LANTMÄTERIET

DOKUMENTVERSION: 1.0 2020-08-20

# Quickstart - "first time user"

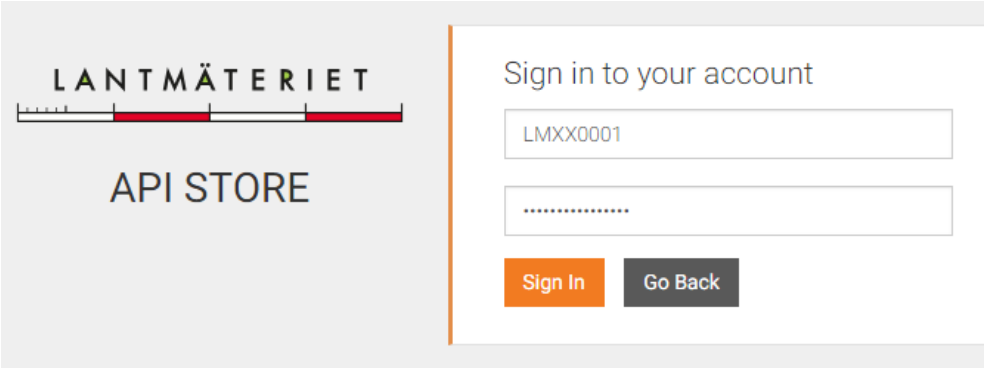
# Table of contents

## Log in

The API portal is available in our two environments:

- Production environment
- Verification environment

*Figure 1. Screenshot from the login page for the API portal.*



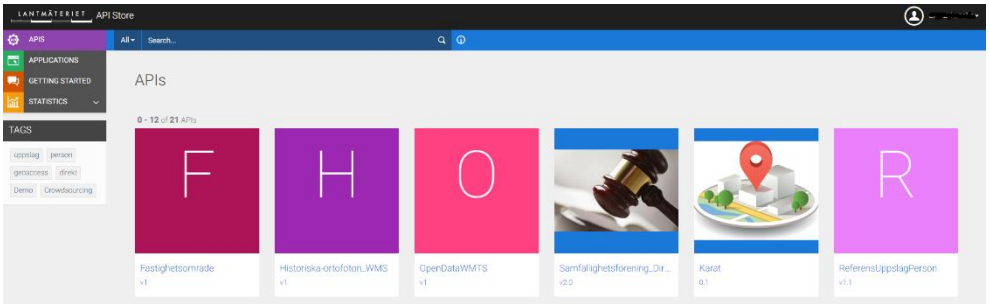

This is where you log in using your username and password for each environment.

## First page

At login, you will find the directory of the APIs and services that are available just for you.

The API:s/services shown here are based on the services your account is authorized to access. If the API/service you are looking for is not visible it is probably because you haven't ordered permission for this particular service. Contact Geodatasupport for ordering.

*Figure 2. Screenshot of the first page of the API portal.*




In the menu to the left there are four options:

- APIS - the catalogue (even after first login) where available API:s/services are gathered
- Applications - the applications/groups you've created
- Getting started - help section
- Statistics - subpages with different gatherings of statistics

## Create an authorization key for API/Service

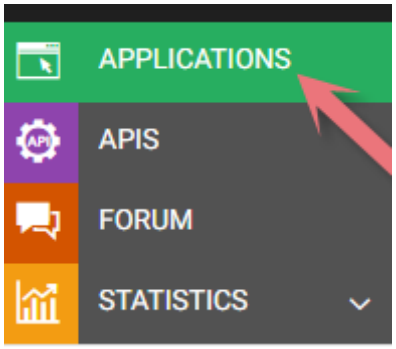
The basic principle of the API portal and its functions is based on gathering the API:s/services to be consumed under different Applications. An Application is, in short, a grouping created to gather and control/restrict access to a gathering of API:s/services. Each Application is assigned a unique authorization key which is then used when consuming the API:s/services linked to the same Application (a API/Service may be part of several Applications).

With this approach, groupings with specific use targets can be created and provide higher security, to the contrary where an authorization key would otherwise give access to ALL API:s/services at the same time. Examples of use cases with this approach:

- a web application should be posted externally on the company's website. An Application is created with the appropriate name and only the API:s/services needed in the Web application are added to the grouping.
- hired consultants need access to certain API:s/services for an assignment. An Application is created with access to only the API:s/services the assignment requires, and a validity time for the authorization key is specified.
- a workgroup or department has tasks that require access to certain API:s/services. Because of privacy or management of personal data an Application is created with the API:s/services needed.

