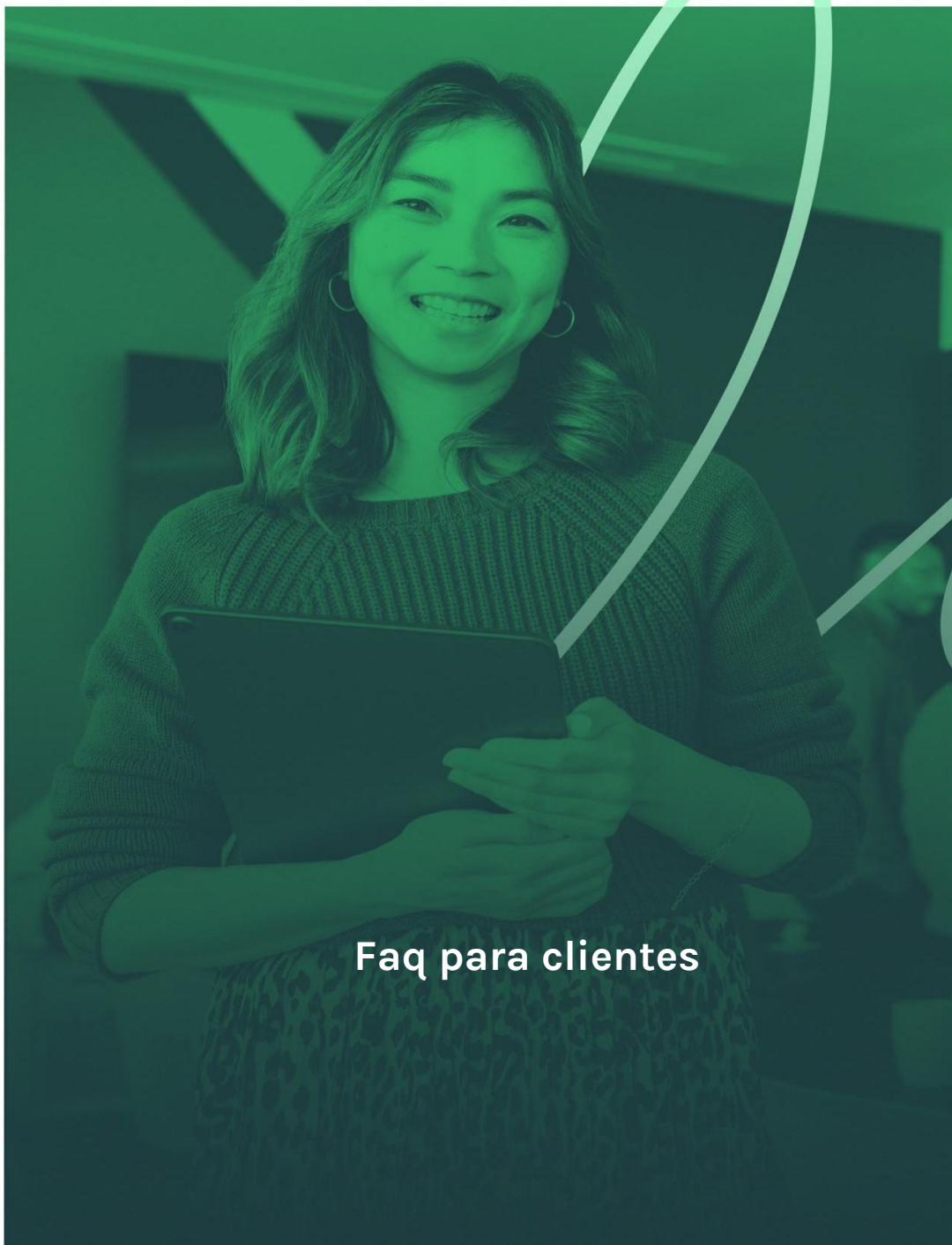




Faq para clientes

Contexto

A raíz de un cambio en la aplicación de Salesforce la conexión que utilizaba el plugin necesita una configuración de seguridad adicional para que Salesforce pueda seguir autorizando el acceso correctamente.

Para adaptar Signaturit, se debe crear una configuración OAuth específica en Salesforce y donde se actualicen las credenciales de conexión. De esta forma, Salesforce reconocerá y autorizará de nuevo a Signaturit, permitiendo que los eventos y estados de los envíos se sincronicen correctamente.

