Indiana Office of Technology (IOT)

Access Indiana / Salesforce OpenID Connect Setup

Solution Documentation

Last Updated: January 30, 2023

Version: 2

Table of Contents

Background 2

Core Workgroup 2

How to Use This Document 2

Target Audience 2

Overall Process Steps 3

Install Access Indiana custom Auth. Provider in your Salesforce org 3

Initial configuration of Access Indiana custom Auth. Provider in your Salesforce org 6

Register an application with Access 13

Final Configuration 15

Set up a User 20

Test Your App 22

Sandbox Creation/Refresh Configuration 24

Background

The Indiana Office of Technology and Indiana Interactive, has been tasked with implementing a single sign-on authentication mechanism and Identity Provider for public online applications for the State of Indiana, referred to as Access Indiana. This project delivers a best practice solution for State Salesforce system administrators to configure an OpenID Connect (OIDC) authentication to work with Access Indiana.

Core Workgroup

The core workgroup consisted of members of the Indiana Office of Technology.

Name	Role / Capacity
Alvin Wilson	Deputy Chief Administrative Officer
Yancy Hollonquest	Project Owner
Bob Braun, CRM Architect	Salesforce Configurator @ Relevant Technologies
Casey Boyd, CRM Architect/Developer	Salesforce Developer @ Relevant Technologies
Sloane Wright	General Manager @ Access Indiana

How to Use This Document

This document is designed to be a roadmap for helping Application Development move toward the vision expressed by project stakeholders. It provides a description of the functional requirements for the changes being requested.

Target Audience

This document is intended to assist Certified Salesforce Administrators and Developers in establishing OpenID Connect authentication with Access Indiana.

Useful links:

Access Indiana	https://www.in.gov/inwp/2678.htm
OpenID Connect Hybrid Flow	https://openid.net/specs/openid-connect-core1_0.html#HybridFlowAuth
Access Indiana well-known endpoints	https://accessintegrate.in.gov/.well-known/openidconfiguration

Access Indiana Client Set-Up Request (online form)	https://app.smartsheet.com/b/form/472a5b71e31f455ebf14b39d9858f77b
Salesforce well-known endpoints	https://na112.salesforce.com/.well-known/openidconfiguration
OpenID well-known endpoints	https://<my-domain>.my.salesforce.com/.wellknown/openid-configuration

Project Execution Steps

1. Install Access Indiana custom Auth. Provider in your Salesforce org
2. Initial configuration of Access Indiana custom Auth. Provider in your Salesforce org
3. Register an application with Access
4. Complete configuration of Access Indiana custom Auth. Provider in your Salesforce org
5. Set up Users
6. Test your app

Install Access Indiana custom Auth. Provider in your Salesforce org

- An authentication provider allows users to log in to their Salesforce org using their login credentials from an external service provider. Salesforce provides authentication providers for apps that support the OpenID Connect protocol, such as Google, Facebook, Twitter, and LinkedIn. For apps that do not support OpenID Connect, Salesforce provides an Apex Auth.AuthProviderPluginClass abstract class to create a custom authentication provider.

- In this case, external service provider is Access Indiana. It is important that while Salesforce support the OpenID Connect protocol, at the time of this writing it does not support the Hybrid Flow (https://success.salesforce.com/ideaView?id=0873A000000TtnAQAS). Access Indiana Custom Auth. Provider leverages the Auth.AuthProviderPluginClass, thus we are able use the OpenID Connect Hybrid Flow as required by Access Indiana.

- Log into your Salesforce Organization, location to install the Access Indiana Custom Auth Provider. Salesforce org should have a "My Domain" subdomain. For help setting up a "My Domain" subdomain, please refer to this link: https://help.salesforce.com/articleView?id=domain_name_overview.htm&type=5.