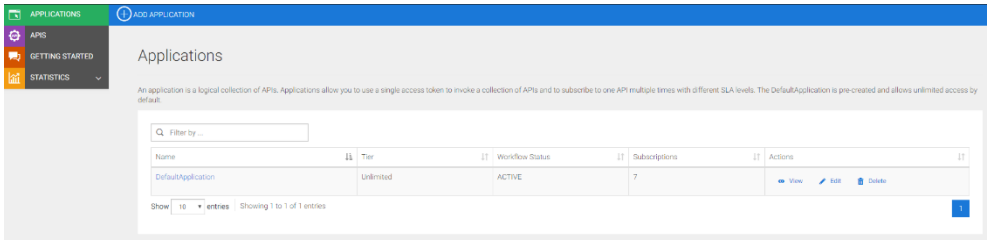
In the menu on the left, select **Applications**.

*Figure 3. Screenshot of the main menu in the API portal.*



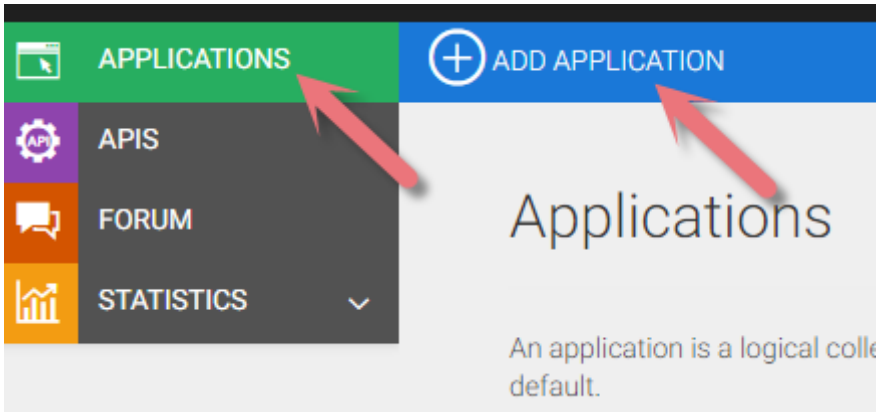
A list of all the applications already created for the current account is now displayed. All accounts have an Application from the start called "Default Application".

*Figure 4. Screenshot of the page where "Applications" are listed.*



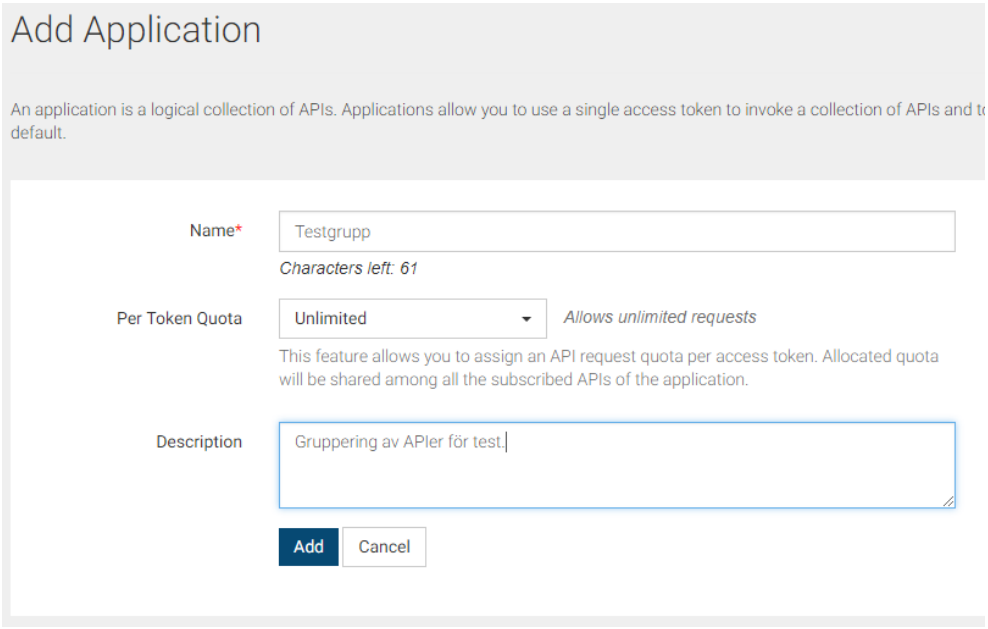

To create a new Application, select **Add Application** at the top of the page.

