JUNTA DE ANDALUCIA

Consejería de Agricultura, Ganadería, Pesca y Desarrollo Sostenible

Api Manager

Guía Uso

Versión:	v02r00
Fecha última edición:	18/04/2023
Visibilidad del documento: **Público**	**Información Confidencial**: información muy sensible, cuyo acceso, revelación o modificación por parte de personal no autorizado puede causar un daño irreparable para la Consejería o las personas cuyos datos maneja la Consejería. Sólo puede ser conocida y utilizada por un número muy reducido de empleados. **Información Reservada**: información sensible cuyo acceso, revelación o modificación por parte de personal no autorizado puede causar daños o pérdidas significativas a la Consejería o perjudicar sus intereses. Sólo puede ser conocida por un grupo de empleados que la necesiten para realizar su trabajo. **Información de Uso Interno**: información cuyo acceso, revelación o modificación por parte de personal no autorizado supone un riesgo bajo para la Consejería o para su imagen. **Información Pública**: Toda información que no encaja en ninguna de las clasificaciones anteriores y cuya divulgación no supone ningún riesgo para la Consejería, para sus empleados ni para los ciudadanos.

HOJA DE CONTROL

Título	Api Manager		
Entregable	Guía Uso		
Nombre del Fichero	CAPDR-Guia Uso Api Store_v2.1.0.odt		
Autor	CAPDR		
Versión/Edición	v02r00	**Fecha Versión**	18/04/2023
Aprobado por		**Fecha Aprobación**	
		Nº Total Páginas	27

REGISTRO DE CAMBIOS

Versión	Causa del Cambio	Responsable del Cambio	Área	Fecha del Cambio
v01r00	Versión inicial	CAGPDS	Software Factory	19/09/2019
v01r01	Aclaración Gws para petición Tokens	CAGPDS	Software Factory	11/11/2021
v02r00	Actualización APIM 4.1.0	CAGPDS	Interoperabilidad	18/04/2023
v02r10	Actualización apartado 3. Invocación de un API.	CAGPDS	Interoperabilidad	21/05/2024

CONTROL DE DISTRIBUCIÓN

Nombre y Apellidos	Cargo	Área	Nº Copias
María del Valle Del Moral Arroyo	Director de Proyectos	CAPDR	1

ÍNDICE

1 INTRODUCCIÓN

1.1 Objeto

Este documento recoge la "Guía de Uso Básica" para el Sistema Api Manager de la Consejería de Agricultura, Pesca, Agua y Desarrollo Rural (CAPDR).

1.2 Alcance

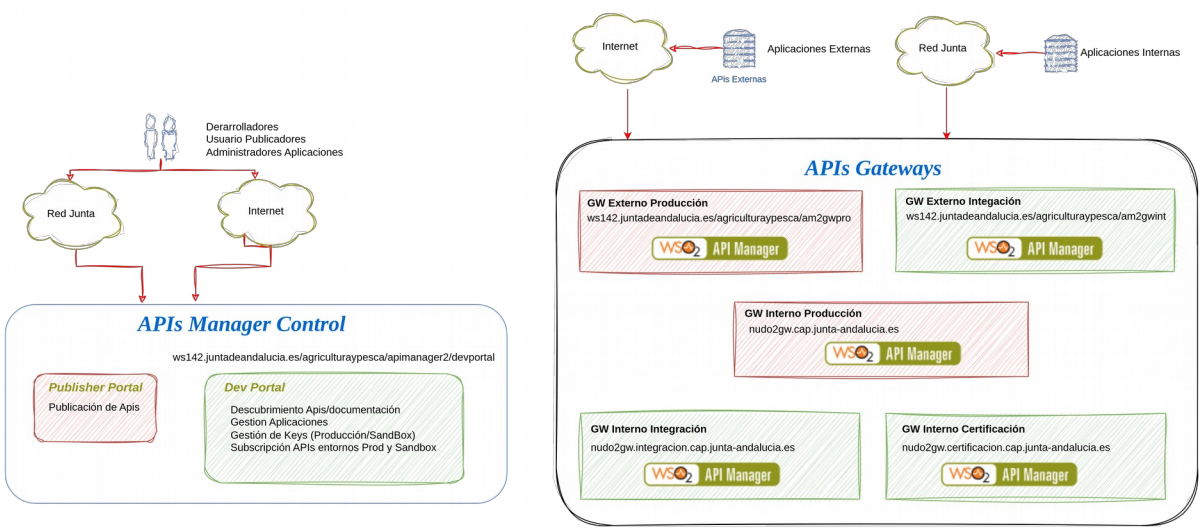
El documento está dirigido a analistas, desarrolladores y administradores que necesiten trabajar con Apis publicadas a través el Sistema API Manager de la CAPDR.

El documento recoge una breve introducción del Sistema Api Manager y describe los pasos necesarios para; registrarse en el mismo, solicitar el uso de un Api y realizar la invocación de dichos Apis, en cualquiera de los entornos disponibles.

2 Api Manager

2.1 Introducción

El diagrama de componentes del Api Manager se muestra en el siguiente diagrama:



API Manager es sistema compuesto por tres componentes:

- Publisher Portal, proporciona un portal web para el alta de Apis y su publicación en los distintos Gateways disponibles.
- Developer Portal, proporciona un portal web para que analistas, desarrolladores y administradores puedan:
  - Descubrir las distintas APIs publicadas por la Consejería, junto a toda su documentación.
  - Solicitar el uso de los Api (suscripción) desde alguna de sus aplicaciones o desarrollos.
  - Solicitar las claves de acceso (keys) para el uso de dichos APIs, a través de alguno de los entorno disponibles; Gateways de producción y pruebas.
- Varios Gateways, a través de los cuales, se publican las APIs en los distintos entornos; producción/pruebas con acceso interno o externo.

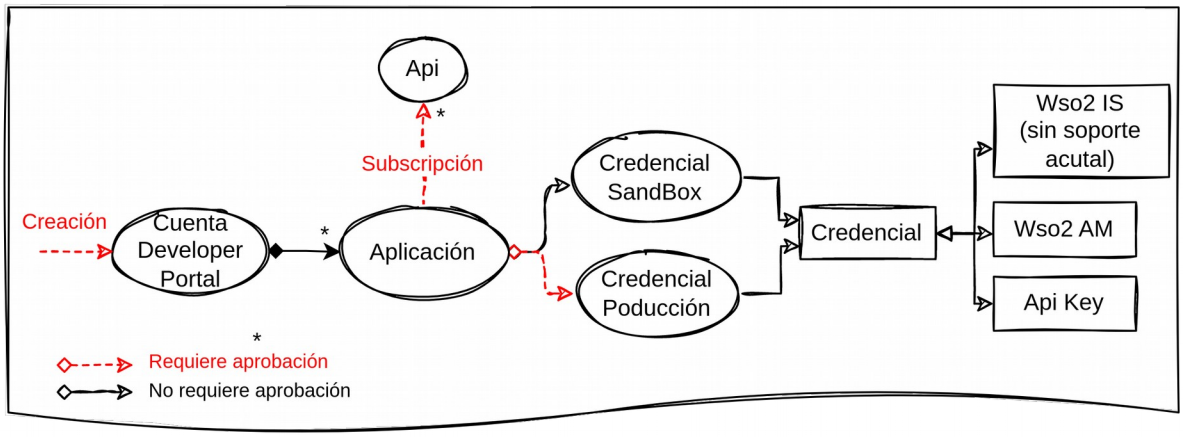
Todas las APIs publicadas a través de los Gateways están securizadas. Para poder hacer uso de estas APIs, se ha de incluir en cada petición un token de acceso válido.

Los tokens se generan realizando una petición al servicio de tokens del APIM/GWs empleando unas credenciales de aplicación.

Para poder obtener estas credenciales será necesario; dar de alta una cuenta en Developer Portal, crear una Aplicación y solicitar la suscripción a los APIs que se necesite.

El concepto Aplicación en APIM es una representación de la aplicación real que consume las APIs, como puede ser; una aplicación móvil, una aplicación web, un dispositivo, etc.

Son un mecanismo que facilita gestionar de forma más eficiente el acceso a los APIs desde las aplicaciones y sistemas consumidores. A cada Aplicación se le asocia unas credenciales para cada entorno (Pruebas/Producción) y un conjunto de APIs a las que tiene acceso (suscripciones).



Actualmente, sólo se publican APIs securizadas con credenciales OAuth2 generadas por el propio APIM. Credenciales del tipo Api Key o generadas por entidades terceras como el WSO2 IS de GUS no están soportadas.

Las aplicaciones le permiten:

- Solicitar desde una misma cuenta distintas credenciales OAuth2
- Controlar que servicios consume cada aplicación concreta.
- Gestión independiente de credenciales para: equipos de desarrollo, aplicaciones en entornos no Producción, aplicaciones de producción, claves para productos comerciales.
- Subscribirse varias veces a un mismo API con diferentes acuerdos de nivel de servicio (SLA).
- Los proveedores de productos, pueden crear credenciales independientes para cada instalación/despliegue que hagan de sus productos.
- Una buena gestión de las aplicaciones/credenciales incrementa la seguridad y disminuye el impacto ante los incidentes de seguridad que puedan suceder.

