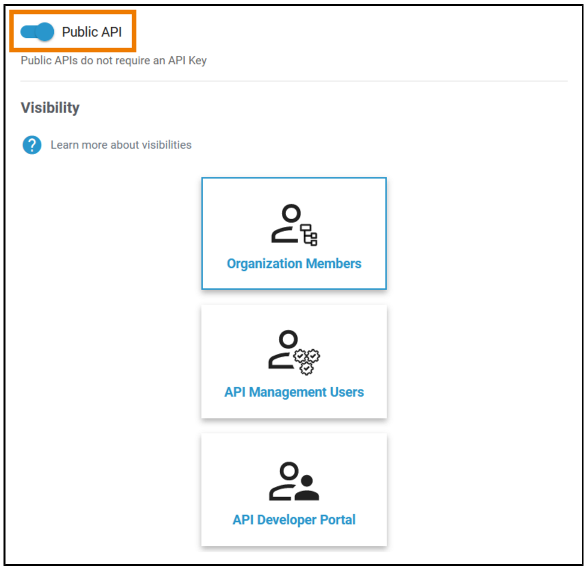
Related Pages:

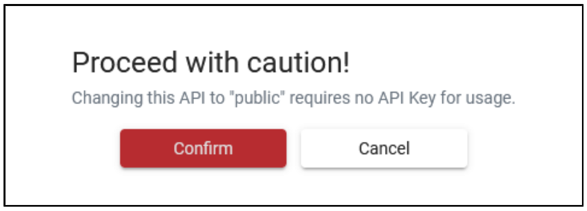
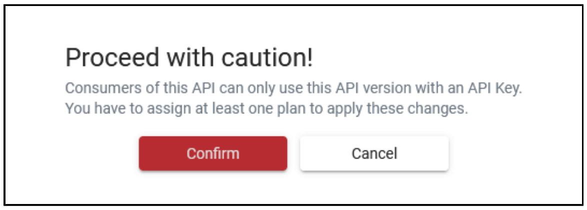
- APIs
  - API Settings
  - Importing APIs
  - Publishing an API

Related Documentation:

- OpenAPI Specification
- WSDL Specification

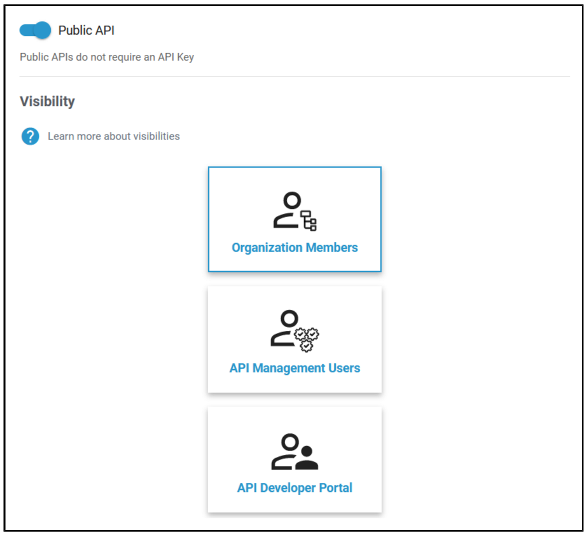
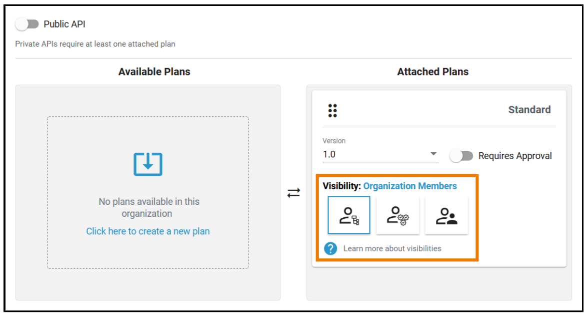
 Private APIs require at least one attached plan This plan is not attached to this API version Attach this plan to configure its version and visibility Attach plans by dragging them from the left to this section	By **default**, newly created or imported APIs are created as **private APIs**. A private 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.

