Creating a secure Bring Your Own External Client Application for Valo.ai

Introduction

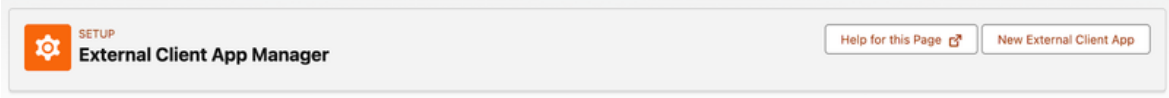
This guide provides a walkthrough for configuring an **External Client Application (ECA)** within Salesforce. This connection serves as the primary integration point for linking **Valo.ai** to your Salesforce environment, serving as the modern successor to the traditional Connected App (CA).

Why the Transition to ECA?
While Valo currently supports both connection methods, Salesforce has officially designated Connected Apps for **End-of-Life** starting with the **Spring '26 release**. To ensure your integration remains secure and future-proof, we have optimized the Valo platform to utilize the enhanced security framework offered by the new ECA architecture.
The process contains the following main steps:

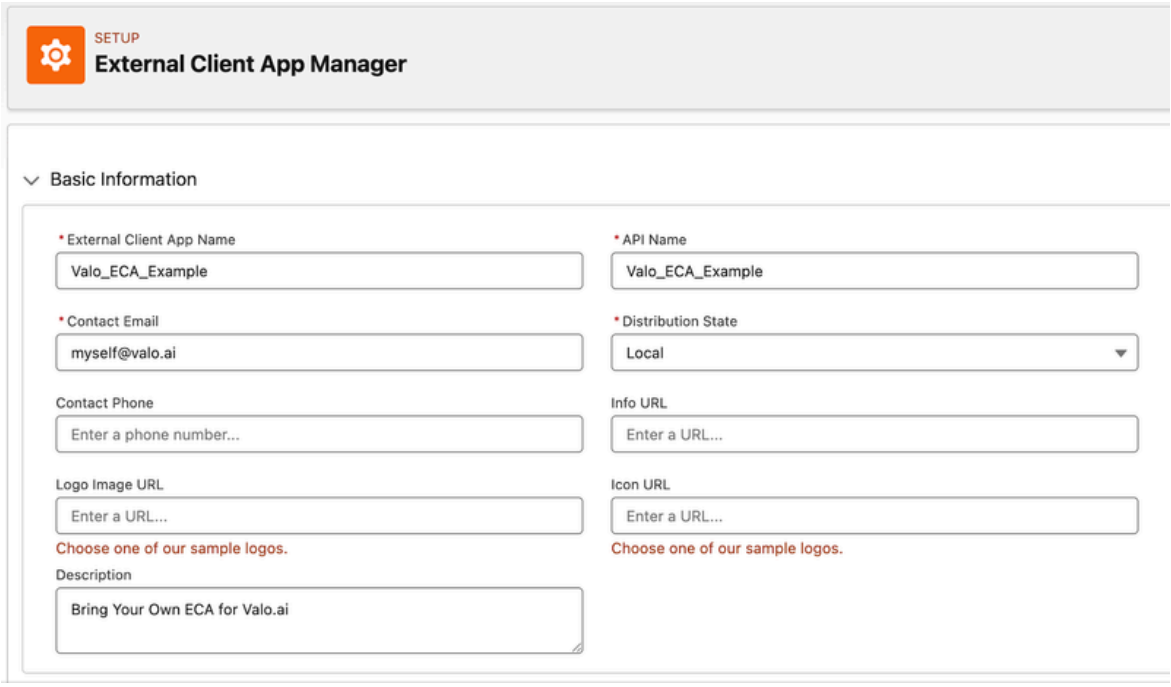
1. **Navigate to ECA Setup page**
2. **Fill in Basic Information**
3. **Configure OAuth Settings**
4. **Enhanced Security Settings**
5. **Finalize ECA creation and retrieve Client ID and secret**
6. **Additional steps**

Step 1: Navigate to ECA Setup page

After logging in to the Salesforce organization navigate to
Setup → Apps → External Client Apps → External Client App Manager