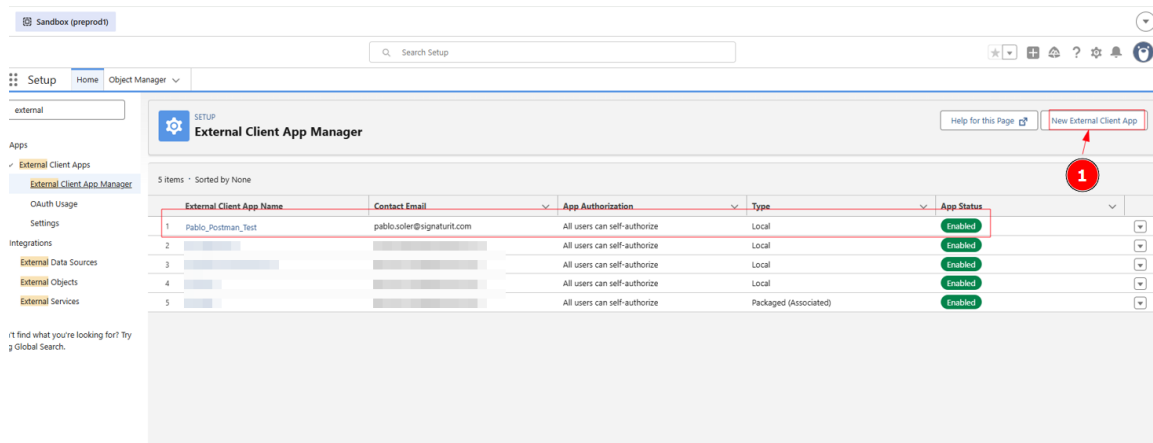
Pasos que seguir:

1. Crear una aplicación de conexión en Salesforce

Se debe crear una **External Client App** en el entorno del cliente para que Salesforce pueda identificar y autorizar de forma segura la conexión con Signaturit.

La ruta es: **Setup** → **External Client App Manager** → **New External Client App**, seleccionando **Distribution State: Local**.

Se adjunta imagen de ejemplo:



2. Habilitar OAuth:

Se activa **OAuth** dentro de la app para que Salesforce permita la autenticación segura con Signaturit. Sin esto, la conexión no puede validarse correctamente.

Dentro de la app, ir a **Settings** → **OAuth Settings** → marcar "Enable OAuth".

Setup Home Object Manager

Internal

ps

External Client Apps

External Client App Manager

OAuth Usage

Settings

Integrations

External Data Sources

External Objects

External Services

Find what you're looking for? Try Global Search.

Policies Settings Package Defaults

Configure basic settings for the external client app and plugins. Save

Basic Information

* External Client App Name Pablo_Postman_Test

* API Name Pablo_Postman_Test

* Contact Email pablo.soler@signaturit.com

* Distribution State Local

Contact Phone Enter a phone number...

Info URL Enter a URL...

Logo Image URL Enter a URL...

Choose one of our sample logos.

Choose one of our sample logos.

OAuth Settings 2

Disable OAuth

3. Configurar la URL de retorno

En este apartado se introduce la **Callback URL**, es decir, la dirección a la que Salesforce devolverá al usuario después de completar la autenticación.

Debe incluirse la URL correspondiente al entorno de Signaturit y, si es necesario, las direcciones adicionales para realizar pruebas. Es importante que la URL coincida exactamente con la que utiliza Signaturit; incluso una pequeña diferencia puede impedir que la conexión se complete correctamente.

- La real que usa el backend de Signaturit en el entorno correspondiente (ej. <https://app.sandbox.signaturit.com/salesforce/auth>) (ej. <https://app.signaturit.com/salesforce/auth>) (Entorno de Producción)
- <https://oauth.pstmn.io/v1/callback> (si se va a probar con Postman)
- <https://test.salesforce.com/services/oauth2/success> (para pruebas manuales)