 Public API Public APIs do not require an API Key Visibility Learn more about visibilities Organization Members API Management Users API Developer Portal	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.

 Proceed with caution! Changing this API to "public" requires no API Key for usage.  Proceed with caution! Consumers of this API can only use this API version with an API Key. You have to assign at least one plan to apply these changes. 	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.

 Public API Public APIs do not require an API Key Visibility Learn more about visibilities Organization Members API Management Users API Developer Portal	If you have enabled the option **Public API**, you can define the desired visibility for your API below.
 Public API Private APIs require at least one attached plan Available Plans No plans available in this organization Click here to create a new plan Attached Plans Standard Version 1.0 Requires Approval Visibility: Organization Members Learn more about visibilities	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.

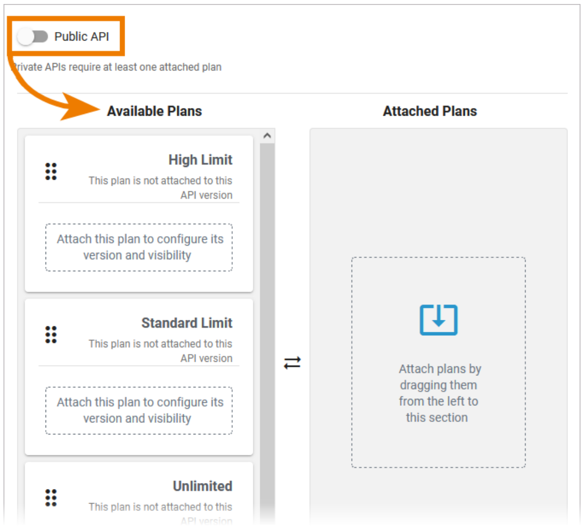
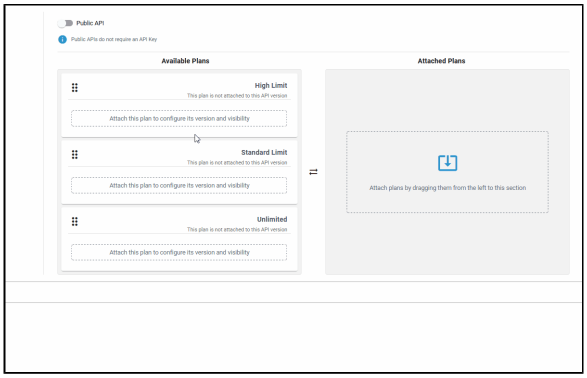
The handling is the same for both API types: Click on the option you want to apply.

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.

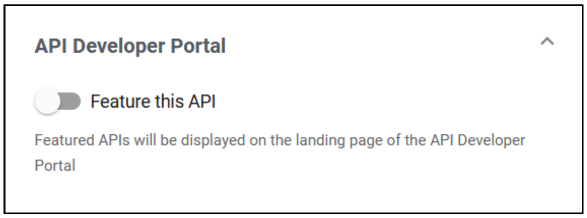
In API Management, a user can see all APIs for which he has explicit permissions (roles **Viewer** and **Editor**). The permissions are assigned in the corresponding organizations, refer to Administrating Organization Members > Applicable Roles.
In addition, a user can be assigned the profile **api_management_admin** 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

 Private APIs require at least one attached plan This plan is not attached to this API version Attach this plan to configure its version and visibility Attach plans by dragging them from the left to this section Public API Available Plans Attached Plans High Limit Standard Limit Unlimited	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.
 Public APIs do not require an API Key This plan is not attached to this API version Attach this plan to configure its version and visibility Attach plans by dragging them from the left to this section Public API Available Plans Attached Plans High Limit Standard Limit Unlimited 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.