  Si una credencial se ve comprometida o se detecta un uso incorrecto de la misma, la Consejería puede proceder a bloquearla o eliminarla. Si esta credencial se emplea desde varios sistemas o despliegues, aunque sólo uno de ellos hubiera sido comprometido, el bloqueo de la credencial afectaría a todos.

  Esto debe tenerse en cuenta a la hora de solicitar y gestionar de forma adecuada las credenciales/aplicaciones.

Dentro de cada cuenta, no existe límite en el numero de aplicaciones, se pueden crear tantas aplicaciones como necesite.

Cuando una aplicación/sistema necesita consumir un API, un usuario (responsable aplicación, responsable entidad, administrador, desarrollador, etc) debe acceder al Developer Portal con una cuenta válida, crear una nueva aplicación o seleccionar una ya existente:

- Desde la interfaz de aplicación podrá solicitará la creación de credenciales para los entornos de pruebas y/o producción.

  La solicitud de credenciales en entornos de pruebas se procesa de forma automática, mientras que las de producción, requiere aprobación por parte de la consejería.

Una vez aprobada/rechazada la solicitud, se notificará por correo electrónico.

En caso de resolución positiva, las claves estarán disponibles a través de la interfaz de gestión de la aplicación.

- Desde la interfaz de aplicación o la interfaz del API, podrá solicitar la suscripción al API.

  La solicitud de suscripción requiere aprobación por parte de la Consejería por lo que una vez solicitada se mantendrá en espera hasta que sea aprobada.

  Una vez aprobada/rechazada la solicitud, se notificará por correo electrónico.

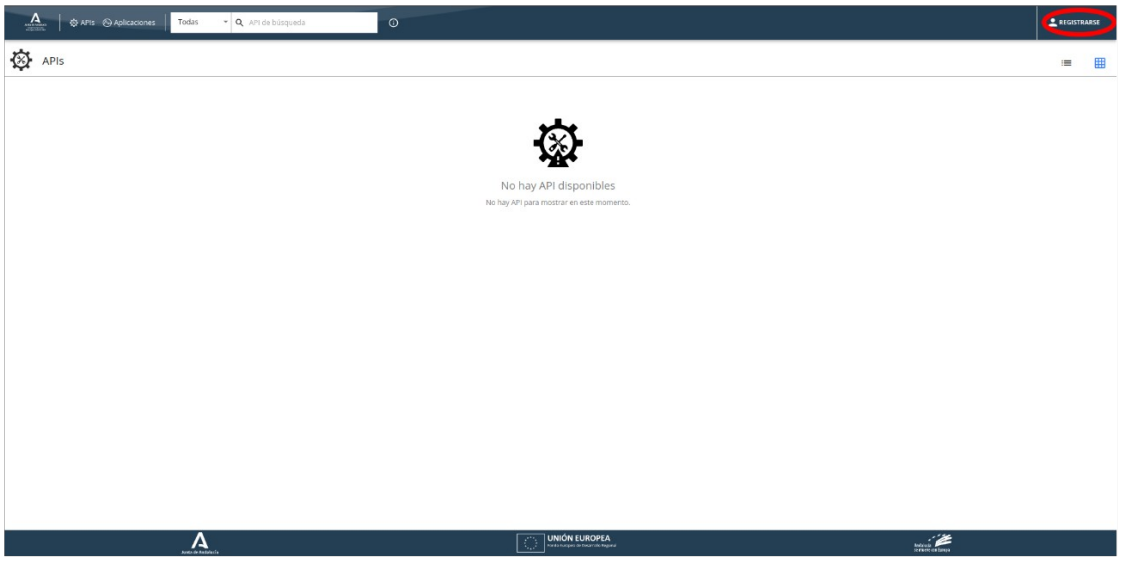
Los siguientes apartados describen en detalle el proceso; de suscripción, generación de claves y solicitud de los tokens de autorización, así cómo trabajar con ellos, a la hora de realizar las peticiones a las APIs.

2.2 Registro Nueva Cuenta en el Developer Portal.

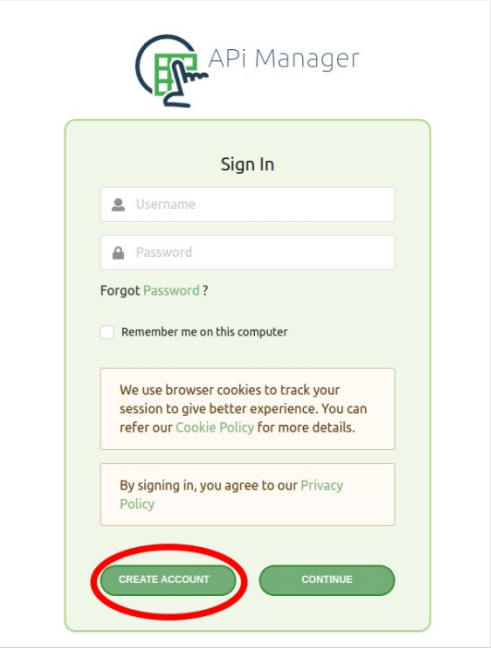
Para solicitar el alta de una nueva cuenta en Developer Portal realice los siguientes pasos:

Paso 1. Acceda a la aplicación Developer Portal y seleccione la opción REGISTRARSE

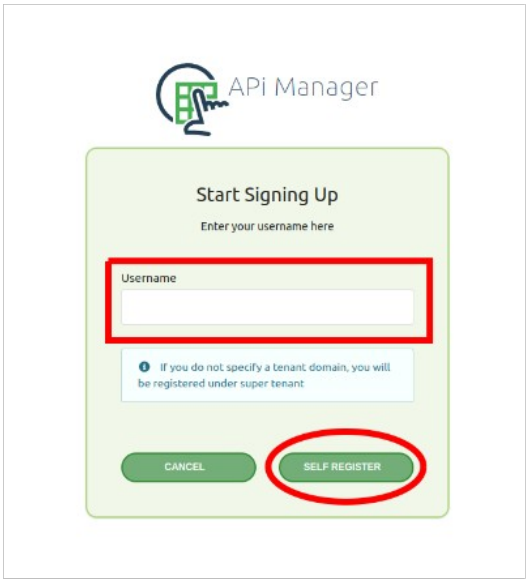
https://ws142.juntadeandalucia.es/agriculturaypesca/apimanager2/devportal/



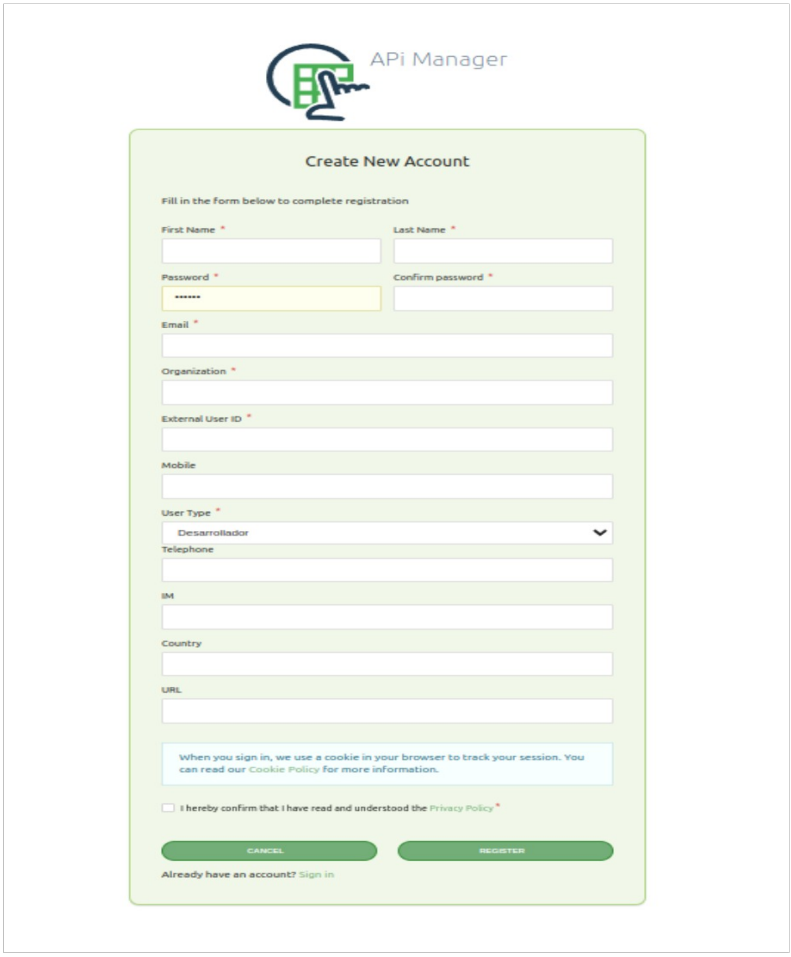
Paso 2. En la página de login, seleccione la opción CREATE ACCOUNT.



Paso 3. Introduzca un nombre de usuario para la cuenta que va a crear y pulse el botón SELF REGISTER



Paso 4. Rellene el formulario de alta de nuevo usuario.



Es importante que en el alta se proporcionen todos los datos solicitados con la mayor veracidad posible. Estos datos serán verificados por la consejería durante el proceso de alta.

En el campo "External User ID" introduzca su NIF/CIF.

Nota: ciertos APIs hacen uso de este campo para realizar proceso internos de autorización.

