

Strataflows

Sample API Callouts — Salesforce AppExchange Security Review
Prepared by: Luke Viering, Founder | luke@strataflows.io | strataflows.io

Overview

This document provides accurate sample HTTP requests and responses for all API callouts made by Strataflows. All callouts are executed server-side from Next.js API routes hosted on Vercel. No API calls are made from the client browser. OAuth tokens are never exposed to client-side code. Values shown are representative examples — not real production credentials.

Integration	Protocol	Auth Method	Direction	Writes Back
Salesforce	HTTPS	OAuth 2.0 + PKCE	Strataflows reads SF	None
Gong	HTTPS	OAuth 2.0	Strataflows reads Gong	None
Google Workspace	HTTPS	OAuth 2.0	Strataflows reads Google	None
Microsoft 365	HTTPS	OAuth 2.0	Strataflows reads M365	None
OpenAI	HTTPS	API Key (server)	Prompts only	N/A
Stripe	HTTPS	API Key (server)	Billing only	N/A

1. Salesforce OAuth 2.0 — Authorization Request (with PKCE)

Strataflows implements PKCE (Proof Key for Code Exchange) S256 for enhanced OAuth security. The server generates a code_verifier and code_challenge before redirecting the user to Salesforce.

Scopes requested: api refresh_token offline_access id

Authorization URL (GET redirect)

```
GET https://login.salesforce.com/services/oauth2/authorize HTTP/1.1

?response_type=code

&client_id=3MVG9WVXk15qiz1KQEXHhSvddeF4cx_3XjvwyyScBm3j...

&redirect_uri=https%3A%2F%2Fstrataflows.io%2Fapi%2Fsalesforce%2Fcallback

&scope=api%20refresh_token%20offline_access%20id

&state=example_csrf_state_token

&code_challenge=E9MeIhoa20wvFrEMTJguCHaoeK1t8URWbuGJSstw-cM

&code_challenge_method=S256
```

2. Salesforce OAuth 2.0 — Token Exchange

After the user authorizes Strataflows, Salesforce redirects to the callback URL with an authorization code. The server exchanges this code for tokens. Token expiry is computed as now + 2 hours (Salesforce does not return expires_in).

Request

```
POST https://login.salesforce.com/services/oauth2/token HTTP/1.1

Host: login.salesforce.com
```

```
Content-Type: application/x-www-form-urlencoded

Accept: application/json

grant_type=authorization_code

&code=aPrxhgZ2MIyE_example_auth_code

&client_id=3MVG9WVXk15qiz1KQEXHhSvddeF4cx_3XjvwyScBm3j...

&client_secret=REDACTED

&redirect_uri=https%3A%2F%2Fstrataflows.io%2Fapi%2Fsalesforce%2Fcallback

&code_verifier=dBjftJeZ4CVP-mB92K27uhbUJU1p1r_wW1gFwF0EjXk
```

Response (200 OK)

```
HTTP/1.1 200 OK

Content-Type: application/json

Cache-Control: no-store

{

  "access_token": "00DdL00000tqqcL!example_access_token",

  "refresh_token": "5Aep861example_refresh_token",

  "instance_url": "https://strataflows-dev-ed.my.salesforce.com",

  "id": "https://login.salesforce.com/id/00DdL00000tqqcLUAQ/005dL000002example",

  "token_type": "Bearer",

  "issued_at": "1714243200000",

  "signature": "example_signature"

}

// token_expires_at stored as: Date.now() + 2 * 60 * 60 * 1000 (2 hours)

// Tokens stored server-side in salesforce_connections table. Never returned to browser.
```

3. Salesforce OAuth 2.0 — Token Refresh

Token refresh is triggered in two ways: (A) proactively via a 5-minute grace window check before each API call in `getValidToken()`, and (B) reactively on a 401 response mid-sync via `withTokenRetry()`. Up to 3 retry attempts with 1-second delay between attempts.

Refresh trigger condition: `token_expires_at` is missing OR `token_expires_at < Date.now() + 5 minutes`

Request

```
POST https://login.salesforce.com/services/oauth2/token HTTP/1.1

Host: login.salesforce.com

Content-Type: application/x-www-form-urlencoded

Accept: application/json

grant_type=refresh_token
```

```
&refresh_token=5Aep861example_refresh_token

&client_id=3MVG9WVXk15qiz1KQEXHhSvddeF4cx_3XjvwyScBm3j...

&client_secret=REDACTED
```

Response (200 OK)

```
HTTP/1.1 200 OK

Content-Type: application/json

{
  "access_token": "00DdL00000tqqcL!new_access_token",
  "instance_url": "https://strataflows-dev-ed.my.salesforce.com",
  "token_type": "Bearer",
  "issued_at": "1714246800000"
}

// New token_expires_at = Date.now() + 2 hours. Persisted to salesforce_connections.
// On 3rd consecutive failure: sync_status set to 'error' in database.
```

4. Salesforce REST API — Get Authenticated User Identity

Fetches the authenticated user's Salesforce identity to associate synced data with the correct Strataflows account and support manager mode rep detection.

