Salesforce Integration

Salesforce Configuration · https://www.easyterritory.com/documentation/territory-designer/administration/salesforce-configuration/salesforce-integration/

Overview:

As of version 3.07.x, EasyTerritory supports integration with Salesforce version 42 and up. The only authentication model EasyTerritory supports with Salesforce is OpenID Connect. The only deployment model supported is cloud for both EasyTerritory and Salesforce. You must register an instance of EasyTerritory in Salesforce in order for Salesforce to be the identity provider.

Advantages:

The advantages of leveraging Salesforce Integration with your EasyTerritory application are:

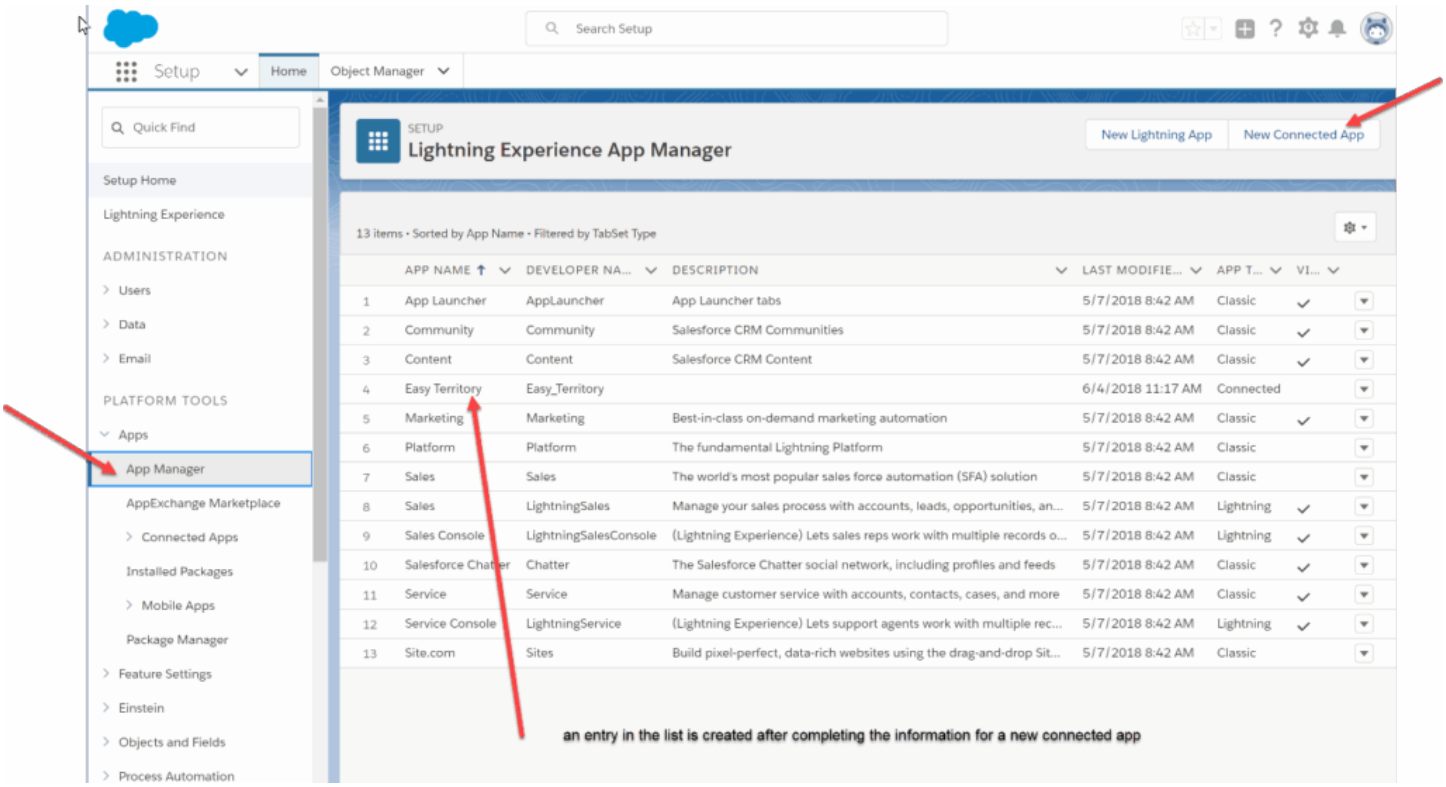
- Simple streamlined SSO access to your EasyTerritory application and Salesforce through company’s Salesforce portal.
- Strengthens security with users not needing to remember additional usernames and passwords.
- Ability for companies to control users’ access to EasyTerritory within their Active Directory.