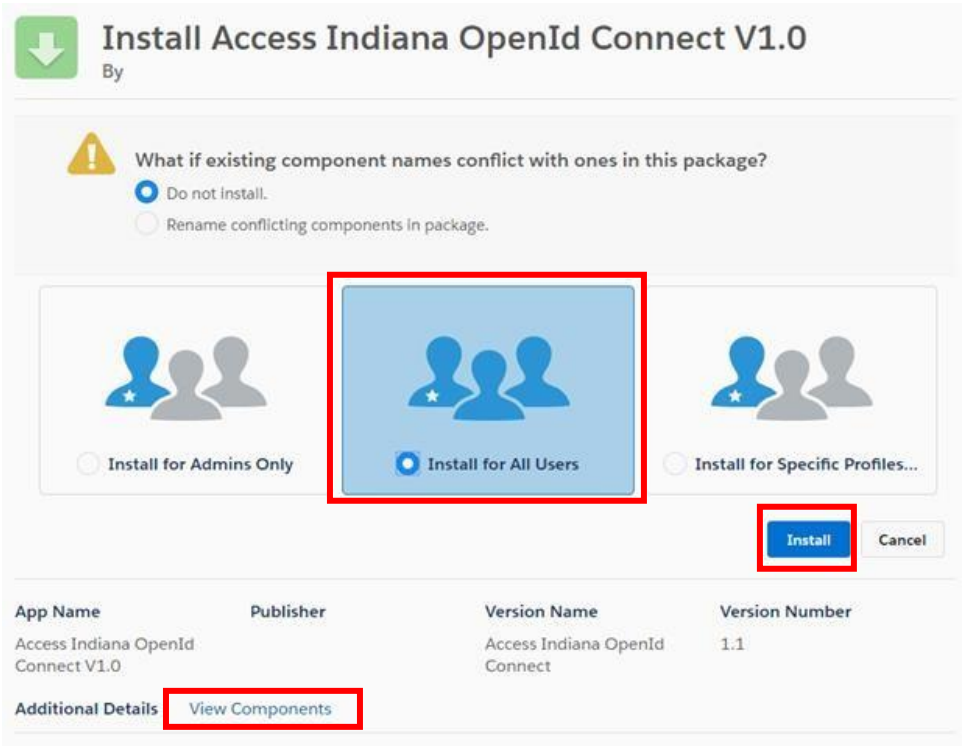
- With My Domain, you create a subdomain within the salesforce.com domain. For example, trailhead is a subdomain of the Salesforce domain: trailhead.salesforce.com. With a subdomain, you replace the instance URL that Salesforce assigned you, like

https://na30.salesforce.com, with your chosen domain name, such as https://somethingcool.my.salesforce.com.

- Access Indiana Custom Auth. Provider is delivered as a Salesforce unmanaged package. The package URL for this solution is: https://test.salesforce.com/packaging/installPackage.apexp?p0=04t350000001Eob

- After logging in to your Salesforce org, append "/packaging/installPackage.apexp?p0=04t350000001Eob" (no quotes) to your "My Domain" Salesforce URL. So, if your "My Domain" for your org is "ingovtech", you would install the unmanaged package using this URL: https://ingovtech.my.salesforce.com//packaging/installPackage.apexp?p0=04t350000001Eob

- If you have not logged in, you will be redirected to do so. Once authenticated, select the "Install for All Users" button and then click the "Install" button. From here, you can also view the solution components by clicking the "View Components" link:



- This is a working solution. However, there are many ways an Agency may want to use this solution. Therefore, because this is an unmanaged package, you have access to customize this solution as you see fit.

Package Components

Objects (1)

Action	Component Name	Parent Object	Component Type	Installation Notes
Create	Access Indiana Setting		Custom Metadata Type	This is a brand new component.

Code (4)

Action	Component Name	Parent Object	Component Type	Installation Notes
Create	AccessIndianaAuthProviderTest		Apex Class	This is a brand new component.
Create	AccessIndianaAuthProvider		Apex Class	This is a brand new component.
Create	AccessIndianaRegHandlerTest		Apex Class	This is a brand new component.
Create	AccessIndianaRegHandler		Apex Class	This is a brand new component.

