# NG SIEM - Salesforce Integration via JWT Authentication

## Introduction

The Salesforce integration enables you to monitor your Salesforce instance. Salesforce is a customer relationship management (CRM) platform that supports businesses in managing marketing, sales, commerce, service, and IT teams from a unified platform accessible from anywhere.

---

### Recommendation - Username / Password Authentication Integration

#### Create New User Account

- Go to **Home** page of **Salesforce** and click **Setup** in the top right menu bar.
- In the left side you will see a **Quick Find** search textbox, type **Users**.
- Click **Users** and it will redirect you to the **Users setup** page.
- Click **New User** button and fill up the form:
  - First Name
  - Last Name
  - Email
  - Set **User License** to "**Salesforce**"
  - Choose an appropriate **Profile** (see below)
    - **Profile and Permission Set Configuration**
      - **Create a custom profile** or clone an existing minimal profile:
        - Clone the **"Standard User"** profile and name it something like **"Log Extraction Service"** or whatever you prefer.
        - Remove unnecessary permissions, keeping only:
          - **API Enabled**
          - **View Setup and Configuration**
          - **Specific object permissions for logs you need to extract**
      - **Essential permissions** for log extraction:
        - **API Enabled** - Required for programmatic access
        - **View All Data** - If you need comprehensive log access

        - **Read** access to specific objects containing log data
    - Scroll down to the bottom and **check** the box that says **Generate new password and notify user immediately.**
    - Click **Save**.
- Open the account and set a new password.

Please take note of the **Email Address, Username** and **Password** associated with this account, as they will be required during the API and integration setup process.

## Salesforce instance URL

This is the URL of your Salesforce Organization.

- **Salesforce Classic:** Given the example URL https://na9.salesforce.com/home/home.jsp, the Salesforce Instance URL is extracted as https://na9.salesforce.com.
- **Salesforce Lightning:** The instance URL is available under your user name in the **View Profile** tab. Use the correct instance URL in case of Salesforce Lightning because it uses *.lightning.force.com but the instance URL is *.salesforce.com.

> Ensure the **Instance URL** is noted, as it will be used in both API creation and integration steps.

---

## Client Key and Client Secret for Authentication

To use this integration, you need to create a new Salesforce Application using OAuth. Follow these steps to create a connected application in Salesforce:

- Log in to **Salesforce** with the user credentials you want to collect data with.
- Click **Setup** in the top right menu bar.
- In the **Quick Find textbox**, search for **App Manager** or you can scroll down to **PLATFORM TOOLS** and select **App Manager.**
- **In the upper right corner, choose the New External Client App.**
- Provide a name for the connected application. This name will be displayed in the App Manager and on its App Launcher tile.
- Enter the API name. The default is a version of the name without spaces. Only letters, numbers, and underscores are allowed. If the original app name contains any other characters, edit the default name.
- Enter the **email address** of the **new account** you created earlier.
- Under the **API (Enable OAuth Settings)** section, check the box for **Enable OAuth Settings**.
- In the **Callback URL** field, enter the instance URL as specified in **Salesforce instance URL.** Example URL: https://na9.salesforce.com
- Select the following OAuth scopes to apply to the connected app:
    - **Manage user data via APIs (api)**

    - **Perform requests at any time (refresh_token, offline_access)**
    - (Optional) If you encounter any permission issues during data collection, add the **Full access (full)** scope.
- Select **Require Secret for the Web Server Flow** to require the app's client secret in exchange for an access token.
- Select **Require Secret for Refresh Token Flow** to require the app's client secret in the authorization request of a refresh token and hybrid refresh token flow.
- **Then scroll up above the Callback URL on the App Settings you will see the Consumer Key and Secret button, click it.**
- **It will create another tab. Verify the user account by entering the Verification Code.**
- **Copy the `Consumer Key` and `Consumer Secret` from the Consumer Details section. These values should be used as the Client ID and Client Secret, respectively, in the integration.**
- **Close that tab and go back to the External Client App Manager. Click Save.**

**Username**

- Provide the **Username** of the new account that you created earlier.

**Password**

- Please provide the **password** you set upon accessing the new account.