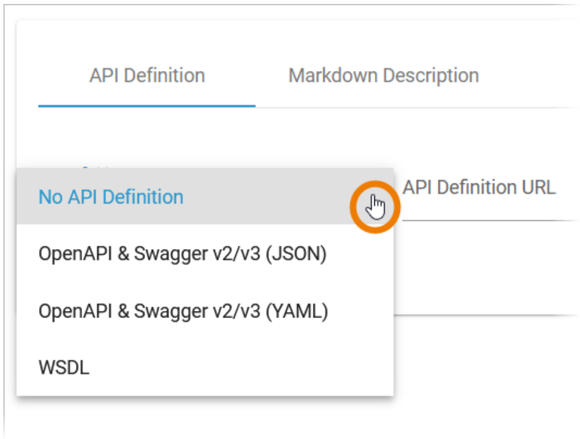
Feature in API Developer Portal

 **API Developer Portal** Feature this API Featured APIs will be displayed on the landing page of the 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.

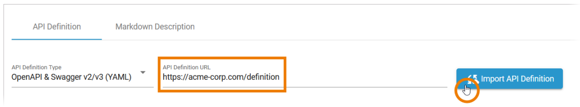
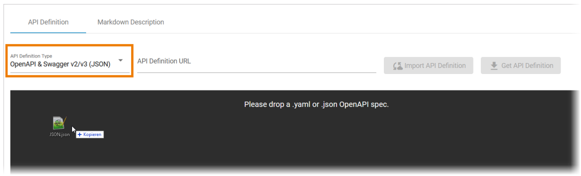
API Tab "Documentation"

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.

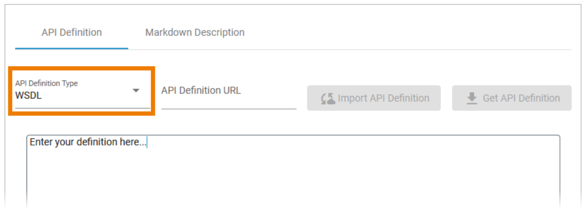
Adding API Definition

 API Definition Markdown Description No API Definition OpenAPI & Swagger v2/v3 (JSON) OpenAPI & Swagger v2/v3 (YAML) WSDL API Definition URL	API Management supports various types of definition files: - **OpenAPI & Swagger v2/v3 (JSON)** - **OpenAPI & Swagger v2/v3 (YAML)** - **WSDL**

	Open the drop-down list in field **API Definiton Type** to select the type you want to use. ⓘ API definition files must be valid JSON or YAML files following the OpenAPI specification or valid WDSL files ac

	cording to the WSDL specification.
 API Definition Markdown Description API Definition Type: OpenAPI & Swagger v2/v3 (YAML) API Definition URL: https://acme-corp.com/definition Import API Definition	If you want to load the API definition from a URL source, enter the URL in field **API Definition URL** and click **Import API Definition** to start the upload.
 API Definition Markdown Description API Definition Type: OpenAPI & Swagger v2/v3 (JSON) API Definition URL Import API Definition Get API Definition Please drop a .yaml or .json OpenAPI spec. JSON.json + Kopieren	To provide a JSON or YAML file, just drop it on the editor below. The editor allows you to adapt the displayed def

	inition. Manual changes are automatically saved, but using **Import API Definition** again overrides the manual changes.

 API Definition Markdown Description API Definition Type WSDL API Definition URL Import API Definition Get API Definition Enter your definition here...	A separate editor is available for definition type WSDL. Enter your definition manually.

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 add a definition manually:

Definition Options	Instructions
Adding a Definition Manually	If no definition has been imported, you can add a definition manually: 1. Select a definition type from the dropdown box. 2. Paste, or drag and drop the definition to the empty definition box.
Loading a Definition from a URL	If no definition has been imported or if you need to update an existing definition, you can import a definition from a URL: 1. Select a definition type from the dropdown box. 2. Add the URL to a Swagger or WSDL file containing the definition. 3. Click **Import API Definition**.
Updating a Definition	If the definition of an imported API needs to be updated, you have to do this manually as there is no automatic re-import: 1. Download the definition file from the source (e.g. from the integration component). 2. Replace the content of the definition box with the content of the downloaded file (manually or by using **Import API Definition** again).

ⓘ Adding or removing policies does not enrich the Open API documentation. You need to adjust your documentation manually. For more information on REST documentation and how to add documentation to xUML services, refer to Bridge Guide > Documenting a REST Service.

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.