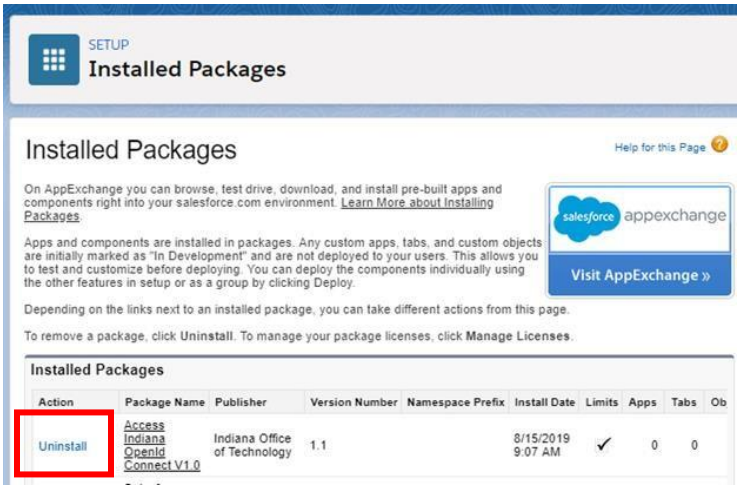
Fields (9)

Action	Component Name	Parent Object	Component Type	Installation Notes
Create	Authorization Endpoint	Access_Indiana_Setting__mdt	Custom Field	This is a brand new component.
Create	Access Indiana Email	User	Custom Field	This is a brand new component.
Create	Redirect URI	Access_Indiana_Setting__mdt	Custom Field	This is a brand new component.
Create	Token Endpoint	Access_Indiana_Setting__mdt	Custom Field	This is a brand new component.
Create	Access Indiana Subject	User	Custom Field	This is a brand new component.
Create	Client Id	Access_Indiana_Setting__mdt	Custom Field	This is a brand new component.
Create	User Info Endpoint	Access_Indiana_Setting__mdt	Custom Field	This is a brand new component.
Create	Scope	Access_Indiana_Setting__mdt	Custom Field	This is a brand new component.
Create	Client Secret	Access_Indiana_Setting__mdt	Custom Field	This is a brand new component.

Resources (1)

Action	Component Name	Parent Object	Component Type	Installation Notes
Create	Access Indiana Setting Layout	Access_Indiana_Setting__mdt	Page Layout	This is a brand new component.

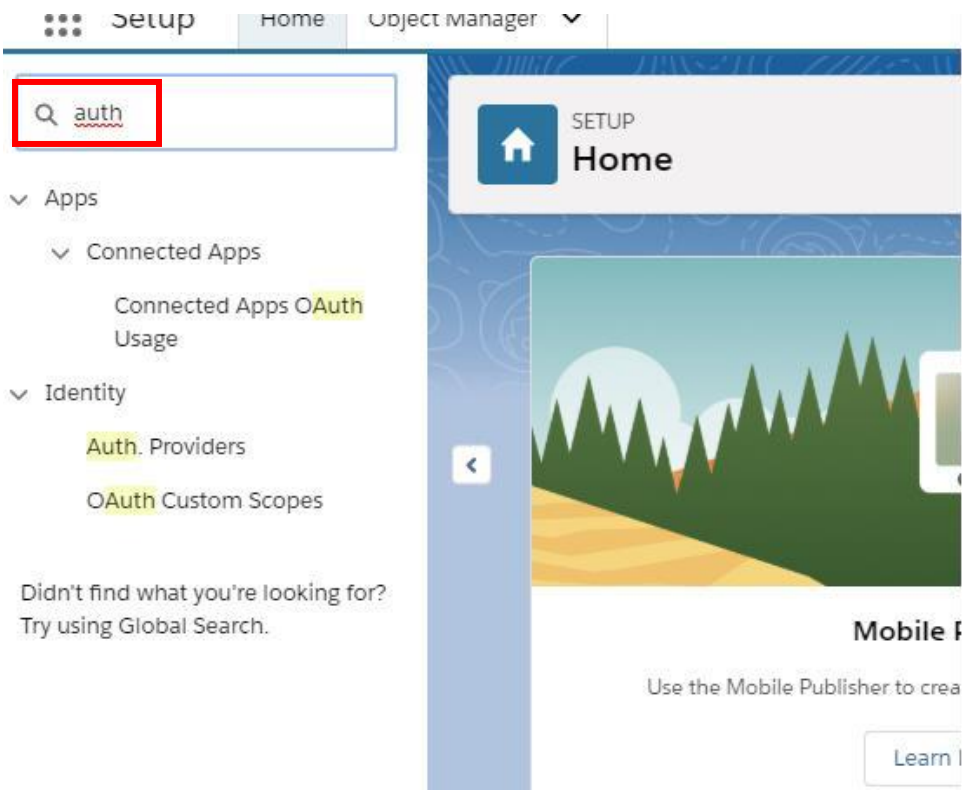
- If you ever want to uninstall this package, you would click the “Uninstall” link to do so.



