Credenciales de acceso al API

Todas las llamadas al API se autentican con un par de credenciales: el **API Token** y el **Access Token**. Ambos se generan desde el perfil de la cuenta y se envían en cada petición como encabezados HTTP.

Requisito previo

> La generación y el uso de credenciales requieren un **plan con acceso a API activo**. Si el plan de la cuenta no lo incluye, la pestaña «API» no aparece en el perfil y las llamadas responden `403` con el mensaje `No posee un Plan Api activo`.

Generar las credenciales

1. Inicie sesión en app.facturadorvirtual.com.
2. Vaya a **Perfil** y abra la pestaña **API**, en `/perfil/api/detalles`.
3. La primera vez verá el aviso «Generación de credenciales». Pulse **Generar accesos**.
4. La pantalla muestra los dos valores en los campos **API Token** y **Access Token**. Cópielos y guárdelos en un lugar seguro.

Si la cuenta ya tiene credenciales, la misma pantalla las muestra junto a un botón **Regenerar accesos**.

Credencial	Encabezado	Formato
API Token	`api-token`	48 caracteres alfanuméricos
Access Token	`access-token`	52 caracteres alfanuméricos

Usar las credenciales

Las dos credenciales viajan como encabezados en cada petición. Junto con ellas debe enviarse siempre `Accept: application/json`.

```
--header 'api-token: iuJPbVCYQY3AmWuVHMflT9ZySlwzxb9ehviLbHNsz6yQnBm4' \
--header 'access-token: IDq4ME4ZUO9YmQ0fOc43AFp7mMO6talIuIALFaUUcs2H2pwLpYN2' \
--header 'Content-Type: application/json' \
```

```
--header 'Accept: application/json'
```

> El encabezado `Accept: application/json` no es opcional. Sin él, una petición cuyas credenciales sean inválidas responde con una redirección al formulario de inicio de sesión en lugar de un error JSON, lo que suele confundirse con un problema de red.

Comprobar que funcionan

La forma más simple de validar un par de credenciales es consultar el tipo de cambio de referencia. Es una llamada de solo lectura que **no consume documentos** del plan.

```
curl --location 'https://app.facturadorvirtual.com/api/2.0/indicadores-economicos/tipo-cambio'
\
--header 'api-token: iuJPbVCYQY3AmWuVHMflT9ZySlwzxb9ehviLbHNsz6yQnBm4' \
--header 'access-token: IDq4ME4ZUO9YmQ0fOc43AFp7mMO6talIuIALFaUUcs2H2pwLpYN2' \
--header 'Accept: application/json'
```

Con credenciales válidas y un plan API activo, la respuesta es:

```
{
  "USD": {
    "compra": 512.45
  }
}
```

Regenerar las credenciales

> Regenerar **elimina de inmediato el par anterior**. Cada cuenta tiene un único juego de credenciales vigente, de modo que toda integración que siga usando los valores antiguos empezará a recibir `401` en la siguiente llamada. Planifique la sustitución antes de pulsar el botón.

Regenere las credenciales cuando:

- Sospeche que fueron expuestas o compartidas por error.
- Cambie el plan de la cuenta. Las credenciales quedan asociadas al plan vigente **en el momento en que se generaron**; tras un cambio de plan conviene regenerarlas para que apunten al plan actual.

- Rote credenciales como parte de su política de seguridad.

Vigencia

Las credenciales **no tienen fecha de expiración**: permanecen válidas hasta que se regeneren. Tampoco es posible mantener varios pares simultáneos por cuenta, por lo que no existe un mecanismo de rotación solapada: la sustitución es instantánea.

Errores relacionados con las credenciales

HTTP	Cuerpo	Causa
302	Redirección al inicio de sesión	Falta el encabezado `Accept: application/json`.
401	`{"message": "Unauthenticated."}`	El `api-token` no existe, o el `access-token` no corresponde a ese `api-token`. Ocurre también cuando se siguen usando credenciales ya regeneradas.
403	`{"error": "No posee un Plan Api activo"}`	Las credenciales son válidas, pero el plan asociado no incluye acceso a API.
403	`{"error": "Ha llegado al límite de facturas del Plan Api contratado"}`	Las credenciales son válidas, pero se agotaron los documentos del ciclo vigente.

Los dos errores `403` confirman que la autenticación fue correcta: el problema está en el plan, no en las credenciales.

Recomendaciones de seguridad

- Trate ambos valores como contraseñas: quien los posea puede emitir comprobantes electrónicos a nombre de su empresa.
- Guárdelos en variables de entorno o en un gestor de secretos, nunca en el código fuente ni en repositorios.
- No los incluya en capturas de pantalla, tiquetes de soporte ni registros de aplicación.
- Úselos solo desde su servidor. No los incruste en aplicaciones móviles ni en código JavaScript que se ejecute en el navegador, donde quedarían a la vista de cualquiera.
- Si sospecha una filtración, regenérelos de inmediato.

Revision #1
Created 31 August 2026 19:27:18 by Manfred

Updated 31 August 2026 19:27:18 by Manfred