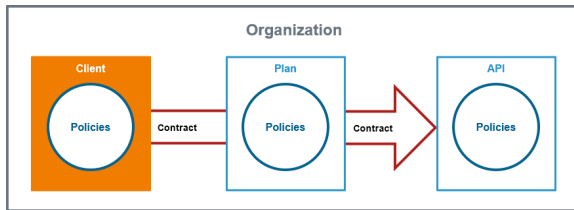


Clients

What is a Client?

The client is the consumer of the API. Typical API consumers are for example mobile or B2B applications. Optionally, policies can also be defined on a client.



Each client can consume multiple APIs within the API Management. Therefore, a contract is created between a client and the APIs it wishes to consume. Once the contract is created, the client can be registered with the gateway. Policies and contracts can be added and removed at any time. However, after any changes are made, the client must be registered again.

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 a Client

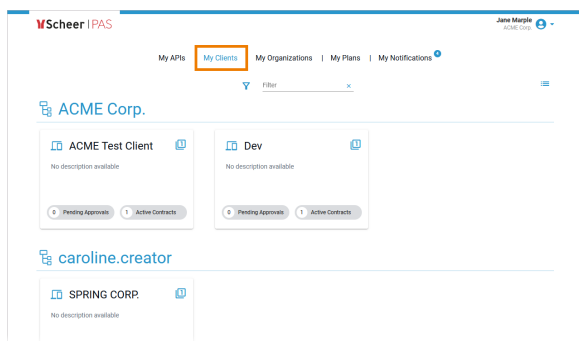
If you are looking for a client that has already been created, go to tab **My Clients**. It shows a list of all clients your user is allowed to see, grouped by organizations:

On this Page:

- [What is a Client?](#)
 - [API Contracts and API Keys](#)
- [Finding a Client](#)

Related Pages:

- [Client Settings](#)
- [Creating a Client](#)
- [Registering a Client](#)
- [Retiring a Client](#)
- [Deleting a Client](#)
- [APIs](#)
- [Contracts](#)
- [Plans](#)
- [The Concepts of API Management](#)



To revise the settings of a client, you need to open its details page (see [Client Settings](#) for further information).



For detailed information about navigating and filtering the list refer to [Working With the API Management](#).

If your user is only authorized to access the API Developer Portal, you can view the list of your clients here. Simply go to tab **My Clients**. The navigation on the right side supports you to browse the page.