Prerequisites:

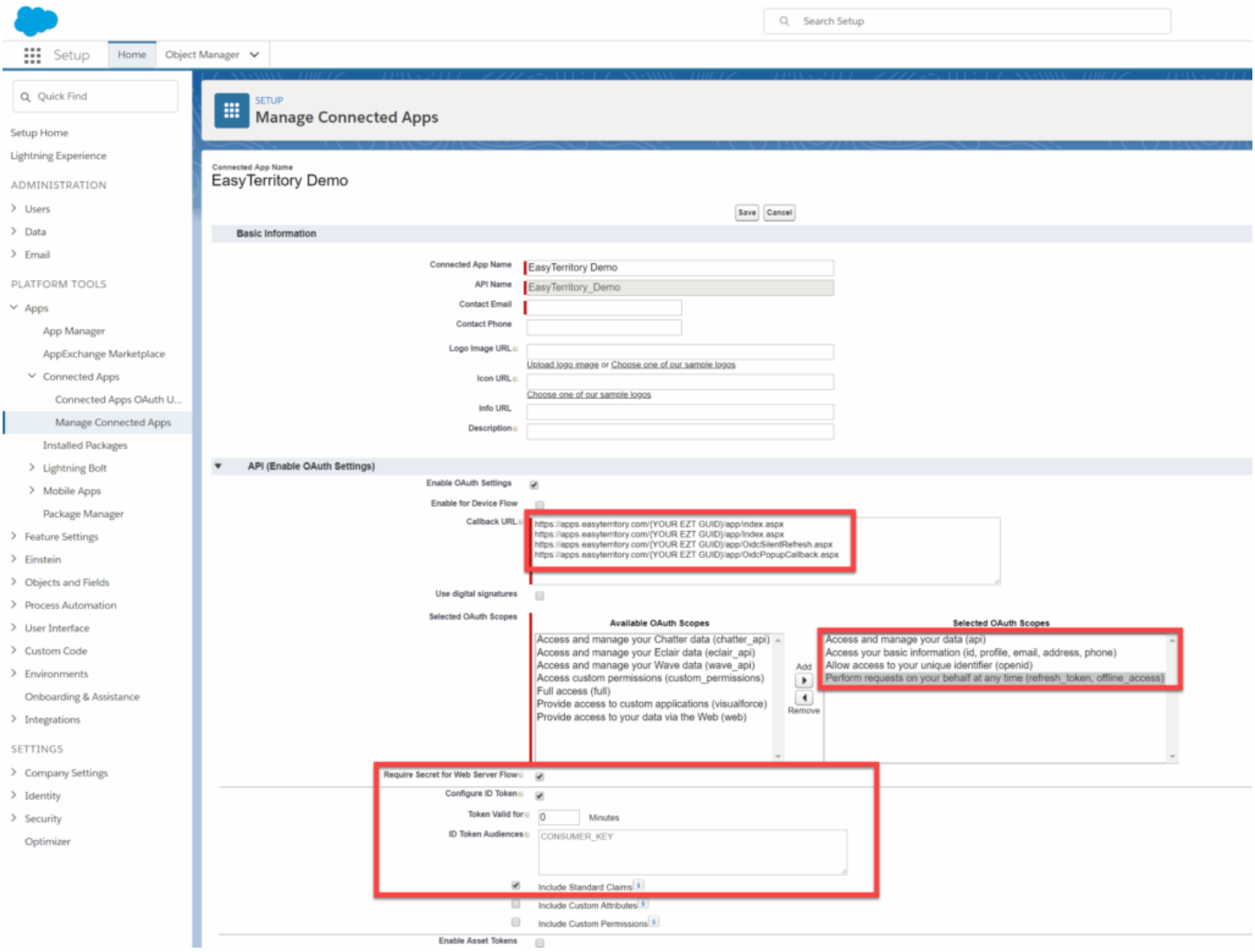
You will need to be an Salesforce admin and have access to the Salesforce setup page for your organization.