OAuth Settings

App Settings

Consumer Key and Secret

* Callback URL

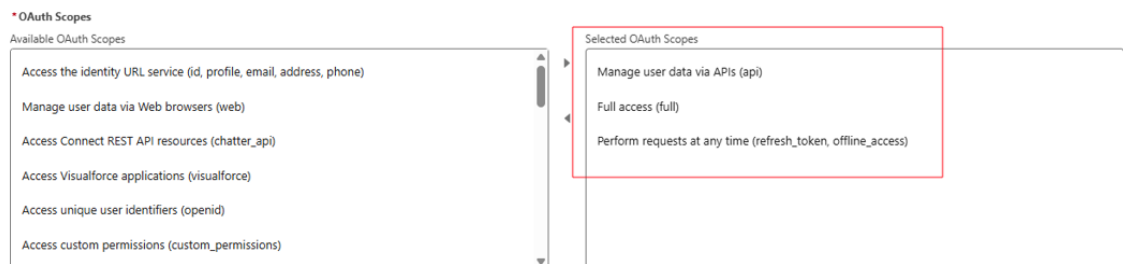
<https://app.sandbox.signaturit.com/salesforce/auth>

*El path debe coincidir carácter por carácter con el que envía el backend. Para confirmarlo: en la pantalla de integración de Salesforce en Signaturit, inspeccionar el enlace del botón "Regístrate" — la URL contiene el parámetro `redirect_uri=` con el valor exacto a usar.

4. Seleccionar los permisos de acceso

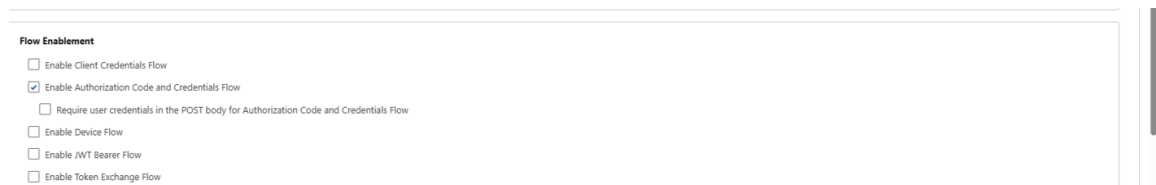
Aquí se eligen los permisos que Salesforce dará a la integración. Como mínimo, hay que permitir acceso para consultar datos y mantener la conexión activa en el tiempo.

En concreto, se seleccionan los permisos **Manage user data via APIs (api)** y **Perform requests at any time (refresh_token, offline_access)**, que son los necesarios para que Signaturit pueda trabajar correctamente con Salesforce sin que la sesión caduque enseguida.



5. Activar el tipo de flujo de autorización

Activar Enable Authorization Code and Credentials Flow.



6. Proveedores autorizados (PRO)

Aquí se dejan activadas las medidas de seguridad recomendadas para proteger la autenticación. En particular, **PKCE** debe quedarse activado porque añade una capa extra de protección al proceso de inicio de sesión.

La opción de **restringir por IP los refresh tokens** solo hace falta si el cliente quiere limitar desde qué redes se puede renovar la conexión. Si no existe ese requisito, puede dejarse desactivada para no complicar el acceso.

- Require Proof Key for Code Exchange (PKCE) → dejar activado.

- Enforce Refresh Token IP Allowlist → activar solo si se necesita restringir por IP.

Security

- ☒ Require secret for Web Server Flow
- ☒ Require secret for Refresh Token Flow
- ☒ Require Proof Key for Code Exchange (PKCE) extension for Supported Authorization Flows
- ☒ Enable Refresh Token Rotation
To change this required setting, contact Support.
- ☐ Issue JSON Web Token (JWT)-based access tokens for named users
- ☒ Limit Idle Refresh Token Time-to-Live (TTL) to 30 Days ⓘ
To change this required setting, contact Support.
- ☐ Enforce Refresh Token IP Allowlist ⓘ

7. Obtener las credenciales de conexión

En este paso se generan las credenciales que identifican la app ante Salesforce: **Consumer Key** y **Consumer Secret**. Son los datos que luego se usarán para conectar Signaturit con esta app. Salesforce las muestra dentro de **Manage Consumer Details**, y por seguridad puede pedir una verificación adicional por email o SMS antes de mostrarlas.

▼ OAuth Settings Disable OAuth

App Settings

Consumer Key and Secret ⓘ

8. Proveedores autorizados (PRO)

Facilitar el **Client ID/Secret** a Signaturit para que lo pueda registrar en su base de datos.

9. Probar la conexión desde la pantalla de integración de Salesforce en la app de Signaturit.

Configuración

[Mi perfil](#)[Integraciones](#)

Utilice nuestra API

Este token te otorga acceso a nuestra API. No lo compartas con nadie más. [Más información](#)

KNdcaGQTTIESmvlLBosLFZmhpDmaeL...