*Figure 5. Screenshot of "Add Application".*



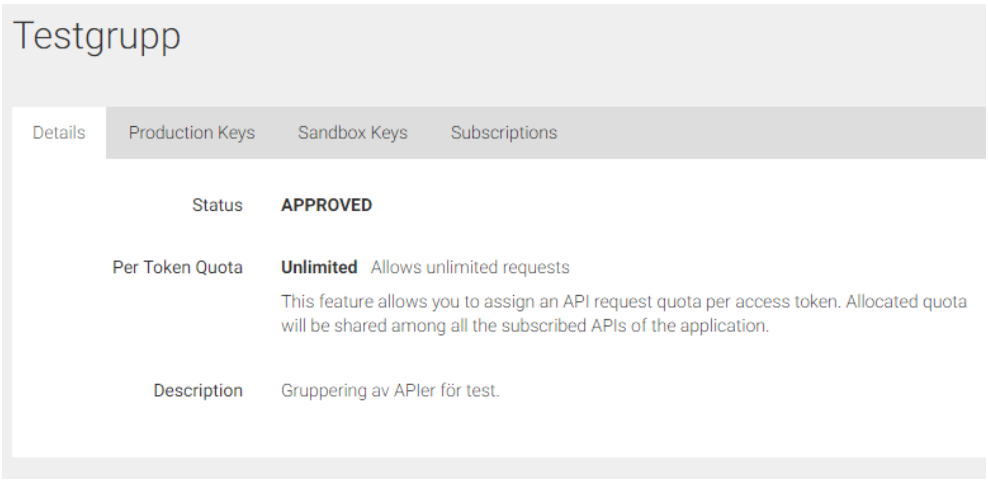
Choose a suitable name for your new Application, as well as a description. **Per Token Quota** allows you to limit the number of calls per minute against the API:s in the grouping, if no restriction is desired, U*nlimited* is specified.

*Figure 6. Screenshot of fields to be filled in when creating an "Application".*



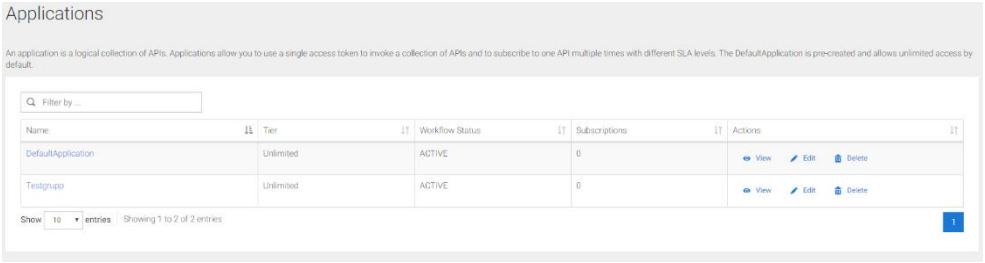

Press **Add** and your new Application will be created.

*Figure 7. Screenshot of test group.*



The new grouping is now visible in the list under the **Applications** menu.

*Figure 8. Screenshot of groupings.*




To create a unique authorization key for this Application, click on the name and select the **Production Keys** tab.

Since no authorization key has been created previously, the message "**No keys found**" appears.

