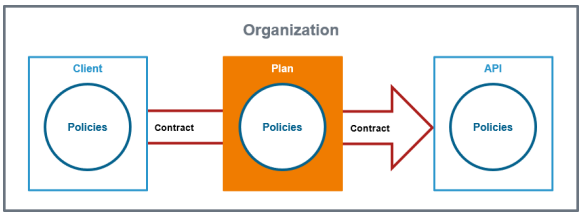
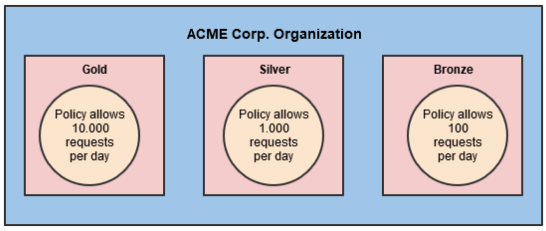
Plans

What is a Plan?

A plan is a set of policies that defines the level of service API Management provides for an API. When a private API is consumed, it may be consumed through a plan.



An organization can have multiple plans associated with it. Typically each plan within an organization consists of the same set of policies but with different configuration details.



Example:

Within the **ACME Corp. Organization** three differents plans have been created:

On this Page:

Related Pages:

- Plan Settings
- Creating a Plan
- Locking a Plan
- Deleting a Plan

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

	• A **Gold** plan with a rate limiting policy that restricts consumers to 10.000 requests per day. • A **Silver** plan with a rate limiting policy that restricts consumers to 1.000 requests per day. • A **Bronze** plan with a rate limiting policy that restricts consumers to 100 requests per day.

Once a plan has been fully configured - all desired policies have been added and customized - the plan must be locked. Only locked plans can be used by APIs. This is necessary to prevent that API providers change the details of the plan while the client developers are already using it.

> ⚠ Once a plan is locked, it cannot be revised anymore. However, you can still create a new version of this plan.

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:

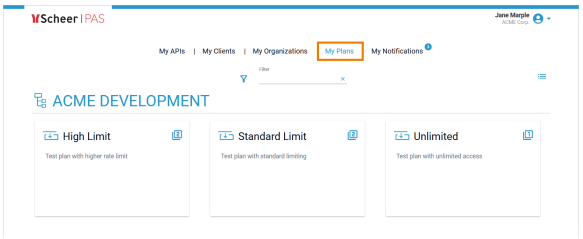
- in the request header,
- to people who have access to API Management metrics/the Log Analyzer,
- in the logs of the integration component (Bridge) if you are using the **API Key** policy.

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 Plan

If you are looking for a plan that has already been created, go to tab **My Plans**. It shows a list of all plans your user is allowed to see, grouped by organization:



To revise the settings of a plan (only possible if the plan is not locked yet), you need to open its details page (see Plan Settings for further information).

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