Si la cuenta va a ser empleada para administrar cuentas en entornos de producción, deberá indicar en el campo "User Type" la opción "Administrador Sistemas Producción", en caso contrario se deberá seleccionar la opción "Desarrollador".

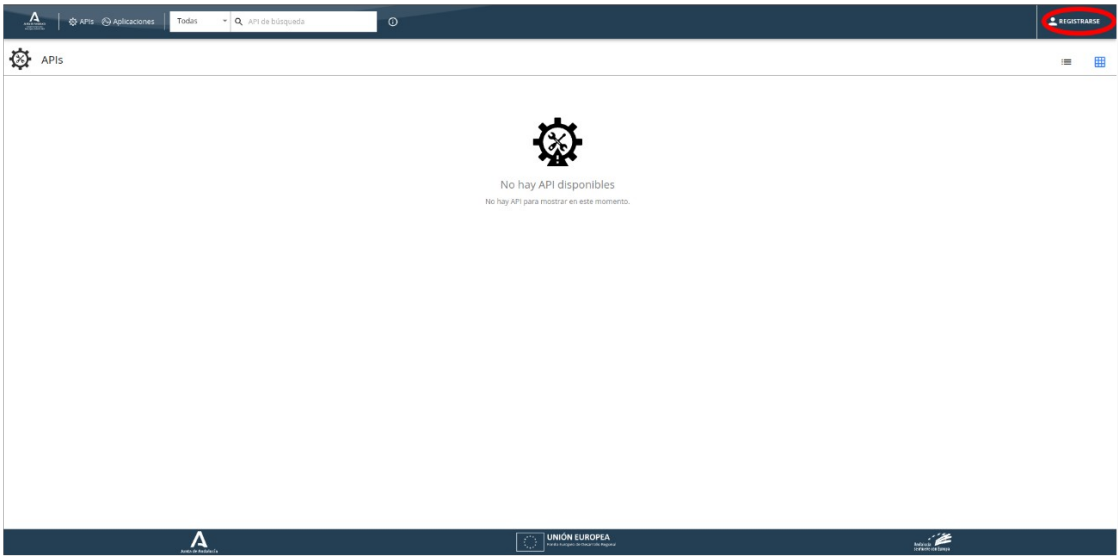
Nota: Si necesita solicitar credenciales de producción con esta cuenta, seleccione en el campo "User Type" la opción "Administrador Sistemas Producción".

Es importante proporcionar una dirección de correo válida, ya que las notificaciones de los procesos de aprobación se realizará usando esta dirección de correo.

Paso 5. Tras la petición de alta, se procederá a la validación de los datos presentados por parte de la Consejería.

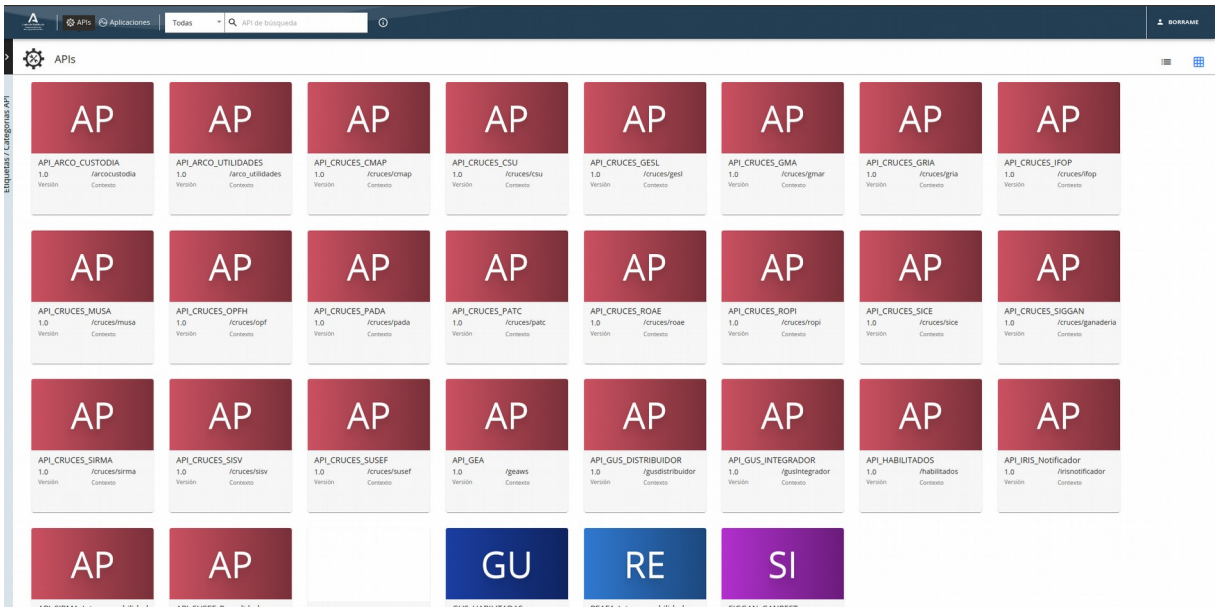
Mediante una notificación por correo, enviada a la dirección indicada en la solicitud, se informará si la creación de la nueva cuenta ha sido aprobada o rechazada.

Una vez validada la cuenta, ya podrá entrar en la aplicación Developer Portal seleccionando la opción REGISTRARSE.



Tras el logado, la aplicación mostrará el listado de APIs disponibles, en función de los permisos asignados a su cuenta.

Una cuenta recién creada sólo tendrá disponible las APIs con visibilidad pública.

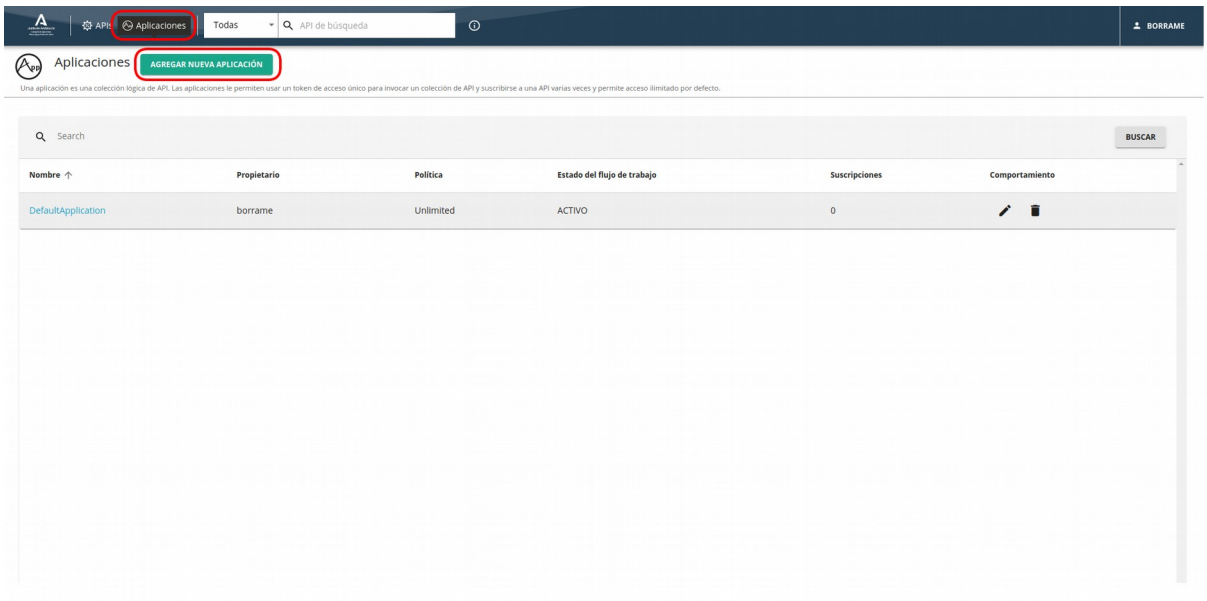


Si no localiza el APIs que quiere utilizar, posiblemente carezca de los permisos necesarios para visualizar y/o utilizar dicho API. En este caso deberá ponerse en contacto con la Consejería, empleando el Centro de Soporte TIC o cualquiera de los mecanismos establecidos para tal efecto, y solicitar permisos para la visualización y uso de las APIs que necesite.