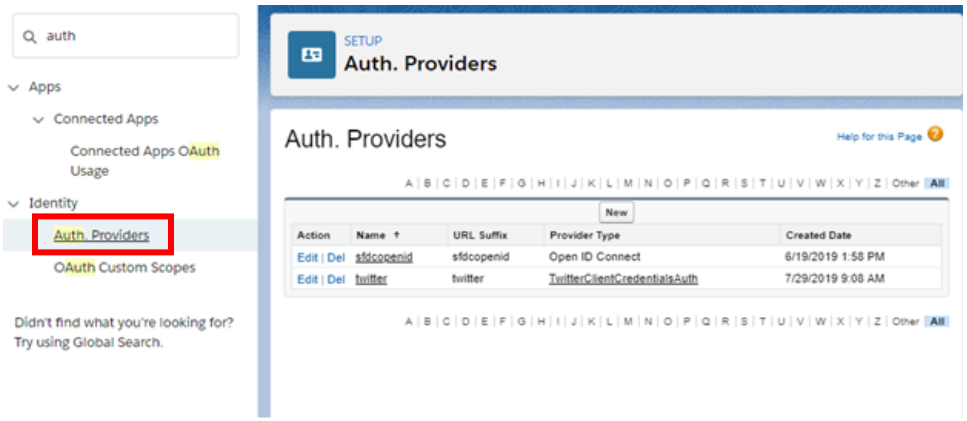
At this point, installation is complete.

Initial configuration of Access Indiana custom Auth. Provider in your Salesforce org

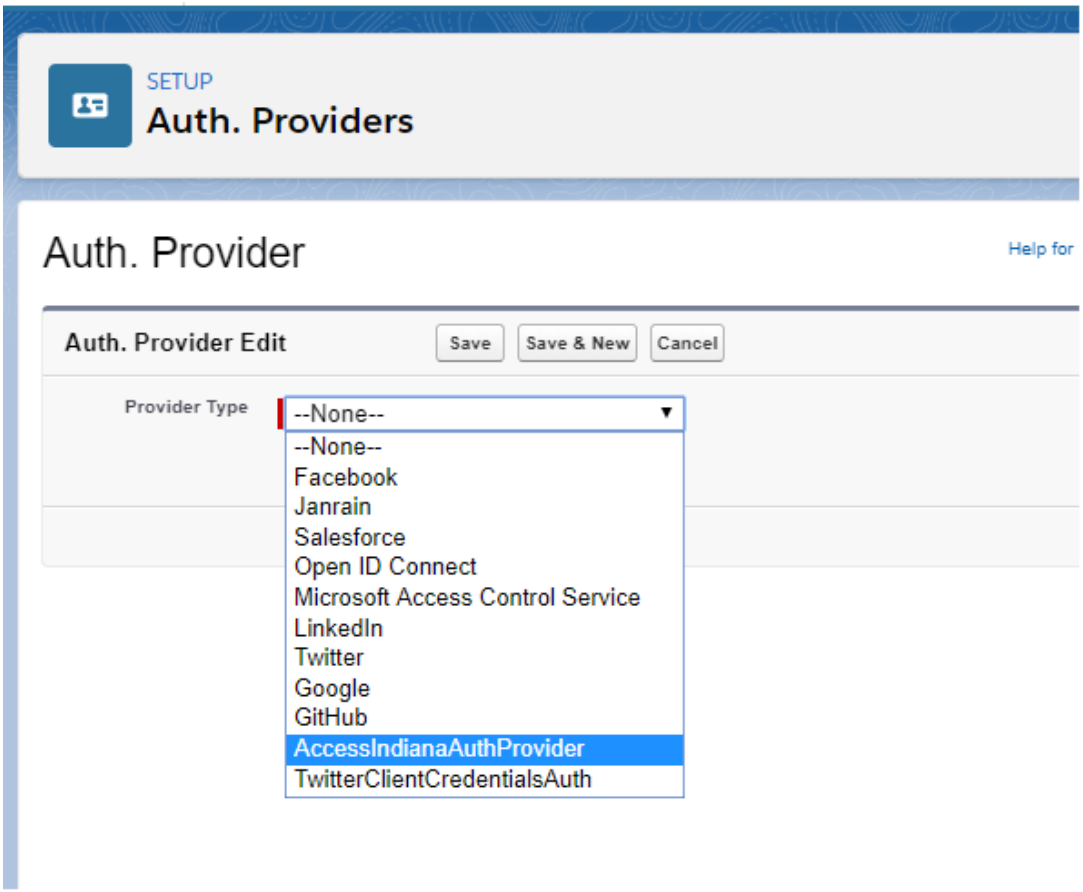
- In Setup, navigate to the Auth. Providers SETUP page by typing “auth” in the Setup “Quick Find” search field.



