APIs

What is an API?

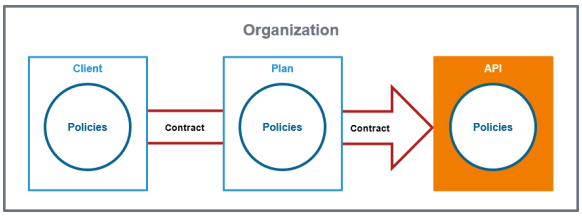
APIs represent real backend APIs (Application Programming Interfaces). An API is also known as a **service**, which offers a HTTP, REST or SOAP interface that can be invoked remotely by a client.

An API consists of a set of meta data including name and description as well as an external endpoint defining the API implementation. The external API implementation endpoint includes:

- The type/protocol of the endpoint (REST or SOAP).
- The endpoint content type (XML or JSON).
- The endpoint location (URL) so that the API can be properly proxied to at runtime.

Scheer PAS *API Management* provides a way to turn unmanaged (raw) back-end APIs into **managed** APIs by attaching policies to them. Any policies configured on an API will be applied at runtime, regardless of the client and API contract. Therefore authentication is a common policy configured at the API level.

An API has to be fully configured, including policies and implementation (and in case of public APIs including plans) to be published. If the API has been published to the gateway it can be consumed - in case of private APIs by clients.



API Contracts and API Keys

Only public APIs can be accessed by any consumer. The only way for a client to consume a private API is by using an API contract. An API contract is a link between a client and an API through a plan offered by that API.

API contracts can only be created between clients and published APIs which are offered through at least one plan. An API contract cannot be created between a client and a public API.

When a client version is created, the system generates a unique API Key. This key is unique per client version and the same for all contracts of this version. All requests made to the API by a client through the gateway must include this API Key to identify the used client version.

> You can forward the X-API-Key to the service using the **API Key policy**. However, you cannot define your own value for the X-API-Key, since the gateway uses the key to identify the clients.

However, **the API Key is not a security feature**! API Keys are not encrypted and visible:

- in the request header,
- to people who have access to API Management metrics/the Log Analyzer,
- in the logs of the integration component (Bridge) if you are using the **API Key** policy.

So, API Keys need to be handled in a secure way - otherwise attackers may be able to use the API Key to gain access to your system.

> As per definition, API Keys are used to identify technical clients only and, subsequently, to apply related policies. **Do not use API Keys to authenticate users.**
>
> Authentication should always be implemented via a dedicated security policy (refer to Policy Configuration > Security Policies and API Security: Authentication and Authorization).

Finding an API

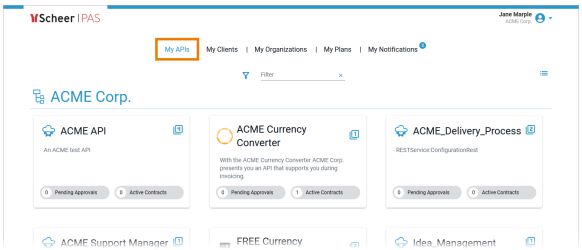
If you are looking for an API that has already been created, go to tab **My APIs**. It shows a list of all APIs your user is allowed to see, grouped by organizations:

On this Page:

Related Pages:

- API Settings
- Creating an API
- Configuring an API
- Importing APIs
- Publishing an API
- Retiring an API
- Testing APIs
- Deleting an API

- Clients
- Contracts
- Plans
- The Concepts of API Management



To revise the settings of an API, you need to open its details page (see API Settings for further information).

For detailed information about navigating and filtering the list refer to Working With the API Management.