Step 2: Fill in Basic Information

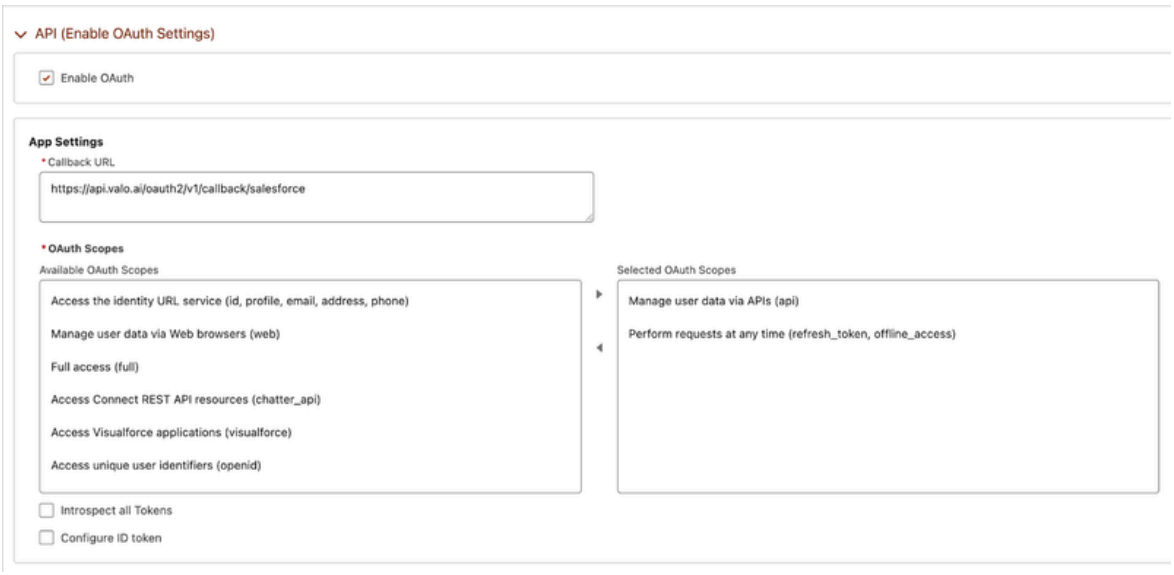


Enter the basic information for your configuration. Since these details are primarily for internal use, you may choose values that best suit your organization; however, we recommend using clear, descriptive names to ensure your team can easily identify the connection. Ensure that you have chosen an unique API Name and that the Distribution State is set as Local.

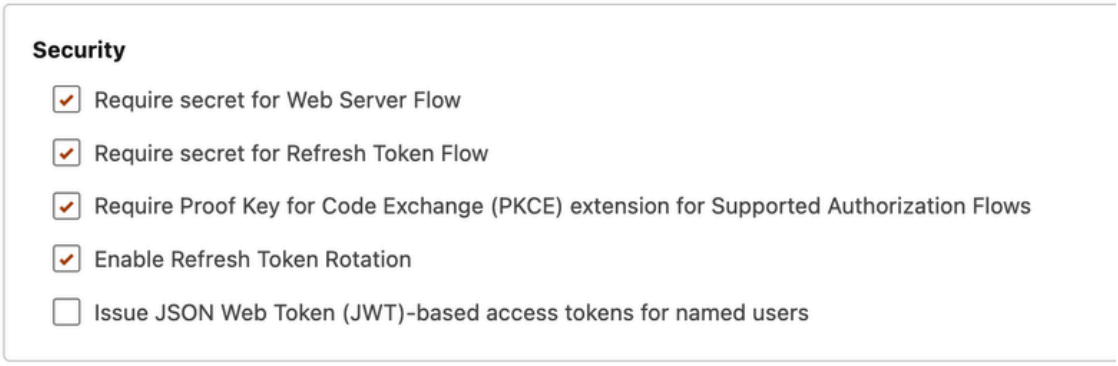
Step 3: Configure OAuth Settings

Next, you will configure the **OAuth settings** for the ECA connection. First, toggle the option to **Enable OAuth Settings**. Once active, please apply the following configurations:

- **Callback URL:** https://api.valo.ai/oauth2/v1/callback/salesforce
- **OAuth Scopes:**
  - api (Manage user data via APIs)
  - refresh_token (Perform requests at any time)
  - offline_access (Perform requests at any time)