Request

```
GET https://login.salesforce.com/id/00DdL00000tqqcLUAQ/005dL000002example HTTP/1.1

Authorization: Bearer 00DdL00000tqqcL!example_access_token

Accept: application/json
```

Response (200 OK)

```
HTTP/1.1 200 OK

Content-Type: application/json

{
  "user_id": "005dL000002example",
  "organization_id": "00DdL00000tqqcLUAQ",
  "username": "luke@strataflows.io",
  "display_name": "Luke Viering",
  "email": "luke@strataflows.io",
  "email_verified": true
}
```

5. Salesforce REST API — Query Opportunities

Queries open opportunities owned by the authenticated user OR where the user is the owner's manager (supports manager mode rep visibility). Ordered by last modified, limited to 1000. Pagination follows Salesforce `nextRecordsUrl` with a safety cap of 20 pages.

Request

```
GET https://strataflows-dev-ed.my.salesforce.com/services/data/v59.0/query HTTP/1.1

Authorization: Bearer 00DdL00000tqqcL!example_access_token

Accept: application/json

?q=SELECT+Id, Name, StageName, Amount, CloseDate, AccountId, Account.Name,
Account.Website, OwnerId, LastModifiedDate, Description, NextStep,
LeadSource, Type
+FROM+Opportunity
+WHERE+(OwnerId+=+'005dL000002example'
+OR+Owner.ManagerId+=+'005dL000002example')
+AND+IsClosed+=+false
+ORDER+BY+LastModifiedDate+DESC
+LIMIT+1000
```

Response (200 OK)

```
HTTP/1.1 200 OK

Content-Type: application/json

{
  "totalSize": 12,
  "done": true,
  "records": [
    {
      "attributes": { "type": "Opportunity" },
      "Id": "006dL000003example",
      "Name": "Acme Corp – Enterprise License",
      "StageName": "Proposal/Price Quote",
      "Amount": 125000,
      "CloseDate": "2026-06-30",
      "AccountId": "001dL000004example",
      "Account": { "Name": "Acme Corp", "Website": "https://acmecorp.com" },
      "OwnerId": "005dL000002example",
      "LastModifiedDate": "2026-04-25T14:30:00.000Z",
      "Description": "Enterprise deal for Q2 close",
```

```
"NextStep": "Send updated security review",

"LeadSource": "Partner Referral",

"Type": "New Business"

}

],

"nextRecordsUrl": null

}
```

6. Salesforce REST API — Query Accounts

Fetches Account records for all AccountIds found in the Opportunities query. Used for account enrichment and domain learning. No ORDER BY or LIMIT applied — constrained by the opportunity set.

Request

```
GET https://strataflows-dev-ed.my.salesforce.com/services/data/v59.0/query HTTP/1.1

Authorization: Bearer 00DdL00000tqqcL!example_access_token

Accept: application/json

?q=SELECT+Id,Name,Website,Industry,NumberOfEmployees,

BillingCity,BillingState,Description,Phone

+FROM+Account

+WHERE+Id+IN+('001dL000004example','001dL000005example')
```

Response (200 OK)

```
HTTP/1.1 200 OK

Content-Type: application/json

{

  "totalSize": 2,

  "done": true,

  "records": [

    {

      "Id": "001dL000004example",

      "Name": "Acme Corp",

      "Website": "https://acmecorp.com",

      "Industry": "Technology",

      "NumberOfEmployees": 500,

      "BillingCity": "San Francisco",

      "BillingState": "CA",
```

```
"Description": "Enterprise software company",

"Phone": "+1-415-555-0100"

}

]

}
```

7. Salesforce REST API — Query Contacts

Fetches Contact records for all accounts. Used for stakeholder mapping and email domain discovery for Google/Microsoft signal matching. Limited to 1000.

Request

```
GET https://strataflows-dev-ed.my.salesforce.com/services/data/v59.0/query HTTP/1.1

Authorization: Bearer 00DdL00000tqqcL!example_access_token

Accept: application/json

?q=SELECT+Id,Name,Title,Email,Phone,AccountId,Department

+FROM+Contact

+WHERE+AccountId+IN+('001dL0000004example')

+LIMIT+1000
```

Response (200 OK)

```
HTTP/1.1 200 OK

Content-Type: application/json

{

  "totalSize": 3,

  "done": true,

  "records": [

    {

      "Id": "003dL0000005example",

      "Name": "Jane Smith",

      "Title": "VP of Engineering",

      "Email": "jane.smith@acmecorp.com",

      "Phone": "+1-415-555-0101",

      "AccountId": "001dL0000004example",

      "Department": "Engineering"

    }

  ]

}
```

```
}
```

8. Salesforce REST API — Query Activities (Tasks only)

Fetches Task records for opportunities from the last 90 days. Events are not queried. Ordered by activity date descending, limited to 500.

