

Exposing Designer Services via API Management

For xUML services that have been deployed from the Designer as a container, secured endpoints are created automatically. However, these services are only usable internally and are not exposed to users outside the company. If you want to make them available to others, you can publish them via **Scheer PAS API Management** and restrict their usage with additional policies.



The following explanations apply to xUML services without user context (forms or role check).

On this Page:

- [Managing the Designer Service](#)
- [Configuring Your API](#)

Managing the Designer Service

ACME_SupportManager

Search Criteria Assets

- + Base Types
- Connectors
- Process**
- Forms
- API
 - SupportCase
 - SupportAPI
 - + supportcases
- Implementation
 - Service
 - + Helper
 - + MongoDB
 - + REST
 - + Support
- Libraries

In the Designer, you have created a REST service that contains neither forms nor a process.

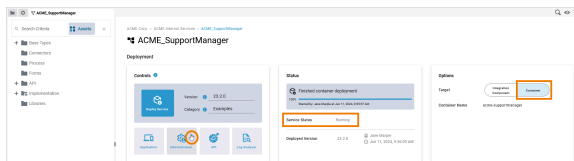
Example:


We use a REST service named **SupportAPI** that handles support cases which are stored to a MongoDB.

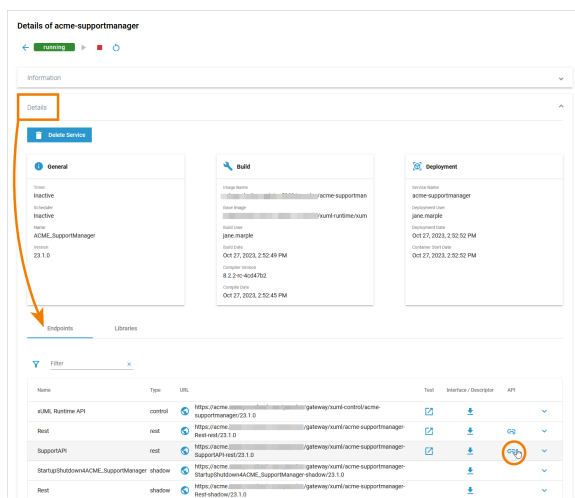
Related Documentation:

- [API Management Guide](#)
 - [Creating an API](#)
 - [Publishing an API](#)
 - [Creating a Plan](#)
 - [Developer Portal](#)
- [Administration Guide](#)
 - [Controlling Containerized xUML Services](#)

Choose the deployment target **Container**. From the service details page, open the service in the PAS Administration:



In the Administration, you can access the service details, which also contain the information about the service endpoints. Use **Import API**  to transfer the endpoint to API Management:



You are now redirected to API Management and a wizard will guide you through the creation of the API (refer to [Creating an API](#) for a step-by-step guide).

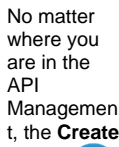
Configuring Your API

You imported the API to API Management, because you want to make it (publicly) available for others to consume. If you want to control the use of your API, differentiate between access groups and benefit from various metrics, we recommend creating a private API (refer to [API Types: Public vs. Private](#) for further details).

Example: Our example service handles support cases. The API should be usable by two different access groups:

- Users with limited permissions who can only create support tickets.
- Support administrators who can create and manage support tickets.

Therefore we choose to create a private API with two different plans.



Open the menu and click **Create Plan** to add a new plan.

✓ Select Entity

✓ Choose Organization

✓ Configure Details

4 Summary

Please confirm if you want to create the plan with the following settings:

Name
Support Case Creator

Version
1.0

Description
Allows the creation of support ticktes

Cancel

Back

Create Plan

Follow the wizard through some simple steps. You need to...

- ... select the organization in which the plan should be created.
- Enter a name for the plan.
- Enter a version for the plan.

You can also enter a description, but this is optional.

Example:

We create a plan for our first use case (users with limited permissions).

jane.marple / Support Case Creator

1.0

Created

Allows the creation of support ticktes

Overview

Policies

Change Log

Attached Policies

No policies attached

Click here to attach new policy

If you want to create plans for users with limited access, you have to assign appropriate policies.

On a newly created plan, you can use the link **Click here to attach a new policy** in the Overview tab. You can also switch to tab **Policies** and add your policies here.



Add Policy for PLAN: [SupportCaseCreator](#)

1 Select Policy 2 Configure Policy 3 Summary

Security

Ignored Resources

Allows the user to prevent access to some API resources without blocking access to all API resources.



Cancel

The policy wizard supports you during policy configuration. Click on the policy tile to open the policy configuration.

Example:

We choose the **Ignored Resources Policy**.

Add Policy for PLAN: [SupportCaseCreator](#)

1 Select Policy 2 Configure Policy 3 Summary

Ignored Resources

Basic Configuration

Use this policy to manage the list of API routes to ignore.