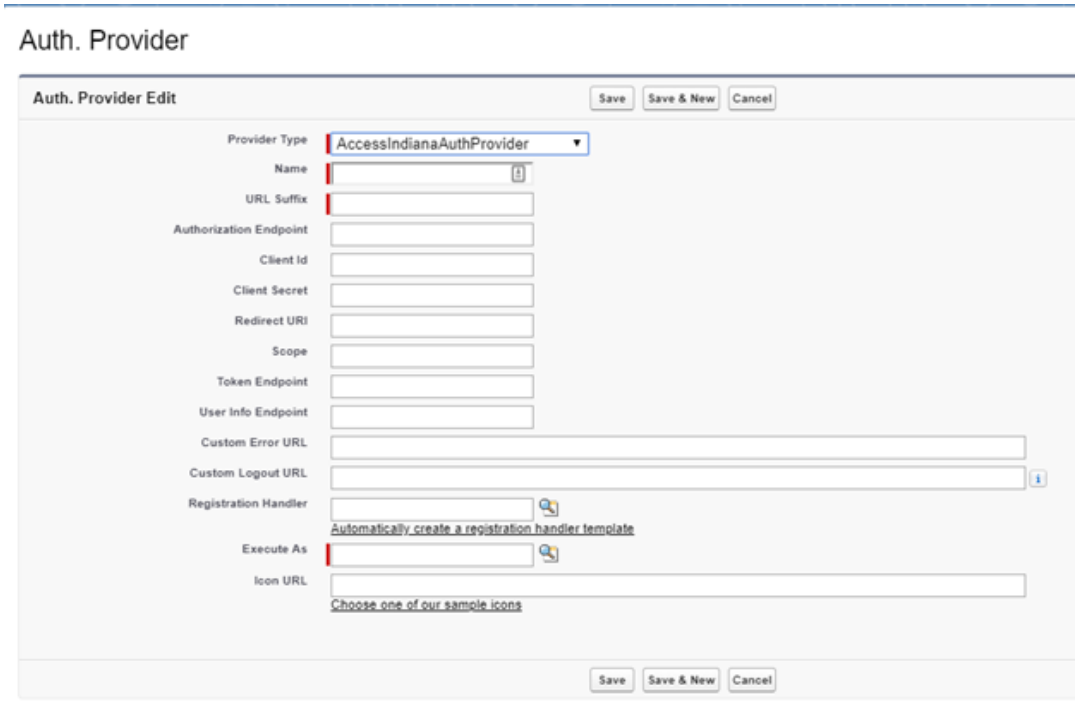
- Click to select Auth Providers.