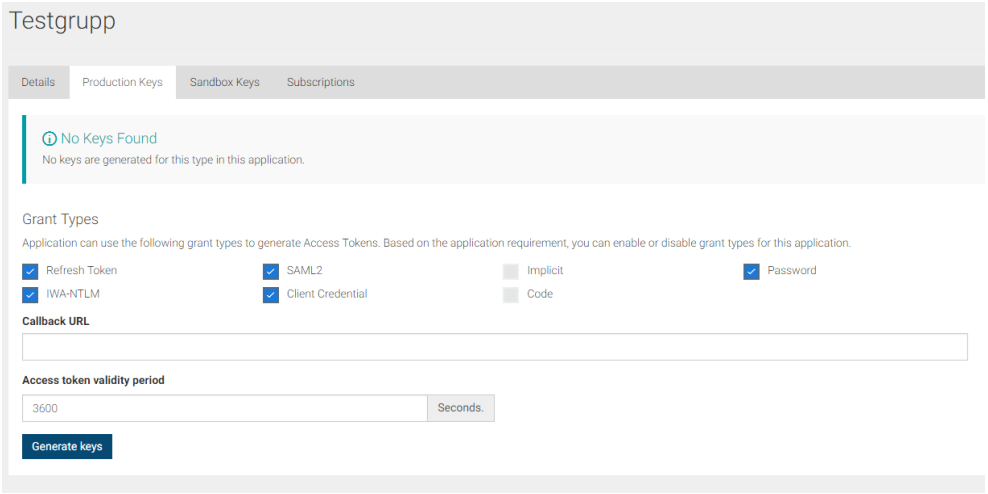
The authorization key is created by clicking **Generate keys**. Prior to this, a validity key should be specified for the authorization key. The validity period is specified in seconds and controls how long the authorization key is valid. The time is mainly intended to be used in the automatic generation of keys via the request from consuming applications or systems, which is described in more detail in a later chapter of this guide.

If you have no need for a time-limited authorization key, but instead want to create a **static authorization key**, the **Access token validity** period is set to **-1**.

**Note:**
Our recommendation is to always use automatic key update via calls from your application or system. Use of static key means a much lower level of security.

Press **Generate Keys** to create an authorization key.

*Figure 9. Screenshot of "Production Keys".*



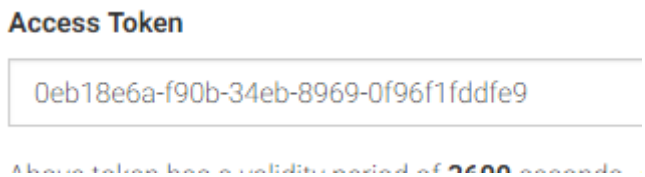

The page is now filled with information.

**Note**: If the keys are hidden on the page, press **Show Keys** at the top and the keys will appear in plain text.

At the top of the page are two keys; **Consumer key** and **Consumer secret**. These are used for automatic renewal of authorization key (read more about this in a separate chapter).

At the bottom of the page is the **Authorization key** under the title **Access Token**. The key is made up of random characters that together creates a unique character string.

*Figure 10. Screenshot of an "Access Token".*




If needed, a new key can be generated by clicking the **Re-generate** button.

**Note:**

If a new key is created, the old key is destroyed and disabled. This means that if the old key is used in the majority applications/systems, all of them must be updated with the new key.

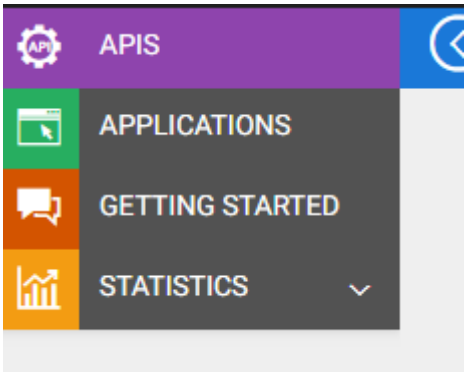
## Add APIs / services for access

After creating an Application/grouping and creating an authorization key for this, you can now add the APIs/services to be consumed.

The following procedure is repeated for each API / service to be added.

Go to the first page by clicking **APIs** in the menu on the left.

*Figure 11. Screenshot of the APIS menu.*



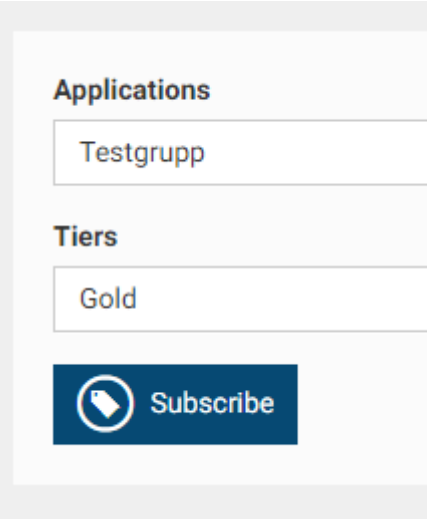

Click on an API/service you want to add to the grouping.