Salesforce Integration Configuration Steps:

- In your Salesforce instance, navigate to the ‘Setup Home’ page. On Sidebar navigation pane expand ‘Apps’ and select App Manager.
- In the App Manager dialogue select ‘New Connected App’ button.



Give the app and API a name. Once the app is created, edit the app to add more required information. The dropdown on the right of the list provides an edit link.



- Enter the fully-qualified callback URLs for the following pages in EasyTerritory:
  - Index.aspx (and index.aspx)
  - OidcSilentRefresh.aspx
  - OidcPopupCallback.aspx (if using a popup login)
- Also add the following Scopes:
  - Access and manage your data (api)
  - Access your basic information
  - Allow access to your unique identifier
  - Perform requests on your behalf
- Check the boxes:

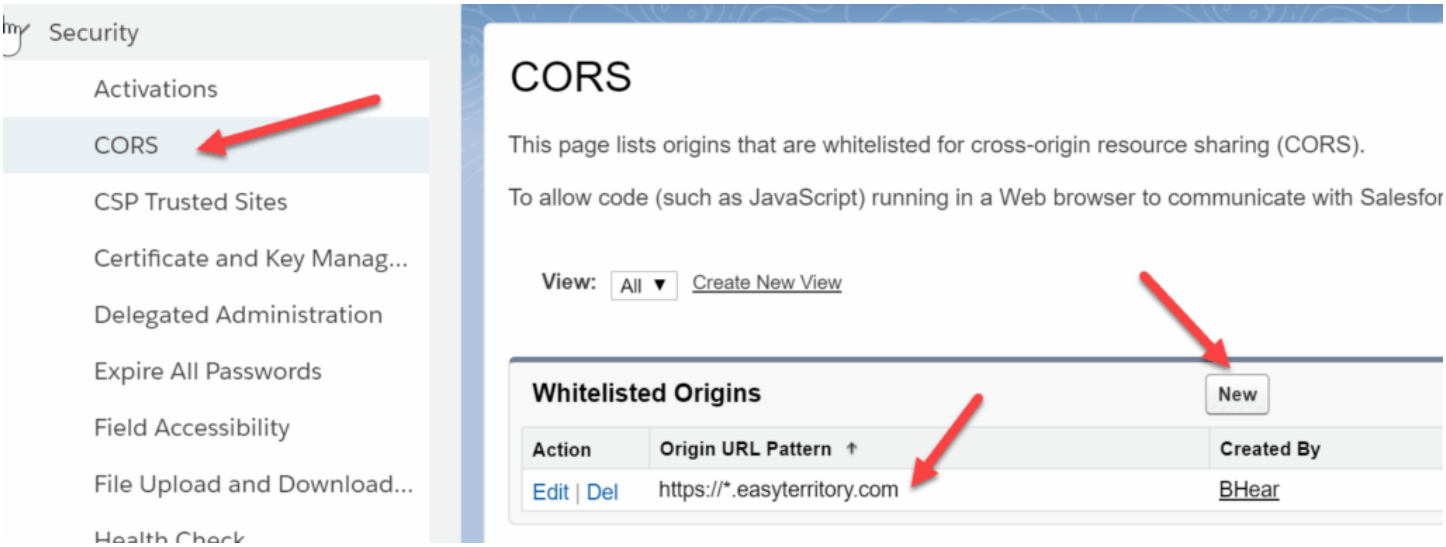
    - Require Secret for Web Server Flow
    - Configure ID Token
    - Include Standard Claims

