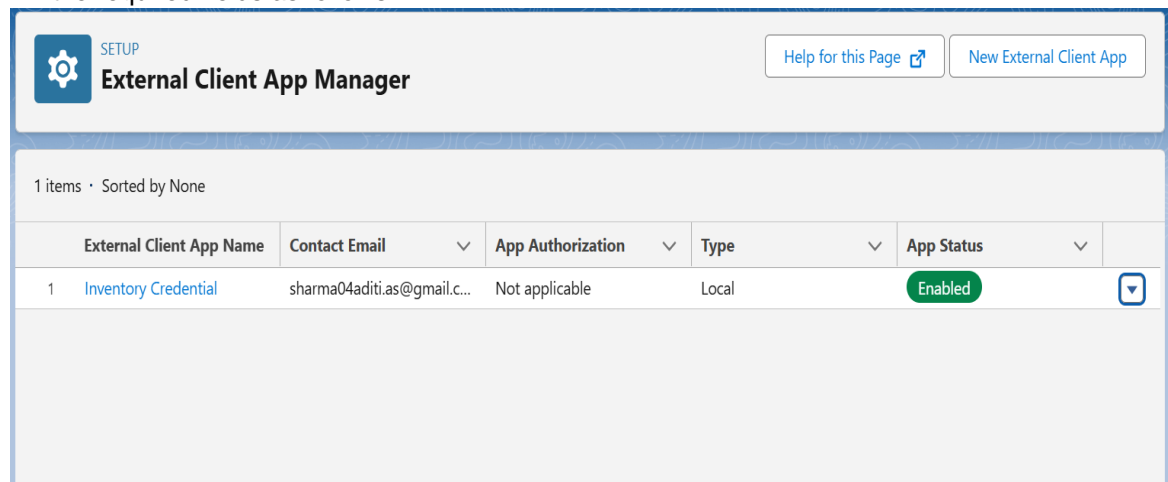


Phase 7: Integration & External Access - Step by Step Guide

Step 1: Create OAuth Client in External System (App Manager)

1. Login to your external system (ERP, API Gateway, Identity Provider) with Admin/Developer role.
2. Navigate to Developer → App Manager / Applications / OAuth Clients.
3. Click 'New Application' or 'Register Client'.
4. Fill the required fields as follows:

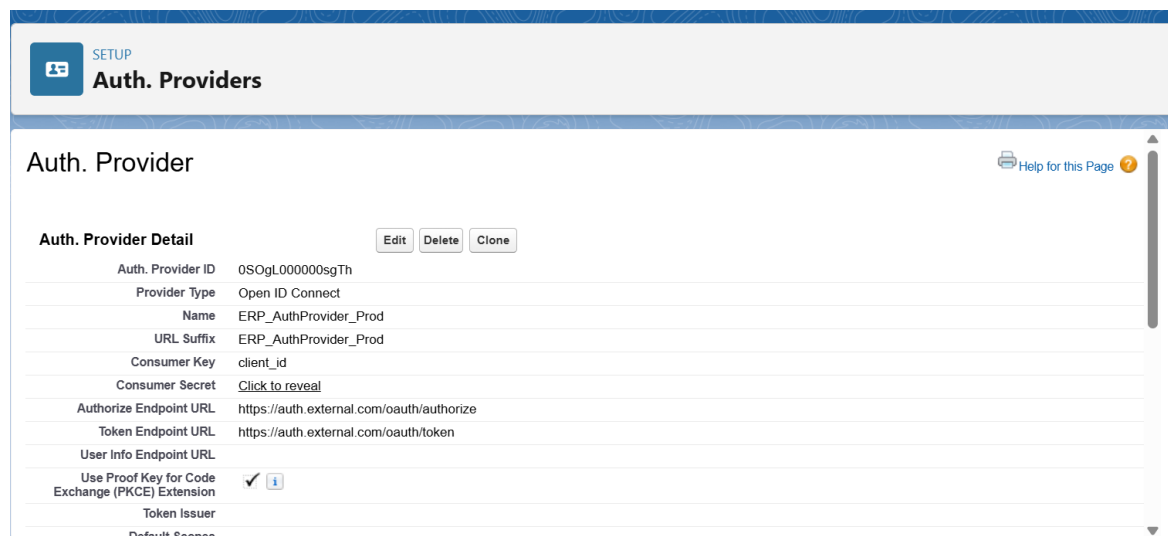


The screenshot shows the 'External Client App Manager' interface. At the top, there's a header with a 'SETUP' button and a 'New External Client App' button. Below the header, a table lists the registered clients. The table has columns for 'External Client App Name', 'Contact Email', 'App Authorization', 'Type', and 'App Status'. One client is listed: 'Inventory Credential' with contact email 'sharma04aditi.as@gmail.c...', 'Not applicable' for authorization, 'Local' for type, and 'Enabled' for status.

External Client App Name	Contact Email	App Authorization	Type	App Status
1 Inventory Credential	sharma04aditi.as@gmail.c...	Not applicable	Local	Enabled

Step 2: Configure Salesforce Auth Provider

1. In Salesforce, go to Setup → Quick Find → Auth. Providers → New.
2. Select Provider Type (OpenID Connect or Generic OAuth 2.0).
3. Fill in Consumer Key, Consumer Secret, Authorize URL, Token URL, Scopes.
4. Save. Salesforce generates a Callback URL.
5. Copy the Callback URL into the external system's App Manager.




The screenshot shows the 'Auth. Providers' configuration page in Salesforce. It displays the details for a provider named 'ERP_AuthProvider_Prod'. The configuration includes fields for Auth. Provider ID, Provider Type (Open ID Connect), Name, URL Suffix, Consumer Key, Consumer Secret, Authorize Endpoint URL, Token Endpoint URL, User Info Endpoint URL, and a checkbox for 'Use Proof Key for Code Exchange (PKCE) Extension' which is checked. There are also buttons for 'Edit', 'Delete', and 'Clone'.

Auth. Provider Detail	
Auth. Provider ID	0SOgLO00000sgTh
Provider Type	Open ID Connect
Name	ERP_AuthProvider_Prod
URL Suffix	ERP_AuthProvider_Prod
Consumer Key	client_id
Consumer Secret	Click to reveal
Authorize Endpoint URL	https://auth.external.com/oauth/authorize
Token Endpoint URL	https://auth.external.com/oauth/token
User Info Endpoint URL	
Use Proof Key for Code Exchange (PKCE) Extension	<input checked="" type="checkbox"/>
Token Issuer	
Default Scopes	

Step 3: Certificates

1. In Salesforce, go to Setup → Certificate and Key Management.
2. Create a Self-Signed Certificate OR Import an existing key.

 **SETUP**
Certificate and Key Management

Certificates

[Help for this Page](#)


Certificate and Key Detail [Edit](#) [Delete](#) [Download Certificate](#)

Label	SF_JWT_ERP_Prod	Unique Name	SF_JWT_ERP_Prod
Type	Self-Signed	Active	<input checked="" type="checkbox"/>
Expiration Date	9/24/2026, 5:00 PM	Created Date	9/25/2025, 2:24 AM
Key Size	2048	Exportable Private Key	<input checked="" type="checkbox"/> i
Certificate	C=USA, ST=CA, L=San Francisco, O=Salesforce.com, OU=00DgL00000BKqtl, CN=SF_JWT_ERP_Prod Expiration: 25 Sep 2026 00:00:00 GMT		

[Edit](#) [Delete](#) [Download Certificate](#)

Step 4: Create Named Credential in Salesforce

1. In Salesforce, Setup → Named Credentials → New.
- 2.Label: ERP_Inventory_API

 **SETUP**
Named Credentials

Named Credentials [External Credentials](#) [External Auth Identity Providers](#)

1 Items · Sorted by Label [New](#) ▼

Label	Type	URL	External Credential	Actions
InventoryAPI	Secured Endpoint	https://api.myinventory.com	InventoryCredential	▼