Copiar token

Verificación de dominio

Utiliza tu token de acceso para definir los dominios o IP desde los que aceptaremos llamadas a la API. Si no añades ninguno, cualquier dominio o IP será válido.

+ Agregar dominio o IP

Conecte Signaturit con otras herramientas

Las integraciones hacen que su cuenta de Signaturit sea aún más poderosa y le permiten trabajar con herramientas que ya está utilizando.

**Salesforce**
Conecte Salesforce con Signaturit para obtener la integración nativa más sencilla y segura.

◀

Por favor, contacta con soporte para la integración con Salesforce®.

Configurar Salesforce

Por favor, siga estos pasos para proceder con la integración:

1. Ve al sitio web de Salesforce y regístrate.

Registrate ☒

2. Copia el token de Salesforce.

Salesforce Token

Cerrar

Aceptar:



Security Warning

If you allow this app, it can access your data and act on your behalf. If someone contacted you via phone or email and instructed you to use this app, **do not proceed.**

Instead, report the incident to your admin and security team, and to Salesforce at <https://security.salesforce.com/contact>.

Signaturit is asking to:

- Access the Identity URL service
- Manage user data via APIs
- Manage user data via Web browsers
- Access Connect REST API resources
- Access Visualforce applications
- Access unique user identifiers
- Access custom permissions
- Access Analytics REST API resources
- Access Analytics REST API Charts Geodata resources
- Manage hub connections
- Manage Pardot services
- Access Lightning applications
- Access content resources
- Manage Data Cloud Ingestion API data
- Manage Data Cloud profile data
- Perform SQL queries on Data Cloud data
- Access chatbot services
- Perform segmentation on Data Cloud data
- Manage Data Cloud Identity Resolution
- Access Headless Forgot Password API
- Manage Data Cloud Calculated Insight data
- Access Headless Registration API
- Access Interaction API resources
- Access all Data Cloud API resources
- Access Einstein GPT services
- Access Headless Passwordless Login API
- Access Salesforce hosted MCP servers
- Access Service Cloud Real Time API
- Authorize user for Data Cloud Data Governance
- Access Agent-to-Agent API
- Perform requests at any time

Do you want to allow access for pablo.soler@signaturit.preprod1? (Not you?)

Deny

Allow

To revoke access at any time, go to your personal settings.

Una vez realizados estos pasos, vemos como los eventos de Signaturit hacia SF vuelven a funcionar:

Reenviar evento

Volver

1 of 34

<

>

Fecha

07/08/2026 - 12:31:20

Dominio

signaturit-es-
preprod1.sandbox.my.salesforce.com

Método

POST

Path

https://signaturit-es-
preprod1.sandbox.my.salesforce.com/services/apexrest/signaturit/SIG_SignatureRequestWS

Content type

application/x-www-form-urlencoded

POST parameters

KEY	VALUE
document[created_at]	2026-08-07T12:29:04+0000
document[file][name]	Template_Signaturit.pdf
document[file][pages]	1
document[file][size]	56195
document[id]	c3c43d30-96f2-4e31-8eab-12be97d4b91d
document[events][0][created_at]	2026-08-07T12:31:03+0000
document[events][0][type]	sms_processed
document[signature][id]	167b7797-e8d5-438a-8ba2-935f97e30fb
document[email]	pablo.soler@signaturit.com
document[name]	pablo
document[signer_phone]	+34649462104
document[status]	ready
created_at	2026-08-07T12:31:17+0000
type	sms_entered

Estado

200 OK

Response body

```
{ 2 items
  "status": 200
  "message": [] 0 items
}
```

Y el estado de los envíos realizados desde el plugin se actualizan correctamente:

Details

Name

MIGUEL TEST

Parent Id

059W0000001aAHQAQ

Signature Id

167b7797-e8d5-438a-8ba2-935f976e30fb

Parent

Pablo Soler

Email

Subject

#rueba SF contrato de trabajo

Rich Body

Hola,

Tu envío el documento a firmar.

Un saludo,

Status

Number Signatures

7/08/2026 14:32

Number Completed Signatures

Completed

Number Cancel Signatures

Completed

Last Status Date

Status

Progress

Completed

End User Error

Signature

pablo

Progress:

Type:

Name:

Signature

#rueba_pablo

Progress:

Origin:

Type:

Files (0)