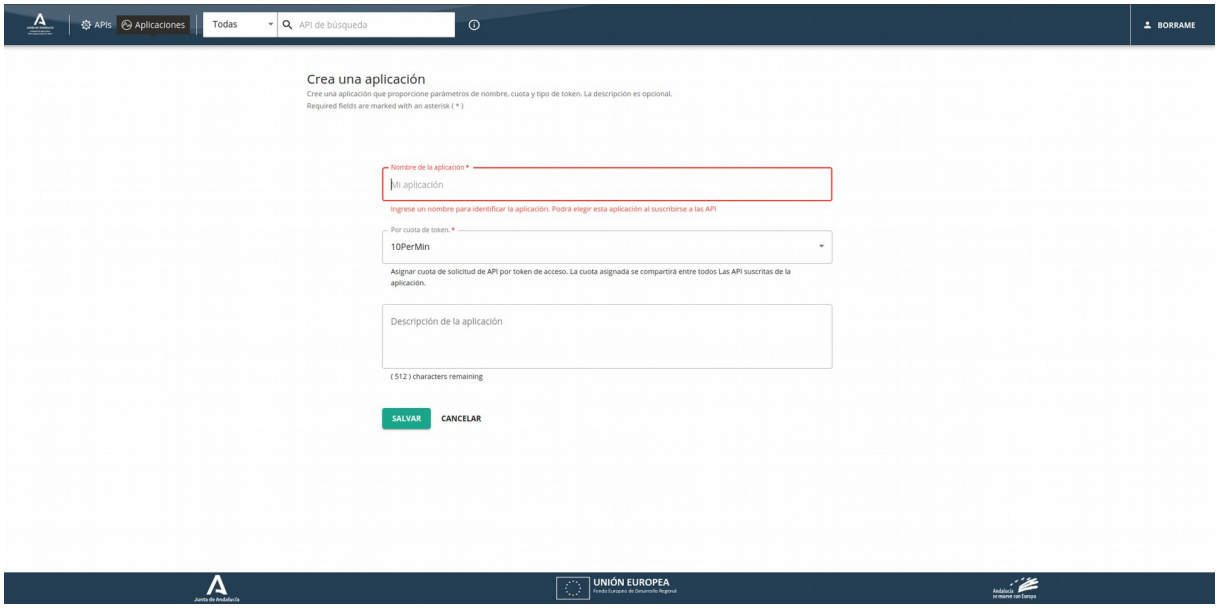
2.3 Alta de Aplicaciones

Para dar de alta una aplicación, acceda al Developer Portal y lóguese con una cuenta válida.

Seleccione la opción “Aplicaciones” y cree una nueva aplicación pulsando en el botón “AGREGAR NUEVA APLICACIÓN”.



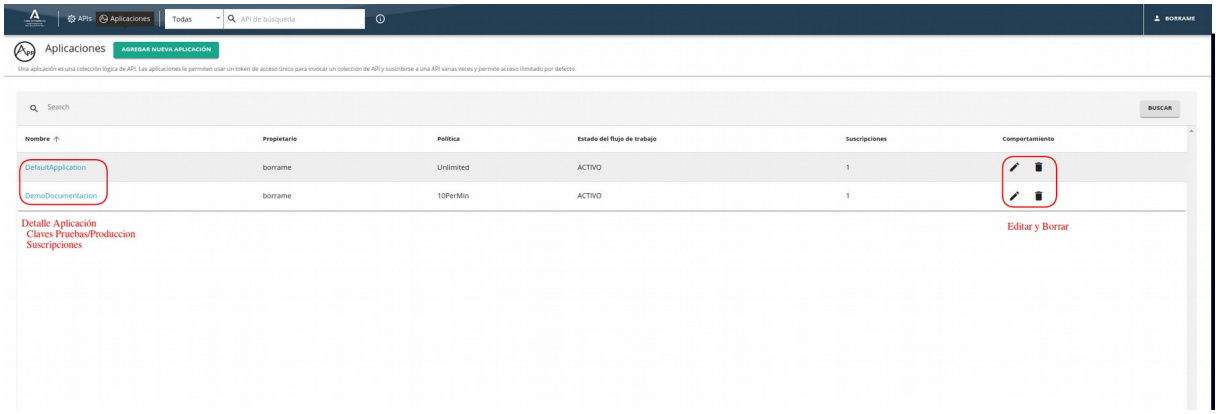
A continuación introduzca los datos solicitados y pulse salvar.



Desde la página de listado de aplicaciones, podrá acceder a las aplicaciones y gestionar sus claves, solicitar suscripciones, etc.

También, a través del listado de aplicaciones, podrá realizar operaciones básicas de edición o borrado de aplicaciones.

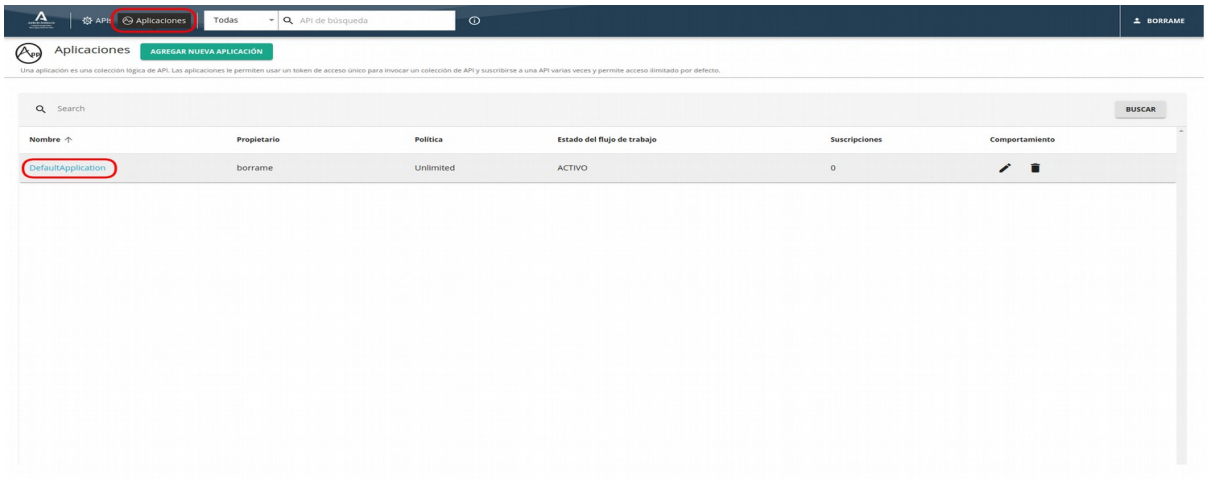
Nota: cuando se elimina una aplicación se eliminan todas las credenciales y suscripciones asociadas. Las aplicaciones que estén haciendo uso de estas credenciales recibirán un error indicando que sus credenciales no son válidas.


APIs
Aplicaciones
Todas
API de búsqueda
BORRAME
Aplicaciones
AGREGAR NUEVA APLICACIÓN
Una aplicación es una colección lógica de API. Las aplicaciones le permiten usar un token de acceso único para invocar un colección de API y suscribirse a una API varias veces y permite acceso ilimitado por defecto.
Search
BUSCAR
Nombre
Propietario
Política
Estado del flujo de trabajo
Suscripciones
Comportamiento
DefaultApplication
borrame
Unlimited
ACTIVO
1
DemoDocumentacion
borrame
10PerMin
ACTIVO
1
Detalle Aplicación
Claves Pruebas/Produccion
Suscripciones
Editar y Borrar

2.4 Generación Credenciales/Keys.

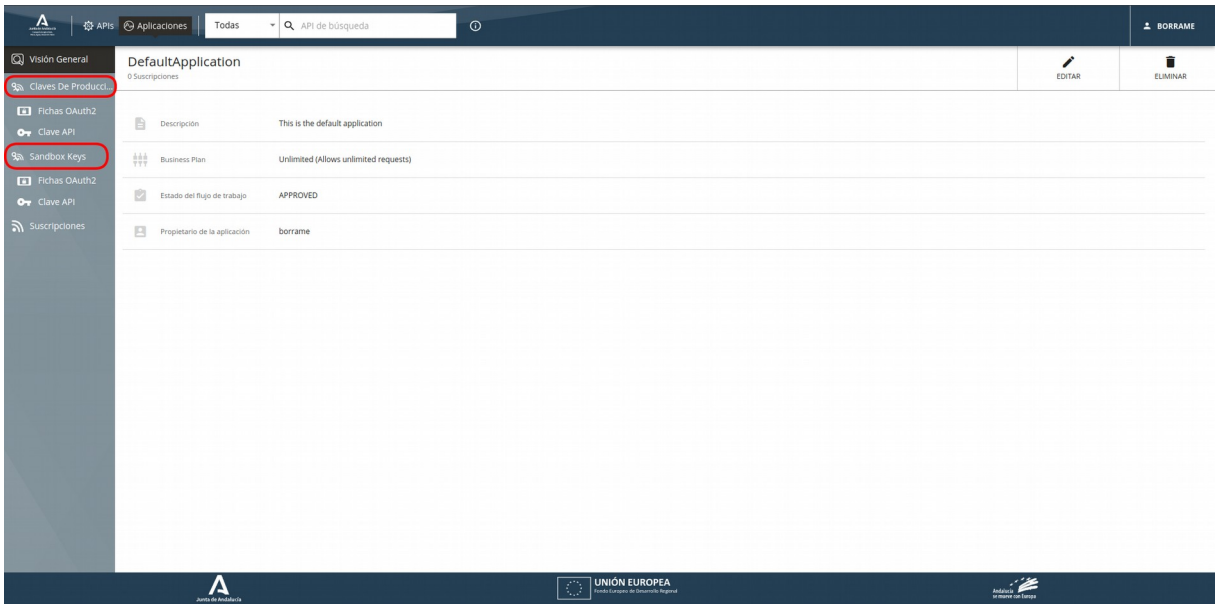
Para generar las credenciales (keys) empleadas en las peticiones de tokens, acceda al Developer Portal y lóguese con una cuenta válida.

Acceda a sus Aplicaciones y seleccione la aplicación donde desea crear las credenciales o cree una nueva siguiendo el apartado 2.3 Alta de Aplicaciones.



