Errores 401 al consumir la API

Diagnóstico de los distintos 401: token inválido, cabecera mal formada, credenciales del SII y sesión caída.

Anonymous · 06/11/2026

Errores 401 al consumir la API

El `401` agrupa seis problemas distintos. El mensaje del campo `detail` te dice cuál es.

“Las credenciales de autenticación no se proveyeron”

Falta la palabra `Token` en la cabecera. La API **no acepta** `Bearer`, ni `X-Api-Key`, ni el token en la URL:

```
Authorization: Token 0123456789abcdef0123456789abcdef01234567   ← correcto
Authorization: Bearer 0123456789abcdef0123456789abcdef01234567  ← incorrecto
Authorization: 0123456789abcdef0123456789abcdef01234567         ← incorrecto
```

“Token de conexión inválido”

El token no corresponde a ninguna conexión activa. Revisa en orden:

1. **Compáralo carácter por carácter** con el de Gestionar conexión → Token API. En la mayoría de los casos el token de la integración quedó desactualizado o se cargó en el lugar equivocado del código.
2. **¿Lo regeneraste?** El anterior deja de funcionar de inmediato.
3. **¿Es el token de la conexión** y no la API Key de tu usuario?
4. **¿La URL base es la correcta?** `https://app.apigateway.cl/api/v2/`, no `apigateway.cl`.

“La conexión está inactiva”

El token está bien: la conexión está **suspendida**. Revisa Errores 401 y 402: créditos y conexión suspendida.

“El usuario propietario de esta conexión está inactivo”

El token y la conexión están bien, pero la **cuenta del usuario** dueño de la conexión está deshabilitada. Mientras siga así, ninguna de sus conexiones puede consultar. Genera un ticket desde

el correo titular de la cuenta para revisar el caso.

Credenciales del SII incorrectas

Cuando el `401` incluye un código de error del propio SII:

```
{
  "detail": "En la respuesta del SII se obtuvo el código de error #612. Descripción del error oficial del SII: Contraseña incorrecta."
}
```

el problema está en las credenciales que envías en el cuerpo, no en la plataforma.

1. **Verifica la clave** ingresando directamente a www.sii.cl.
2. **Verifica el formato del RUT**: sin puntos, con guión, `11111111-1`. Un RUT con puntos puede producir errores que parecen de otra naturaleza, incluidos timeouts de navegación.
3. **Verifica la estructura de `auth`**: debe ser exactamente `auth.pass.rut` y `auth.pass.clave`.
4. **Si cambiaste la clave recientemente**, actualízala en tu integración y fuerza una sesión nueva con `auth_cache=0` en la primera consulta.

“Se debe volver a autenticar al usuario” o “El SII está solicitando volver a autenticar al usuario”

```
{ "code": 401, "detail": "Se debe volver a autenticar al usuario, problema con la sesión del SII (HTTP200)." }
```

```
{ "code": 401, "detail": "El SII está solicitando volver a autenticar al usuario (HTTP200)." }
```

El código entre paréntesis puede variar (`HTTP200`, `HTTP302` o `HTTP401`) según cómo respondió el SII. La sesión reutilizada quedó en mal estado. Puede venir acompañado de la cabecera `X-Auth-Session-Problem: 1`.

Agrega `auth_cache=0` a la URL en esa consulta, y vuelve a operar sin el parámetro después.

No lo dejes puesto en producción

Cada `auth_cache=0` equivale a un login nuevo en el SII. Usarlo en todas las peticiones aumenta el riesgo de que el SII bloquee tus accesos.

401 en un recurso específico, mientras otros funcionan

Si un recurso devuelve `401` de forma reproducible y otros funcionan con las mismas credenciales, revisa el **método de autenticación que ese recurso requiere**. Algunos exigen certificado digital y no RUT y clave.

Un caso real: `bienes_raices/propiedades/contribuyente` devolvía `401` en contribuyentes con muchos roles inmobiliarios al consultarlo con RUT y clave. Ese recurso requiere **certificado digital**.

Revisa Token y certificado y la documentación del recurso en /docs/api.

Última actualización el 06/11/2026