Request

```
GET https://strataflows-dev-ed.my.salesforce.com/services/data/v59.0/query HTTP/1.1

Authorization: Bearer 00DdL00000tqqcL!example_access_token

Accept: application/json

?q=SELECT+Id,Subject,ActivityDate,Description,WhatId,
Who.Name,Who.Email,Status,Type
+FROM+Task
+WHERE+WhatId+IN+('006dL000003example')
+AND+ActivityDate+>=+LAST_N_DAYS:90
+ORDER+BY+ActivityDate+DESC
+LIMIT+500
```

Response (200 OK)

```
HTTP/1.1 200 OK

Content-Type: application/json

{
  "totalSize": 4,
  "done": true,
  "records": [
    {
      "Id": "00TdL0000006example",
      "Subject": "Follow up on security review",
      "ActivityDate": "2026-04-28",
      "Description": "Send updated pricing deck",
      "WhatId": "006dL000003example",
      "Who": { "Name": "Jane Smith", "Email": "jane.smith@acmecorp.com" },
      "Status": "Completed",
      "Type": "Call"
    }
  ]
}
```

```
}
```

9. Salesforce REST API — Query Users (Rep Enrichment)

Fetches User records for rep identity enrichment in manager mode. Called when the Opportunities query returns OwnerId values that need to be resolved to names and emails. Limited to 200.

Request

```
GET https://strataflows-dev-ed.my.salesforce.com/services/data/v59.0/query HTTP/1.1

Authorization: Bearer 00DdL00000tqqcL!example_access_token

Accept: application/json

?q=SELECT+Id,Name,Email

+FROM+User

+WHERE+Id+IN+('005dL000002example','005dL000007example')

+LIMIT+200
```

Response (200 OK)

```
HTTP/1.1 200 OK

Content-Type: application/json

{
  "totalSize": 2,
  "done": true,
  "records": [
    {
      "Id": "005dL000002example",
      "Name": "Luke Viering",
      "Email": "luke@strataflows.io"
    }
  ]
}
```

10. Salesforce Disconnect — Token Nullification

When a user disconnects Salesforce from Strataflows, the server nulls all token columns in the `salesforce_connections` table and sets `sync_status` to 'disconnected'. Note: Strataflows does not call the Salesforce OAuth revoke endpoint on disconnect — token revocation is handled by nulling stored values. This differs from the Google integration which does call Google's revoke endpoint.

Note: No outbound HTTP call is made to Salesforce on disconnect. Tokens are invalidated by deletion from the Strataflows database.

Internal Database Operation (Supabase)

```
// app/api/salesforce/disconnect/route.ts
```



```
// Server-side Supabase UPDATE – no outbound Salesforce API call

UPDATE salesforce_connections SET

access_token = NULL,

refresh_token = NULL,

token_expires_at = NULL,

sync_status = 'disconnected',

sync_error = NULL

WHERE user_id = :authenticated_user_id

// Result: tokens deleted from database.

// Salesforce session remains active on Salesforce side until natural expiry.

// Users can revoke access directly in Salesforce Settings > Connected Apps.
```

Security Notes

Item	Implementation
PKCE	OAuth 2.0 PKCE S256 implemented. code_verifier generated server-side. code_challenge sent in authorization URL.
Token storage	All tokens stored server-side in Supabase salesforce_connections table. AES-256 at rest. Never logged or exposed to browser.
Token refresh	Proactive 5-minute grace window check before each API call. Reactive 401 retry mid-sync. Up to 3 attempts with 1-second delay.
TLS	All outbound calls use HTTPS. login.salesforce.com and instance_url are always HTTPS. Enforced by Vercel for inbound traffic.
Read-only	Zero POST/PATCH/PUT/DELETE calls to Salesforce API. Strataflows reads only — no data written back to Salesforce.
Manager mode SOQL	Opportunities query includes Owner.ManagerId = userId to support manager visibility of rep deals. Read-only throughout.
Pagination	nextRecordsUrl followed until done: true. Hard safety cap of 20 pages per query to prevent runaway loops.
State parameter	OAuth state token validated on callback to prevent CSRF attacks.
Disconnect	Tokens nulled in database on disconnect. Users can also revoke directly in Salesforce Connected Apps settings.