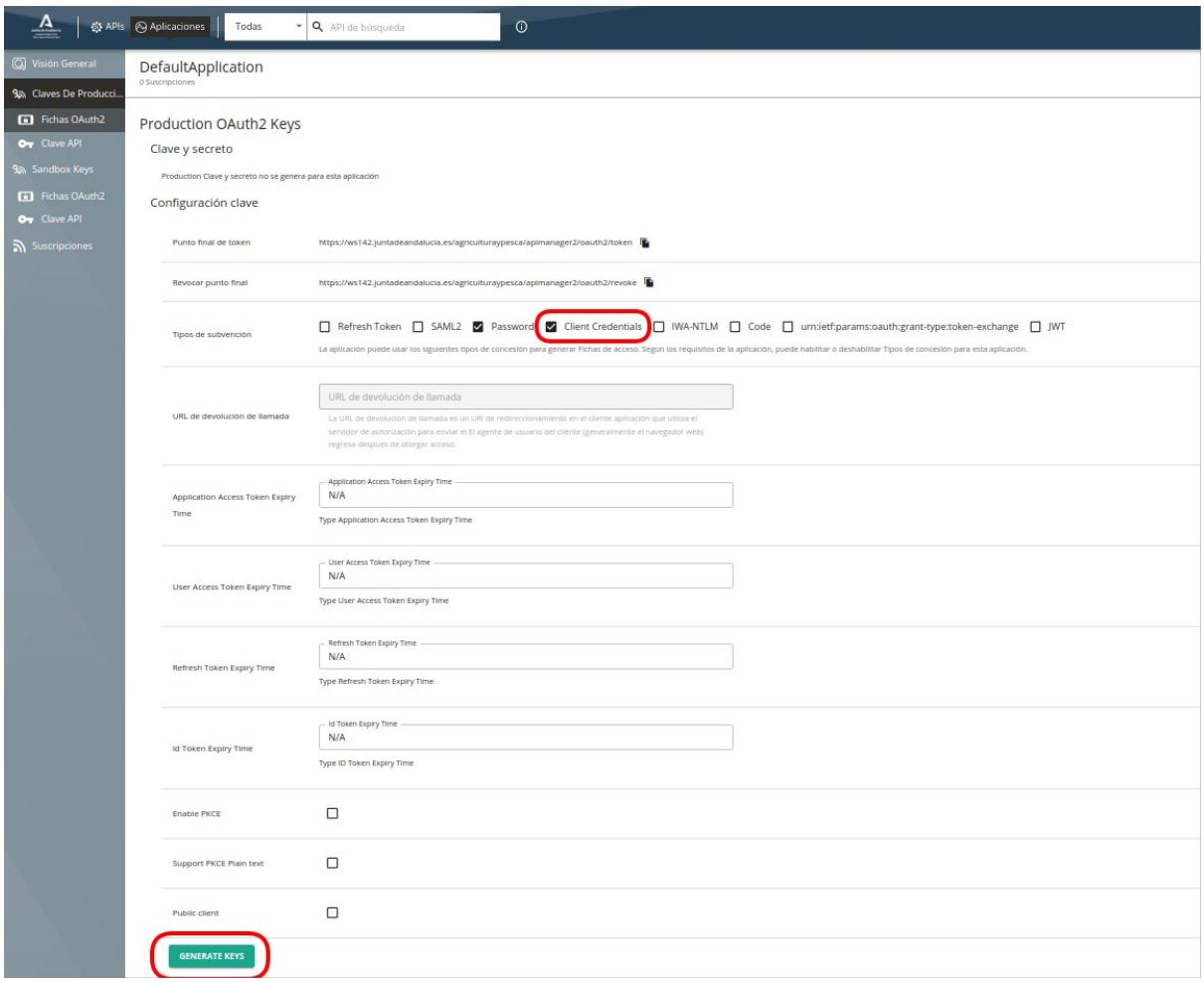
Seleccione el tipo de Credencial a generar: Producción y/o Pruebas (SandBox), en el menú de la izquierda.

Nota: Todos los APIs publicados requieren autenticación con claves OAuth2, no hay ningún API publicado que requiera Clave Api (Api Key).



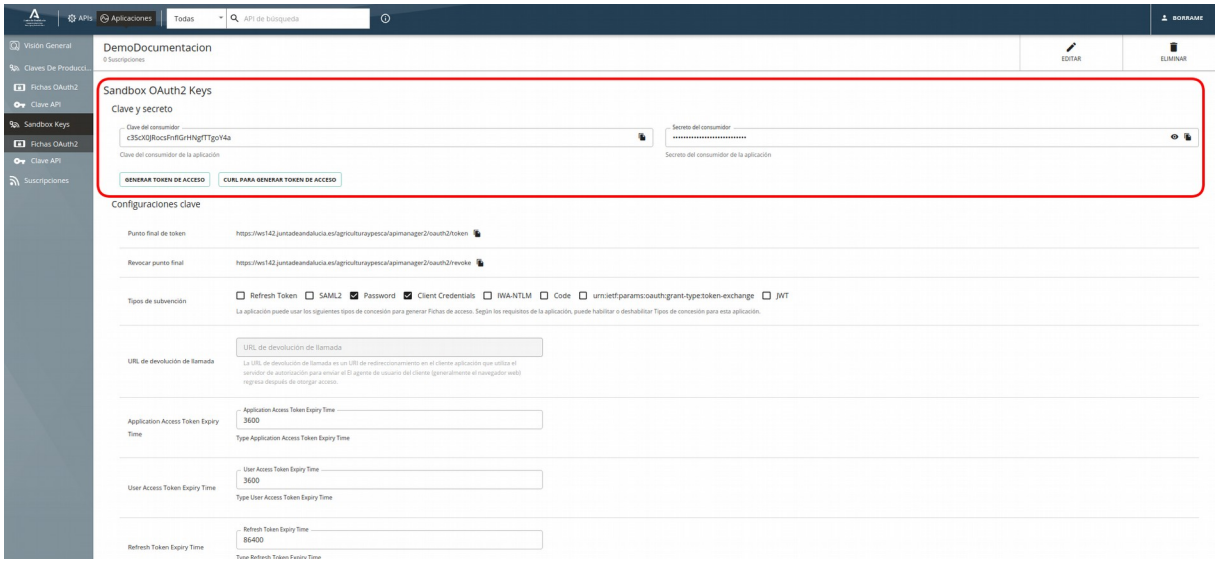
En el formulario de creación de clave seleccione unicamente “Client Crentials“ como mecanismo de autenticación y pulse Generar Keys.

Nota: Los otros mecanismo no están soportados en la actualidad.



Si se ha solicitado claves de producción, aparecerá un mensaje indicando que están pendientes de aprobación. Cuando estás sean aprobadas o rechazadas por la Consejería, se enviará un correo a la dirección registrada en su cuenta.

Una vez aprobada la creación de claves de Producción o generadas la clave de Pruebas, podrá acceder a las mismas desde la página de detalle de la aplicación, seleccionando el tipo de credencial que desee consultar.



El formulario de Aplicación mostrará ahora en la parte superior la credencial generada.

La credencial o key está formada por dos elementos; el "Client Id" o "Clave de consumidor" que correspondería con el identificado de la cuenta/clave y el "Secreto del consumidor" o client key que corresponde con la clave o password.

La pantalla también incluye un nuevo botón para generar los tokens de acceso desde el propio Developer Portal. Este botón es sólo para pruebas, en el apartado "3 Invocación de un API" se detalla la forma correcta de generar los tokens y su uso desde las aplicaciones.

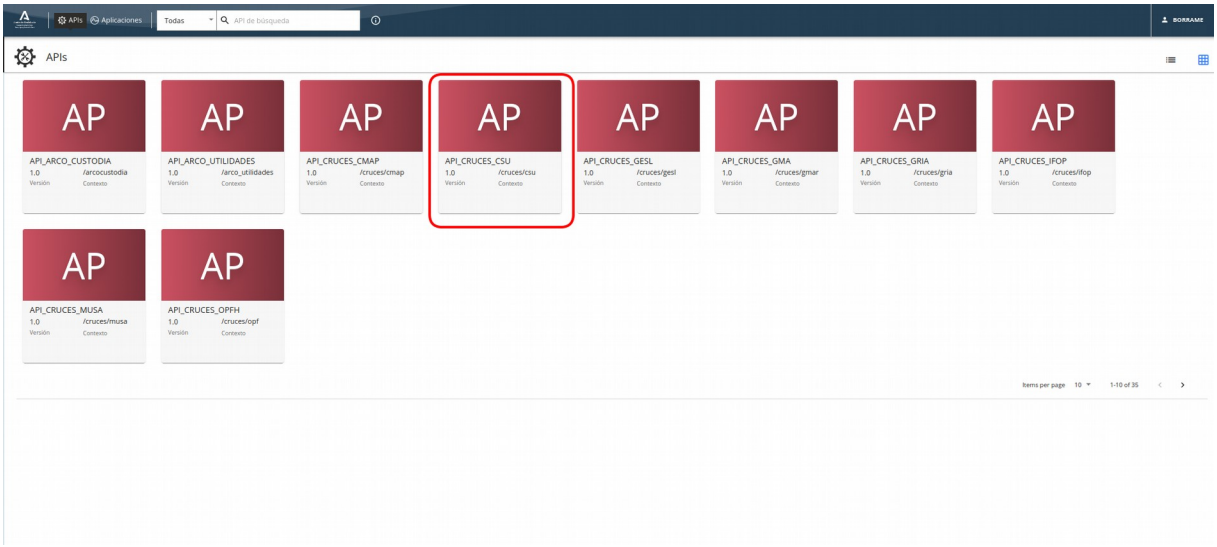
2.5 Suscripción a un API

Para realizar la suscripción a un API acceda al Developer Portal y lóguese con una cuenta válida.