At the top right of the page there is a drop-down list - **Applications** - where you select the Application/grouping to use. In this case, we select Test Group that we previously created.

*Figure 12. Screenshot of scroll bar with "Applications".*

**Tiers** is used to place an API/service-specific limit on the number of calls per minute allowed.

*Figure 13.Screenshot of Tiers.*

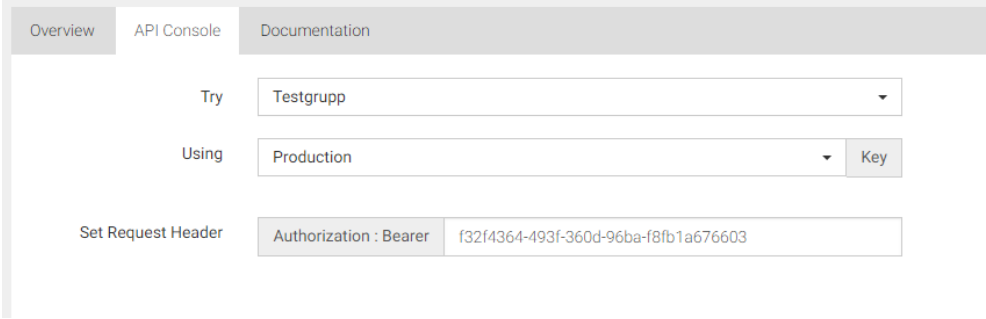



Then select **Subscribe** and the API/service is added to the selected grouping.

*Figure 14. Screenshot of when creating a subscription.*

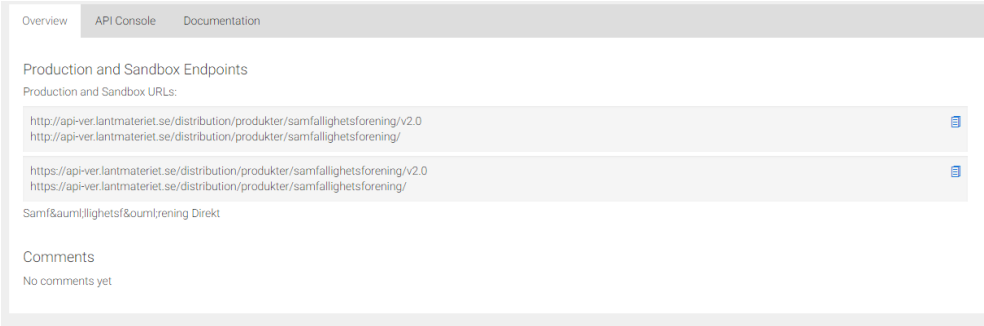

Under the **API-Console** tab, the authorization key is then found.

*Figure 15. Screenshot of API-Console.*



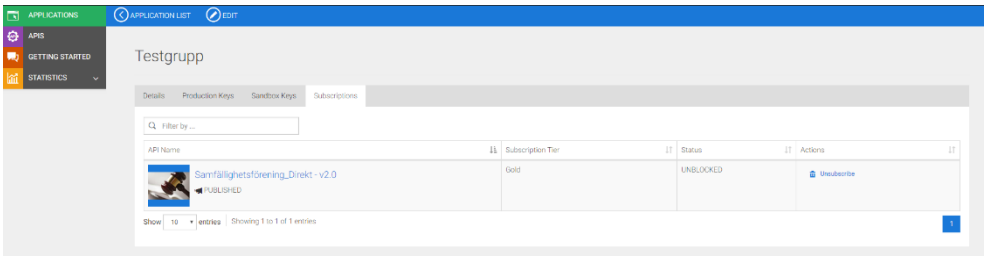
The **Overview** tab then lists the addresses used to connect to the API/service in software, applications or systems.

*Figure 16. Screenshot of Overview.*




You can see the current API:s/services associated with an Application/Grouping by clicking into the Grouping, and then selecting the **Subscriptions** tab.

*Figure 17. Screenshot of Subscriptions.*




To remove an API/service from a grouping, click **Unsubscribe** under Actions in the far right.