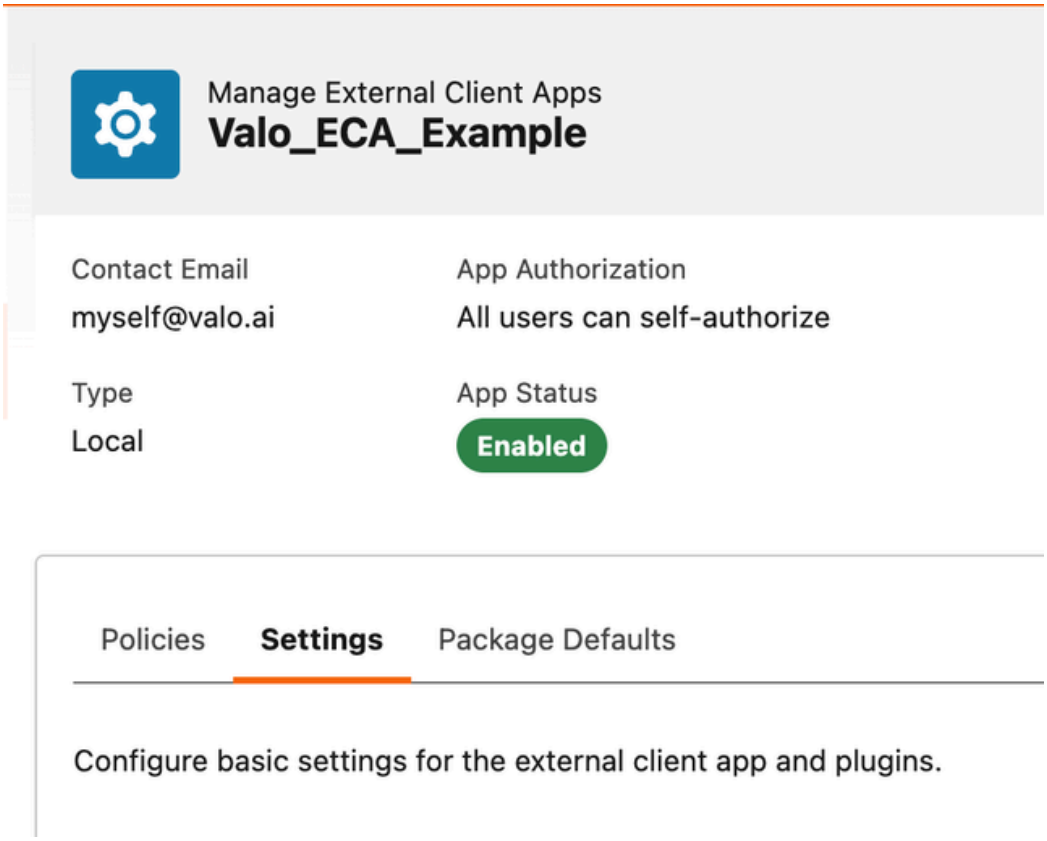
Step 4: Enhanced Security Settings



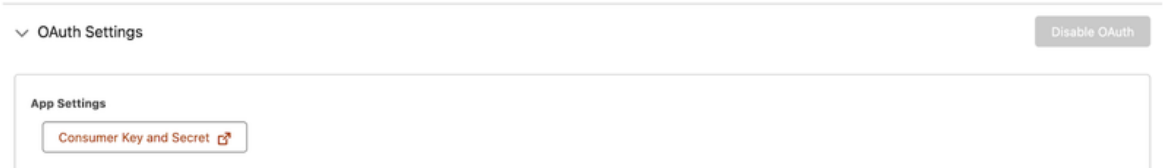
Next, ensure that the following **Security** settings are enabled to maintain a secure and functional integration:

- 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

Step 5: Finalize ECA creation and retrieve Consumer Key and Secret



Once you have finished configuring the settings, click **Create** at the bottom of the Setup UI. Salesforce will typically redirect you to the specific ECA configuration page or the **External Client App Manager**. If you find yourself in the Manager, locate your new application and select **Edit**. From there, navigate to the **Settings** tab within the ECA interface to finalize the setup.



The **OAuth Settings** section that was configured earlier now contains a link to the **Consumer Key and Secret**. This link demands authentication and forwards you to a page where the credentials are provided. They are used for connecting your previously created ECA to Valo.ai. The values can be copied to the Valo user interface when prompted accordingly.

IMPORTANT

The **Consumer Key and Secret** are both secret values that can be used to access data in your Salesforce organization. **Do not share** them anywhere under any circumstances outside of these setup instructions. **Valo personnel will not** ask you to provide them under any situation. In the case that someone **identifies themselves as Valo personnel** and asks about the secrets, please contact **support@valo.ai** and do not provide them with anything.

Step 6: Additional steps

The External Client Application also includes a **Policies** tab. This section allows for organization-specific configurations that enhance the security of your integration. Within this tab, Salesforce Administrators can define granular controls, such as restricting which users are permitted to self-authorize or applying strict IP range restrictions.

Because these policies are environment-specific, they should be managed by your local **Salesforce Administrator** to align with your company's internal security standards. You can also ask Valo personnel for guidance on setting up secure policies.