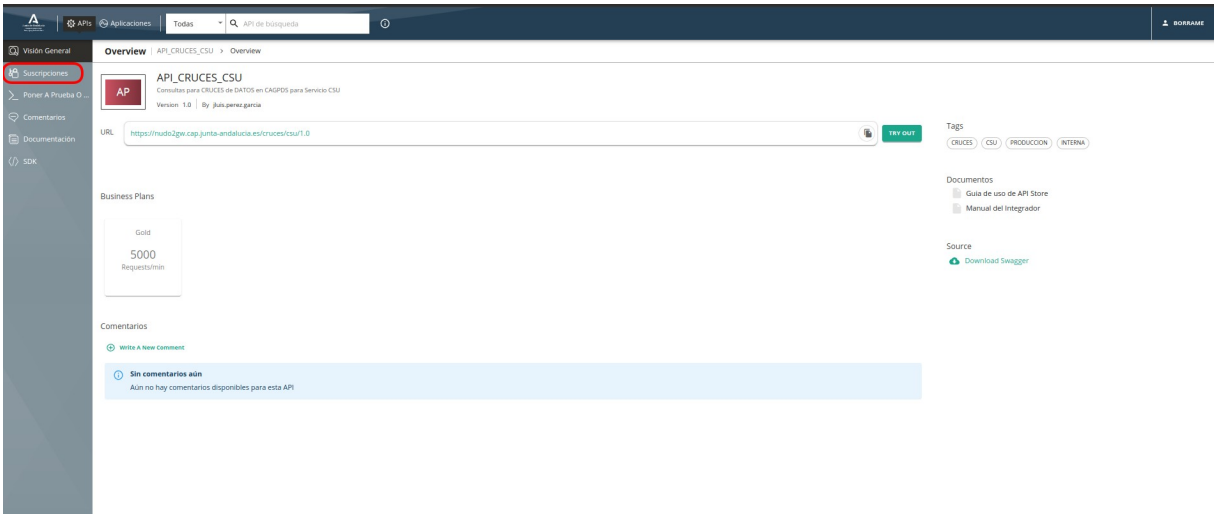
La suscripción puede realizarse de dos forma; desde la página de detalle del API al que se desea suscribirse o desde la página de detalle de la aplicación donde se va a realizar la suscripción.

2.5.1 Suscripción desde API

Desde la pantalla de listado de API seleccione el API al cual desea suscribirse.

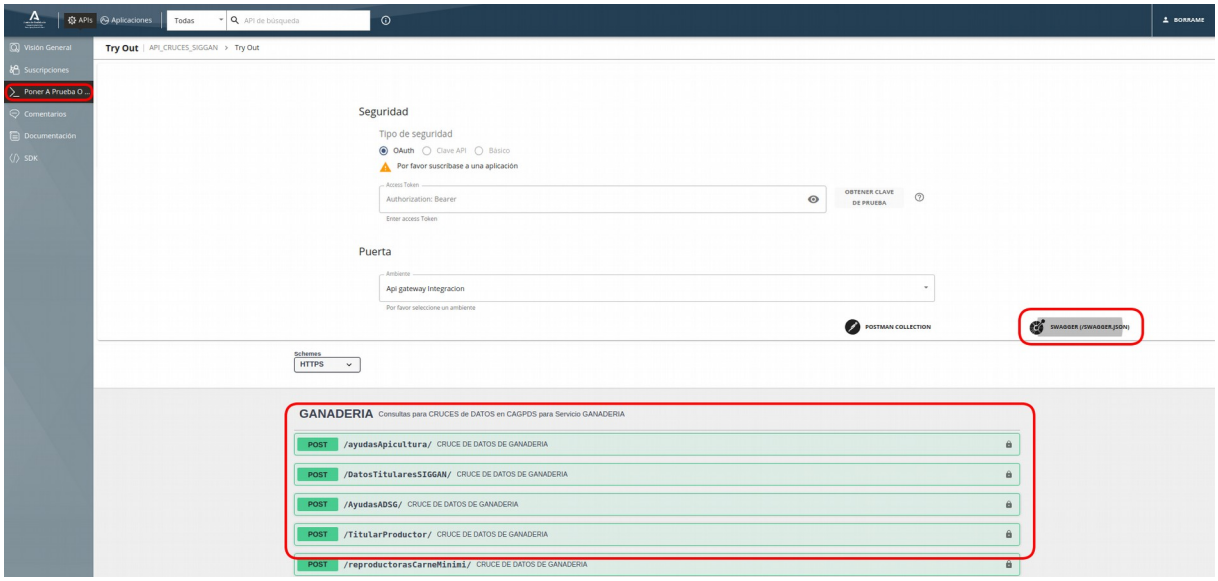


Se mostrará la pantalla de detalle del API seleccionado.

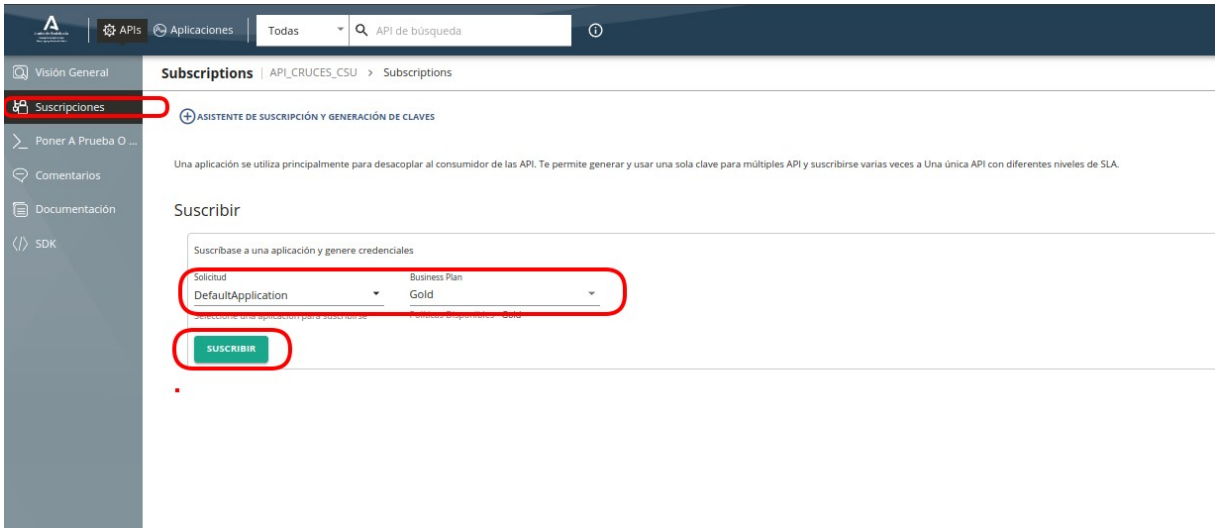


En esta interfaz se presenta la información básica del API: Url del servicio en los distintos entornos donde está publicada (GWs), documentación/ficheros asociados, etc.

Dese la opción "Poner a prueba" del menú lateral, podrá acceder al detalle del API, ver los métodos y operaciones, descargar el swagger del API, etc.



Para solicitar la suscripción, seleccione la opción Suscripciones del menú lateral.



Seleccione la aplicación con la que realizará la suscripción y pulse el botón "Suscribir".

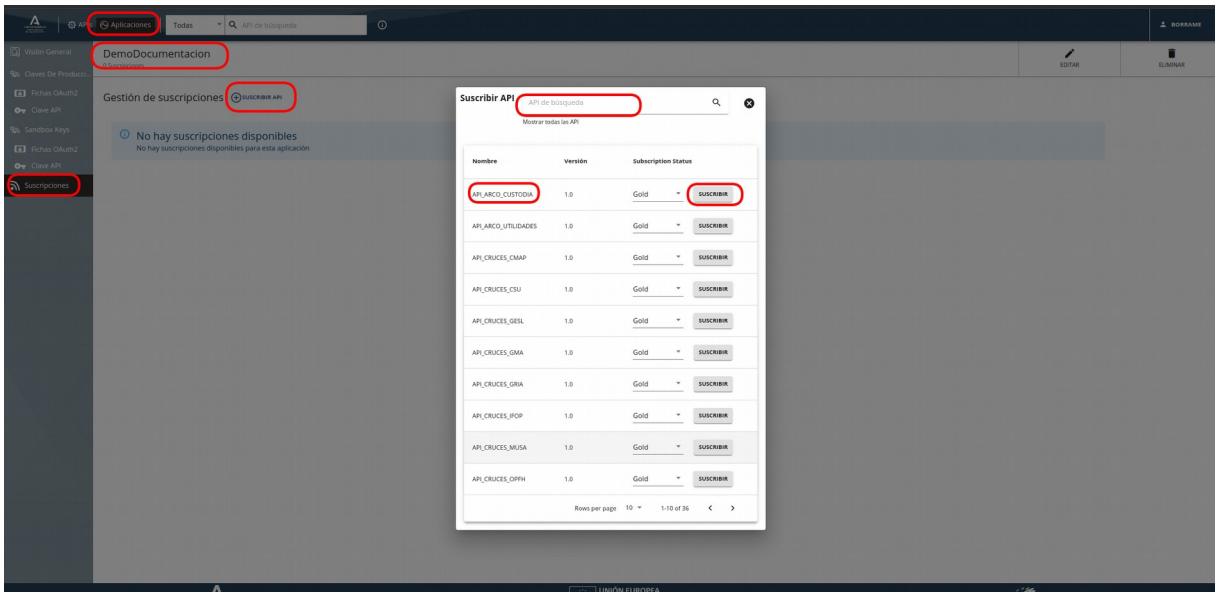
La suscripción deberá ser aprobada por la consejería, cuando esto se realice recibirán un correo notificándole el resultado de la misma.