<input type="checkbox"/>	Path	Method
<input type="checkbox"/>	/supportcases/*	DELETE
Regular expressions must be written in java syntax .		
<input type="checkbox"/>	/supportcas	GET
Regular expressions must be written in java syntax .		

Add

Delete

Items per page: 20

1 - 2 of 2

< > >>

Cancel

Back

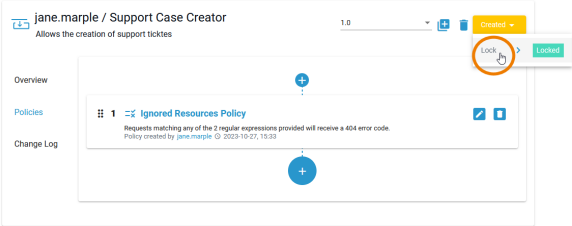
Next

Now, configure the policy according to your requirements.

Example:

We configure the **Ignored Resources Policy** so that support case creators cannot receive or delete support requests.

Click **Next** to see a summary of your configuration. Confirm the summary to attach the policy.



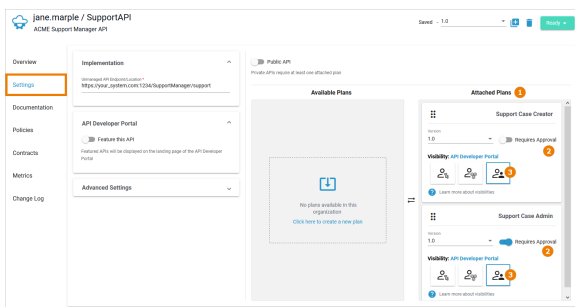
The policy is added to the plan, you are now able to lock it.

Only locked plans can be used by APIs in the organization. Refer to [Locking a plan](#) for details.



In the same way, we create a second plan for support case administrators.

Administrators don't have any restrictions because they should be able to access all support tickets. Therefore, their plan has no policies assigned.



Now, you need to assign the plans to your API. Go to the API details page, open tab **Settings** and do the following:

1. Attach the plans you want to use with drag & drop.
2. Set **Require Approval** for the plans that are not to be available to everyone.
3. Choose the visibility of the plans.

✔ **Expert Advice**

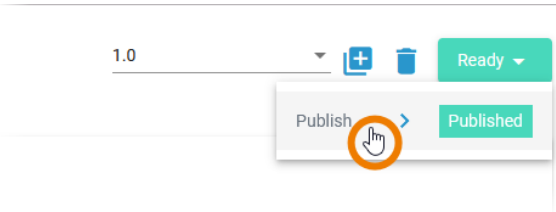
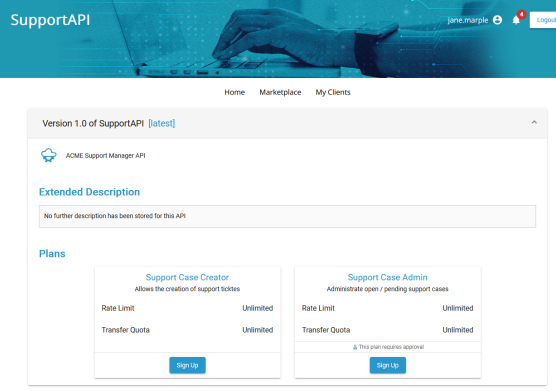
Read more about the visibility concept on page [The Concepts of APIManagement](#).

Example:

-
1. **Attach:**
We want to use both created plans, so both are attached to the API.

2. **Require Approval:** Everyone should be able to use the API for support ticket creation, but we want to approve the users with admin permission. Therefore, the usage of plan Support Case Admin needs approval.

3. **Visibility:** Both plans should be visible to all visitors of the API Developer Portal.

 <p>A screenshot of a software interface showing a version control or deployment menu. At the top, it says '1.0' next to a dropdown arrow. Below this are icons for a plus sign, a trash can, and a green button labeled 'Ready'. A modal window is open, showing a 'Publish' button with a hand cursor icon and a 'Published' button.</p>	<p>You have completed the necessary steps to configure your API. Now, you can publish it to make it publicly available.</p>
 <p>A screenshot of the 'SupportAPI' developer portal. The header shows 'SupportAPI' and a user profile 'jane.marple' with a 'Logout' button. The main content area is titled 'Version 1.0 of SupportAPI [latest]' and shows 'ACME Support Manager API'. Under 'Extended Description', it says 'No further description has been stored for this API'. Under 'Plans', there are two options: 'Support Case Creator' (allows creation of support tickets, unlimited rate limit and transfer quota) and 'Support Case Admin' (administrate open / pending support cases, unlimited rate limit and transfer quota). Both plans have a 'Sign Up' button.</p>	<p>The API is available in the API Developer Portal. Users can now sign up for it.</p>