- Enter the following values:
    - In the ‘Token Valid for’ field enter value ‘0’
    - In the ‘Token Audiences’ enter ‘CONSUMER_KEY’
    - Save and Close

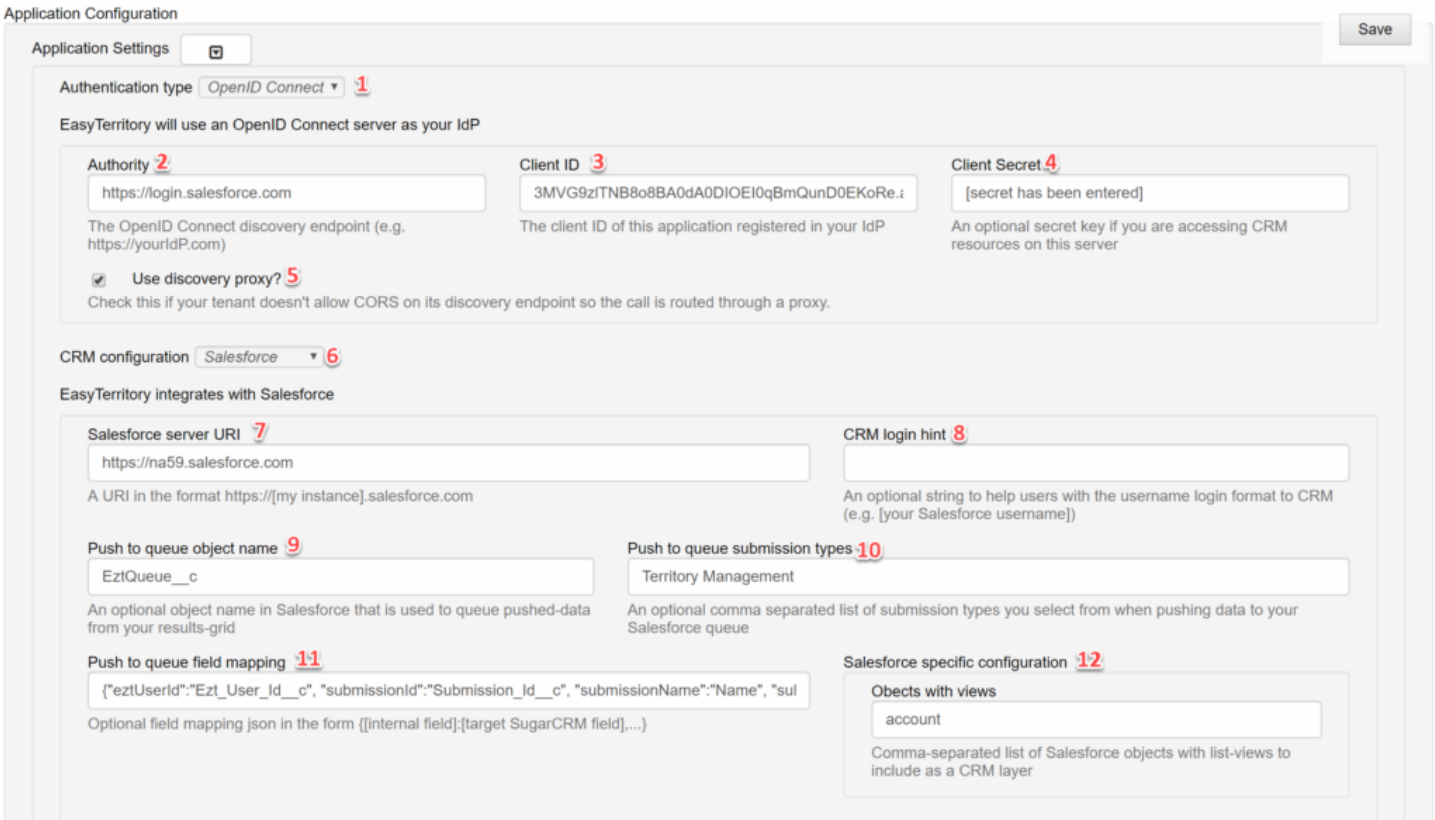
- Configure connected OAuth Usage so that users can self-authorize
- In the ‘setup home’ page navigate to Apps > Connected Apps > Manage Connected Apps. Click ‘edit’ next to the name of your App.