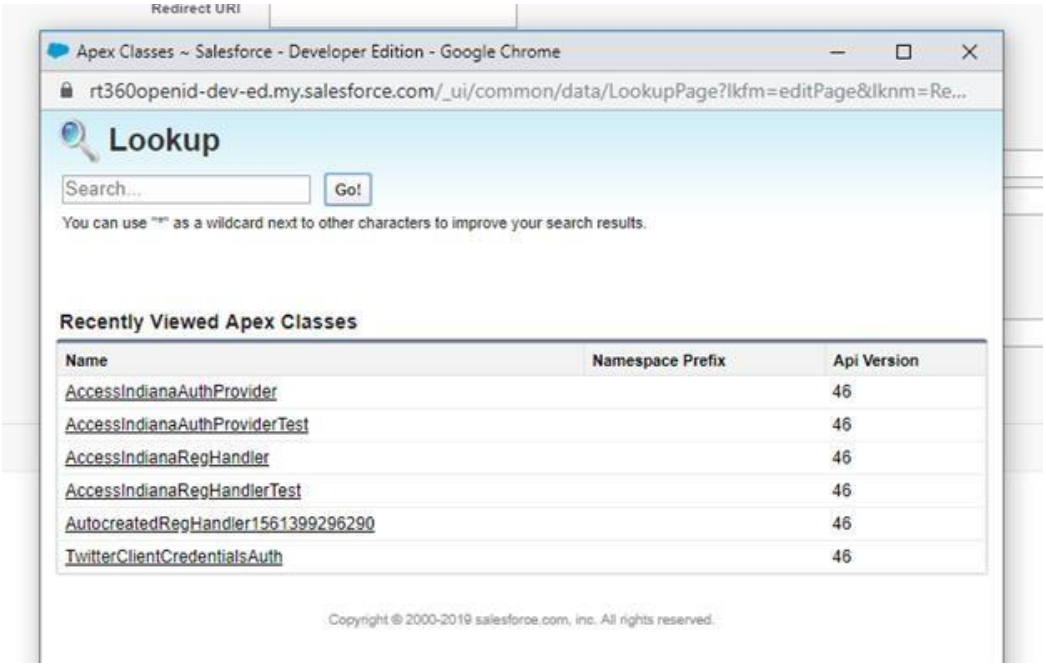
- Click the “New” button and select the “AccessIndianaAuthProvider” from the Provider Type picklist.