Una vez aprobada la suscripción, el API podrá llamarse empleando cualquier token de autorización (pruebas o producción) expedido para la aplicación con la cual ha sido subscrito.

2.5.2 Suscripción desde Aplicación

Desde la pantalla de listado de Aplicaciones seleccione la aplicación desde la cual desea suscribirse.

En el menú lateral, seleccione la opción Suscripciones y pulse sobre "+ SUSCRIBIR API".



Aparecerá un formulario con el cual puede localizar el API y solicitar la suscripción.

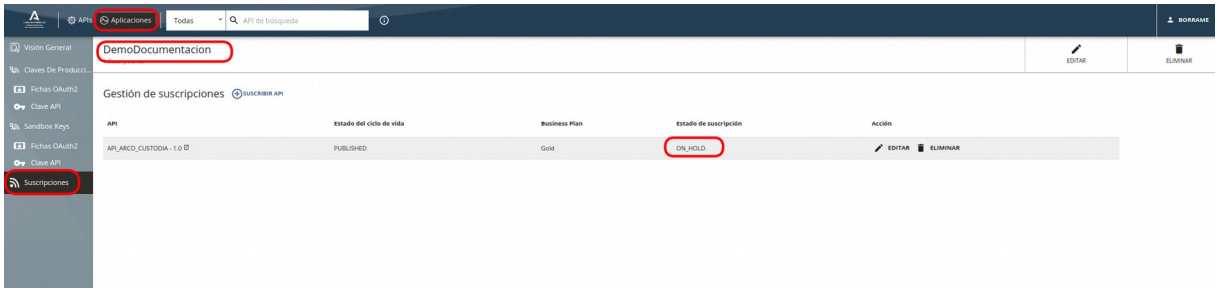
La suscripción deberá ser aprobada por la consejería. Cuando esto se realice recibirán un correo notificándole el resultado de la misma.

Una vez aprobada la suscripción, el API podrá llamarse empleando cualquier token de autorización (pruebas o producción) expedido para la aplicación con la cual ha sido subscrito.

2.5.3 Listado de Suscripciones de una Aplicación

Para ver el estado de sus suscripciones, acceda a la aplicación correspondiente y selecciona la opción Suscripciones del menú lateral.

La pantalla mostrará el listado de suscripciones y su estado.



A través de esta pantalla podrá eliminar una suscripción o petición de suscripción que tenga pendiente.

3 Invocación de un API.

Introducción

Todos los APIs publicados dentro de la plataforma están securizados mediante protocolo OAuth2.

Los Gateways cumplen los roles de Servidor de autorización y Servidor de Recursos. Es decir, son los responsables de la generación y validación de los tokens, además de la publicación y control de los permisos de acceso a las APIs.

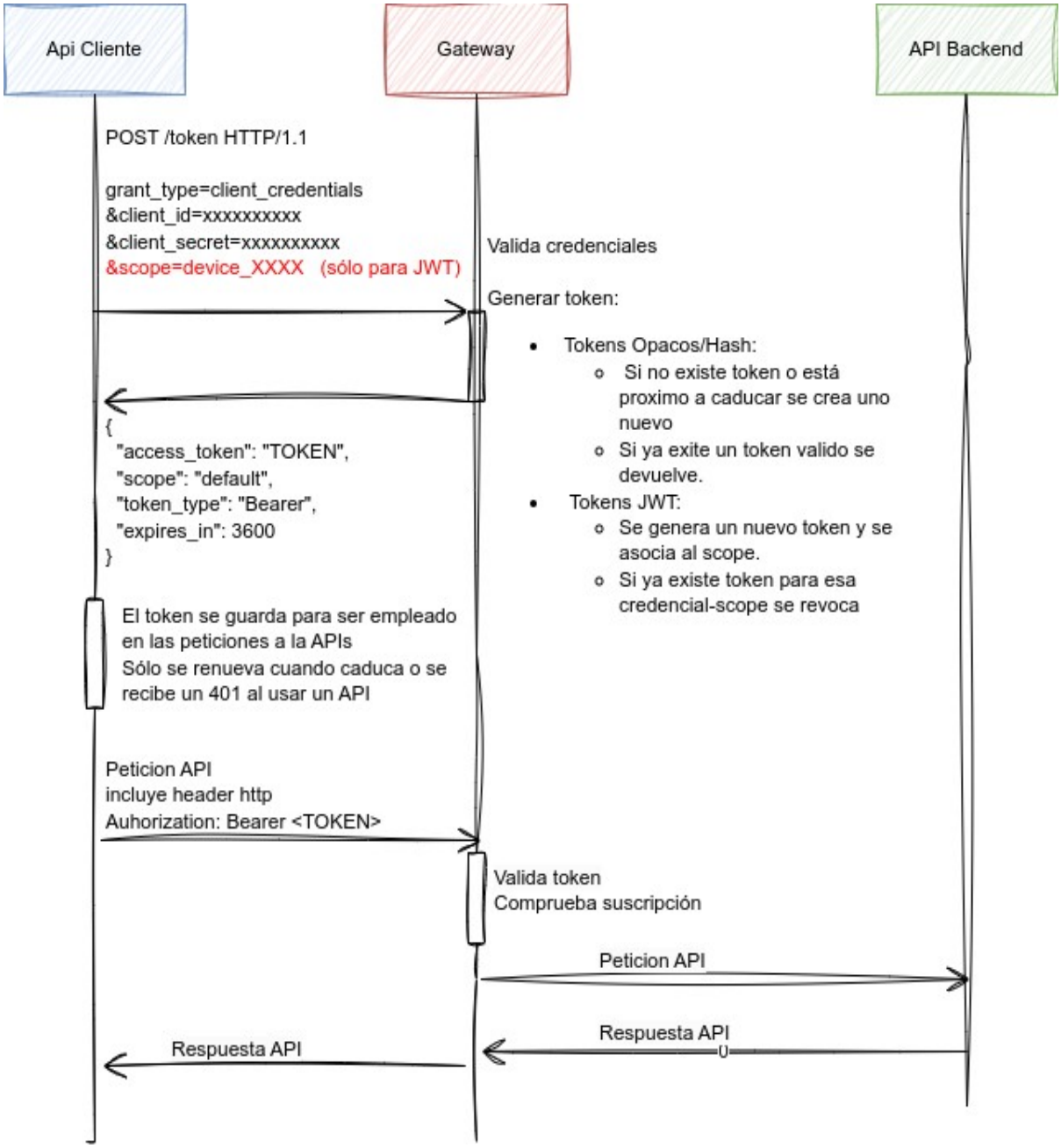
Los Gateways pueden generar los tokens en dos formatos; Opacos(hash) y JWT. Para las aplicaciones y cuentas importadas desde la versión anterior de APIM, los tokens se siguen generando en formato Opaco, mientras que para las nuevas altas, se generan en formato JWT.

Este dato es importante, ya que el APIM introduce cambios en la forma en la que genera/revoca los tokens cuando están en un formato u otro:

- Para los tokens en formato Opaco, el sistema devuelve el mismo token ante sucesivas peticiones realizadas con una misma credencial.
- Para los tokens en formato JWT, cuando se realizan varias peticiones de tokens con una misma credencial, el sistema revoca (invalida) el token anterior y genera un nuevo token. Esto, en entornos con clientes en cluster/multihilos o aplicaciones que comparten la misma credencial, dará lugar a errores por revocación de tokens al hacer uso de estos tokens,

  Los sistemas afectados por este comportamiento tendrán que:

  - Compartir los tokens entre las instancias/hilos, por ejemplo, guardándolos en BD.
  - O emplear scopes en las peticiones de token, de forma que cada instancia, emplee un scope (device_XXX) distinto del resto. En este caso, el sistema lo que hace es asociar el token a la credencial-scope, aislando la generación/revocación de tokens entre scopes.



En OAuth 2.0, las peticiones de acceso son iniciadas por el cliente; aplicación móvil, sitio web, aplicación de escritorio, etc.

Las peticiones, el intercambio y la respuesta de los tokens siguen el flujo mostrado en la imagen anterior:

- El cliente solicita autorización al servidor de autorización (GW), para ello emplea procotolo OAuth2 con grant type "Client credetials" y proporciona el client id y el client secret como identificación.

  En caso de tokens JWT, podrá incluir un scope en la petición con el formato device_NOMBRE-SCOPE, por ejemplo: device_nodo1, device_host1, etc.