- In the ‘Permitted Users’ dropdown select ‘All users may self-authorize’.
- And in the ‘Refresh Token Policy’ select the ‘Expire refresh token if not used for 1 Day(s)’ radio button.
- Add Whitelisted Origin for the EasyTerritory.com domain.
- In the Salesforce setup navigate to Security > CORS
- Click ‘New’.
- Add Whitelisted Origin for the EasyTerritory domain:
    - Value: https://apps.www.easyterritory.com or https://*.www.easyterritory.com



- Configure Salesforce as Identity Provider in EasyTerritory.
- Notify an EasyTerritory administrator that you would like your Salesforce URL as a permitted origin in your EasyTerritory instance.
- Login to EasyTerritory with an admin user and click the ‘admin‘ link on the top right corner of the application.
- In ‘Application Settings’ configure the following fields:



- **Authentication type:** The only Authentication type supported with Salesforce is OpenID Connect.
  - **Authority:** This will always be https://login.salesforce.com.
  - **Client ID:** This obtained from the Consumer Key in the Connected Apps management area.
  - **Client Secret:** This is obtained from the Consumer Secret in the Connected Apps management area.
  - **Use Discovery proxy?:** This is checked for Salesforce so that all OpenID Connects calls are routed through the EasyTerritory Server avoiding and CORS conflicts.
  - **CRM configuration:** This will always be set to *Salesforce.*
  - **Salesforce server URI:** This is your cloud hosted salesforce instance.
  - **CRM login hint:** This is for future expansion for supporting Salesforce without it being an IdP (currently unused).
  - **Push to queue object name:** This is an optional object schema name of the EZT queue in Salesforce to receive pushed data.
  - **Push to queue submission types:** This is an optional comma-delimited list of submission types.
  - **Push to queue field mapping:** This is the optional JSON field mapping between internal EasyTerritory fields and Salesforce fields in your EZT queue:
  - {"eztUserId":"Ezt_User_Id__c", "submissionId":"Submission_Id__c", "submissionName":"Name", "submissionType": "Submission_Type__c", "submissionInfo":"Submission_Info__c", "assignedDate":"Assigned_Date__c", "markupTagValue":"Markup_Tag_Value__c", "relatedCrmEntityName":"Related_Crm_Object_Name__c", "relatedCrmEntityId": "Related_CRM_Object_Id__c"}
  - **Salesforce specific configuration:** This is a comma-delimited list of Salesforce objects to look for list-views for creating CRM layers in EasyTerritory. These views must have some kind of location information such as an address or latitude and longitude.
- Browse to your EasyTerritory instance URL you will be redirected to your Salesforce Idp login page and after entering in your Salesforce credentials you will be prompted to allow EasyTerritory to access you Salesforce user information.



Allow Access?

EasyTerritory is asking to:

- Access your basic information
- Allow access to your unique identifier
- Access and manage your data

Do you want to allow access for benton@easyterritory.com? (Not you?)

Deny | Allow

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

Click allow and you will be logged in to your EasyTerritory instance.