> **Note:** When using a Salesforce instance with a security token, append the token directly to your password without spaces or special characters. For example, if your password is **Password** and your security token is **12345** enter: **Pasword12345**

---

## Token URL:

- Use the token URL to obtain authentication tokens for API access.
- For most Salesforce instances, the token URL follows this format: https://login.salesforce.com/services/oauth2/token.
- If you're using a Salesforce sandbox environment, use https://test.salesforce.com/services/oauth2/token instead.
- For custom Salesforce domains, replace `login.salesforce.com` with your custom domain name. For example, if your custom domain is `mycompany.my.salesforce.com`, the token URL becomes https://mycompany.my.salesforce.com/services/oauth2/token. This applies to Sandbox environments as well.
- In the Salesforce integration, we internally append `/services/oauth2/token` to the URL. Make sure that the URL you provide in the Salesforce integration is the base URL without the `/services/oauth2/token` part. For example, if your custom domain is `mycompany.my.salesforce.com`, the complete token URL would be

https://mycompany.my.salesforce.com/services/oauth2/token, but the URL you provide in the Salesforce integration should be https://mycompany.my.salesforce.com. In most cases, this is the same as the Salesforce instance URL.

> **NOTE:** Salesforce Lightning users must use URL with *.salesforce.com domain (similar to the Salesforce instance URL) instead of *.lightning.force.com because the Salesforce API does not work with *.lightning.force.com.

---

### API Version

To find the API version:

- Go to the search textbox and type **Api Version**. Click the first **Api Version** on the list.

***Reference**: https://www.integrate.io/blog/salesforce-rest-api-integration/*

> **Please provide these credentials and send it to CyTech Support:**

- **Salesforce instance URL**
- **Client key and client secret for authentication**
- **Username**
- **Password**
- **Token URL**
- **API version (Optional)**

---

# Recommendation - JWT Integration

This guide provides a step-by-step process for setting up a secure integration between Salesforce and AQUILA. The focus is on using JWT (JSON Web Token) Bearer authentication, which is recommended for server-to-server communication as it avoids sharing passwords. We'll cover preparing Salesforce (where you generate and upload required credentials) and entering those into AQUILA configuration fields.

## Prerequisites

- **Salesforce Account**: Admin access to create users and apps. Ensure your org supports API access (most do).
- **AQUILA Setup**: Access to Aquila (for managed agents).
- **Tools Needed**: OpenSSL (free, install via your OS: e.g., apt install openssl on Linux, or download for Windows/Mac).
- **Dedicated Integration User**: Create a Salesforce user specifically for this (not your personal account) with minimal permissions:
  - License: Salesforce Integration (API-only).
  - Permissions: "API Enabled" (required); add "View Event Log Files" if ingesting logs.

---

## Create a Connected App in Salesforce

This app generates the Client ID and links your certificate for JWT trust.

1. Log in to Salesforce > Click the gear icon > **Setup**.
2. Search for Setup > External Client Apps> Enable and click button **New Connected Apps.**
3. Fill in:
   - **Connected App Name**: e.g., "AQUILA JWT Integration".
   - **API Name**: Auto-fills (edit if needed).
   - **Contact Email**: Your integration user's email.
4. Under **API (Enable OAuth Settings)**:
   - Check **Enable OAuth Settings**.
   - **Callback URL**: Enter http://localhost (placeholder; not used in JWT).
   - **Selected OAuth Scopes**: Add api, refresh_token, offline_access. (Optional: Add full for broader access if needed.)
   - Check **Use digital signatures** > Upload salesforce_cert.crt.
5. Do **not** check any "Require Secret" options (no secret needed for JWT).
6. Click **Save** (wait 2-10 minutes for activation).
7. On the app page, copy the **Consumer Key**—this is your **Client ID**.
8. Click **Manage** > **Edit Policies** > Set **Permitted Users** to "Admin approved users are pre-authorized".
9. Assign the app to your integration user: Under **Profiles** or **Permission Sets**, add your user's profile.

Now Salesforce is ready—note your Instance URL (e.g., from your Salesforce homepage: https://your-instance.my.salesforce.com).

*References:*

*OAuth 2.0 JWT Bearer Flow for Server-to-Server Integration*

*OAuth Authorization Flows*

*Salesforce input | Beats*

*Salesforce Connector - How to authenticate using JWT*

> 

**Please provide these credentials and send it to CyTech Support:**

- **Username**
- **Client ID**
- **JWT Authentication Audience URL**
- **JWT Authentication Client Key Path**

## Summary Table

| Field | Username–Password | JWT |
|---|---|---|
| Client ID | ✔ required | ✔ required |
| Client Secret | ✔ required | ☐ not used |
| Username | ✔ required | ✔ required |
| Password | ✔ required | ☐ not used |
| Private Key Path | ☐ | ✔ required |
| Audience URL | ☐ | ✔ required |
| Token URL | ✔ required | ☐ leave blank |
| API Version | optional | optional |

*If you need further assistance, kindly contact our support at **support@cytechint.com** for prompt assistance and guidance.*

---

Revision #19
Created 23 September 2025 08:13:58 by Richmond Abella
Updated 3 December 2025 07:21:29