  Notas:

  - En el apartado "2.4 Generación Credenciales/Keys" se detalla cómo generar y consultar los client id y client secret.
  - En JWT, si no se define scope el sistema asocia la petición al scope "default"

- Los scopes definidos como device_XXX no necesitan darse de alta en el APIM

- El servidor de autorización (GW):
  - Autentica al cliente y verifica que los ámbitos solicitados están permitidos.
  - Genera el token. La generación del token varía en función del formato del token a devolver:
    - Tokens Opacos:
      - Si no existe token asociado a la credencial o está próximo a caducar, se crea uno nuevo.
      - Si ya existe un token válido se devuelve.
    - Tokens JWT:
      - Se genera un nuevo token y se asocia a la credencial-scope.
      - Si ya existía token para esa credencial-scope, se revoca.
  - Devuelve el token indicando el tiempo que queda hasta su caducidad.

    Nota: Los tokens tienen un tiempo de caducidad de 3600s (1h)

- El cliente, una vez obtenido el token, deberá almacenarlo temporalmente para evitar tener que pedir un token cada vez que realice una llamada a un API y el token aún esté vigente.

  Sólo deberá pedir un nuevo token cuando este caduque o esté próximo a caducar. También deberá pedir un nuevo token cuando el GW devuelva errores al validar el token. Normalmente esto se comunica mediante una respuesta 401 y puede ser debido a que el token ha caducado o haya sido revocado.

- Al realizar peticiones a los APIs, el cliente incluirá en las peticiones una cabecera http con el token de acceso.

  La cabecera tiene el siguiente formato:

  Authorization: Bearer <token>

- El GW recibe la petición, valida el token, comprueba que el token corresponde a una aplicación con una suscripción al API, procede a llamar al backend y devuelve la respuesta generada por este.

Petición Token

Las peticiones de tokens se realizan siguiendo el protocolo OAuth2.

Son peticiones HTTP de tipo POST que se lanzan sobre el servicio de petición de tokens publicados en los distintos GWs.

https://[GW_URL]/oauth2/token

La petición incluye un parámetro “grant_type” donde se indica el mecanismo empleado para la autenticación de la petición: “client_credentials” en nuestro caso.

También se incluirá las credenciales de la aplicación, mediante alguno de los mecanismos soportados:

- Empleando cabecera HTTP “Authorization” de tipo “Basic”. Las credenciales se codifican en Base64 siguiendo el formato:

  Authorization: Basic Base64(consumer-key:consumer-secret)

  Ejemplo de petición usando curl y la respuesta obtenida:

```
curl -k -d "grant_type=client_credentials&scope=device_NOMBRE-SCOPE"  -H "Authorization: Basic
Wjk0ZMRwQUp0ZHNzZza9SQ3JtMk10RGFapqSkJamlFNaZNTUwzZlpqMThka1g5T3Nh"
https://ws142.juntadeandalucia.es/agriculturaypesca/am2gwint/oauth2/token

{"access_token":"TOKEN en formato hash o JWT","scope":"am_application_scope default","token_type":"Bearer","expires_in":731}
```

- Otra opción, es incluir las credenciales como parámetros (client_id y client_secret) dentro de la petición.

  Ejemplo de este tipo de petición usando curl y la respuesta obtenida:

```
curl -k -d
"grant_type=client_credentials&client_id=3f6AZxMyZqKKbwWUSD2gzqocoa&client_secret=nvaSEE_PTjGVUaa9NXPvoa&scope=device_nodo1"
https://ws142.juntadeandalucia.es/agriculturaypesca/am2gwint/oauth2/token

{"access_token":"TOKEN en formato hash o JWT","scope":"am_application_scope default","token_type":"Bearer","expires_in":1364}
```

Nota: el scope sólo en necesario en peticiones de tokens JWT que implementen la solución de scopes para evitar problemas de revocación de tokens en entornos clusterizados y/o multihilos.

Si la petición se realiza correctamente, el servicio de token responderán con un json, que incluye el token de acceso y su tiempo de expiración.

```
{"access_token":"TOKEN en formato hash o JWT","scope":"am_application_scope
default","token_type":"Bearer","expires_in":1364}
```

La petición de tokens deberá realizarse sobre el GW donde se estén publicando las APIs que se quiere consumir.

A continuación se incluyen las direcciones de petición de tokens para cada entorno disponible:

- GW Externo producción:

  https://ws142.juntadeandalucia.es/agriculturaypesca/am2gwpro/oauth2/token
- GW Externo integración:

  https://ws142.juntadeandalucia.es/agriculturaypesca/am2gwint/oauth2/token
- GW Interno producción:

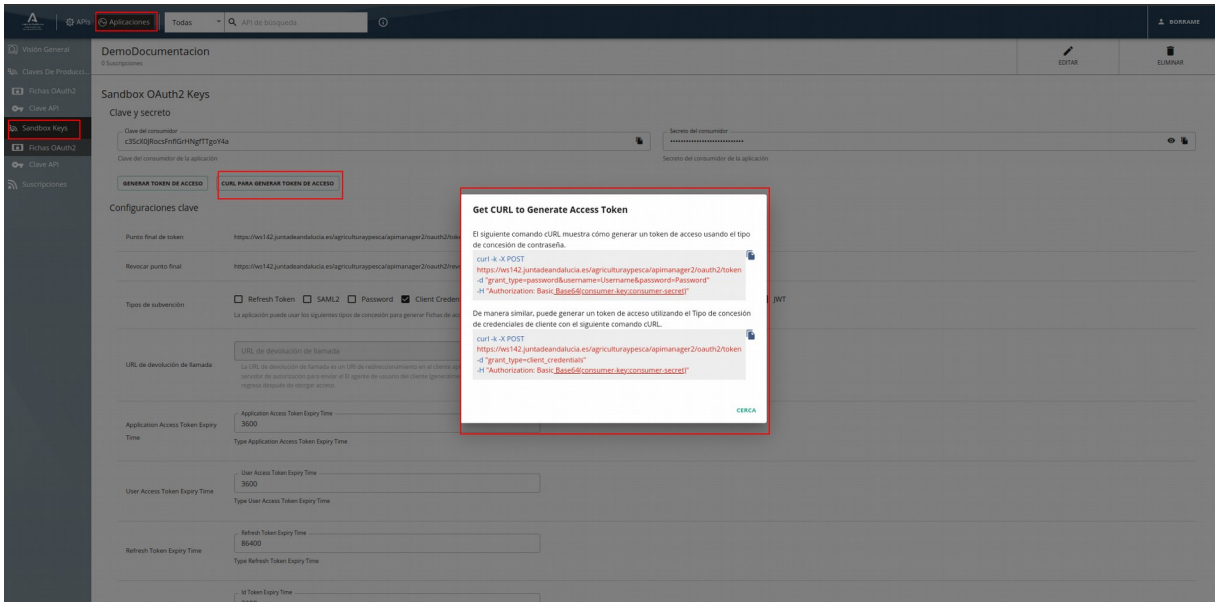
  https://nudo2gw.cap.junta-andalucia.es/oauth2/token
- GW Interno integración:

  https://nudo2gw.integracion.cap.junta-andalucia.es/oauth2/token
- GW Interno certificación:

  https://nudo2gw.certificacion.cap.junta-andalucia.es/oauth2/token

Dentro del Developer Portal, en la pantalla de gestión de las keys de una Aplicaciones, se incluye una opción para generar tokens y ejemplos con CURL de cómo realizar las peticiones de tokens.

Por ejemplo, la siguiente imagen muestra la página de gestión para las claves de pruebas (Sandbox) de una aplicación.



La pantalla muestra la Key generada, campos; “Clave del consumidor” y “Secreto del consumidor”.

Nota: si la pestaña no muestra los campos de Keys, pulse sobre el botón de generar claves.

El botón “GENERAR TOKEN DE ACCESO” lanza un formulario que genera un token de acceso que se puede emplear para realizar pruebas a los APIs empleando herramientas como: curl, postman, swagger-ui, etc.

El botón “CURL PARA GENERAR TOKEN DE ACCESO” incluye dos ejemplos de petición de tokens con curl, el primero usando grant_type=password y el segundo usando grant_type=client_credential.

No se recomiendo emplear el primer método, las peticiones de token siempre se deben realizar usando grant_type=client_credential.

Uso del Token de Autorización

Una vez obtenido un token de autorización, este puede ser empleado para realizar peticiones a los APIs. Sólo necesita incluir en token en una cabecera HTTP Authorization con el siguiente formato:

Authorization: Bearer <Token>

A continuación, se incluye un ejemplo con curl de cómo realizar una llamada a un API, a través del GW externo de Integración, empleando un token de acceso.

curl -k -X GET "https://ws142.juntadeandalucia.es/agriculturaypesca/am2gwint/demo/3.0/demorecurso" -H "accept: application/json" **-H "Authorization: Bearer 5433182-ff2c-3f06-956c-dbb8ae30e0f3"**

Nota 1: Los Tokens de Autorización tienen un tiempo de caducidad de 3600s (1h). Cuando se emplea un token caducado el servicio responderá con un error 401. En este caso, se deberá pedir un nuevo token y reintentar la petición.

Nota 2: Se recomienda emplear algún framework/API que implemente un cliente oauth2 y que permita automatizar todo el proceso de petición, renovación de tokens e inyección de este en las peticiones.

4 GLOSARIO

Término	Descripción
CAPDR	Consejería de Agricultura, Pesca, Agua y Desarrollo Rural
GWs	Gateways