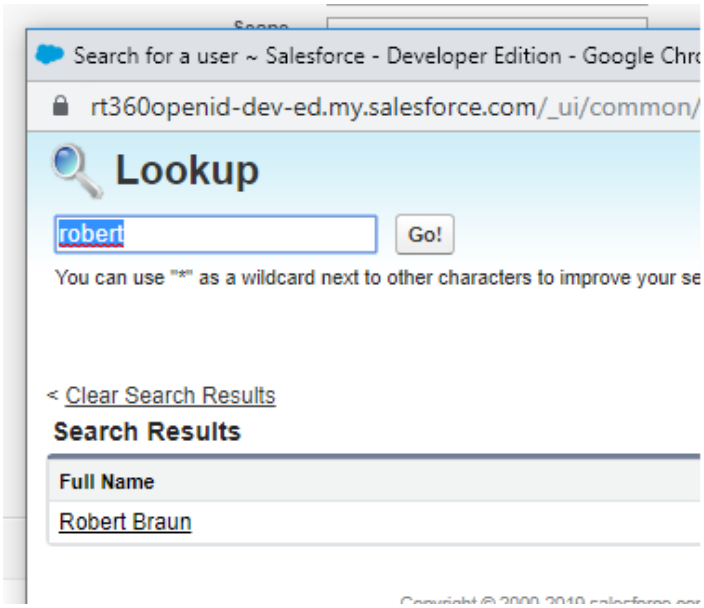


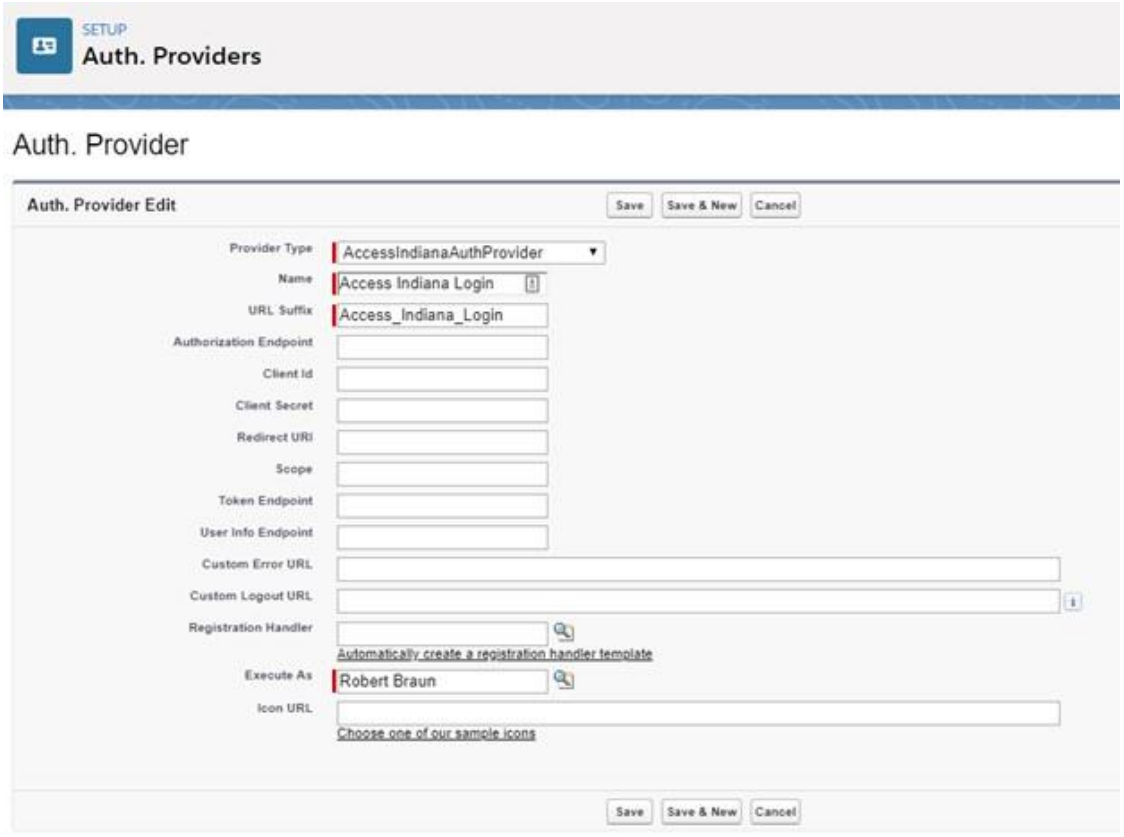
- You will then be presented with the following page:

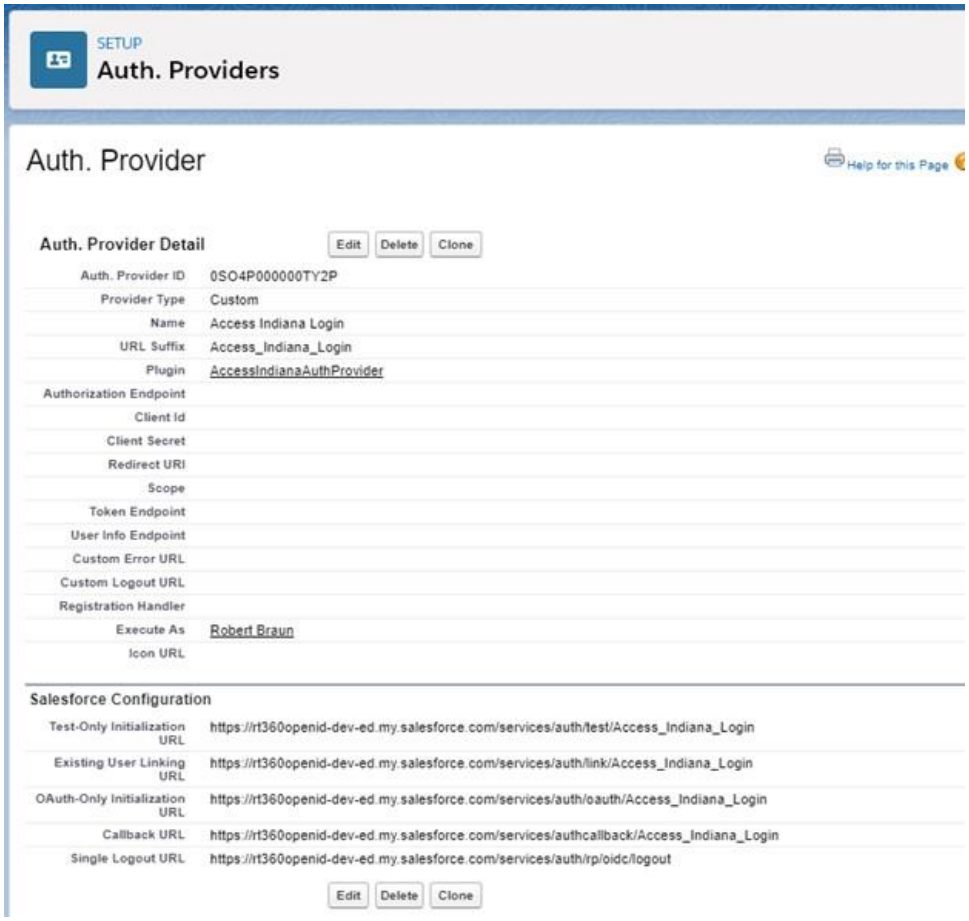


- Type in the “Name”, “URL Suffix”, select a “Registration Handler”, select an “Execute As” User that will be used as the running user for this authentication.




Search for a user ~ Salesforce - Developer Edition - Google Chr
rt360openid-dev-ed.my.salesforce.com/_ui/common/
Lookup
robert
Go!
You can use "*" as a wildcard next to other characters to improve your se
< Clear Search Results
Search Results
Full Name
Robert Braun

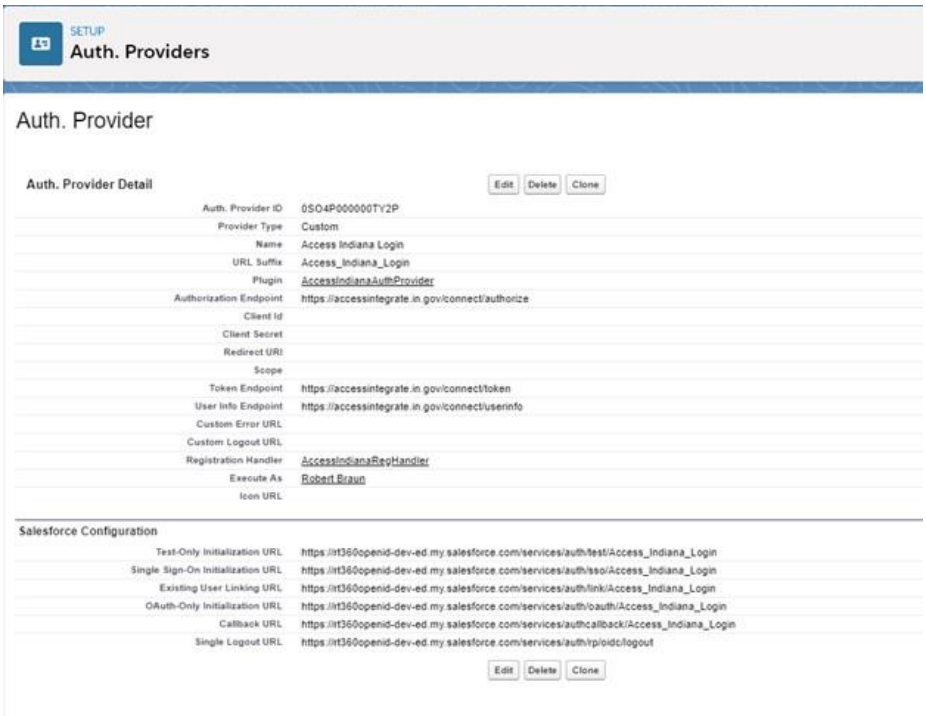

SETUP
Auth. Providers
Auth. Provider
Auth. Provider Edit
Save
Save & New
Cancel
Provider Type
AccessIndianaAuthProvider
Name
Access Indiana Login
URL Suffix
Access_Indiana_Login
Authorization Endpoint
Client Id
Client Secret
Redirect URI
Scope
Token Endpoint
User Info Endpoint
Custom Error URL
Custom Logout URL
Registration Handler
Automatically create a registration handler template
Execute As
Robert Braun
Icon URL
Choose one of our sample icons
Save
Save & New
Cancel



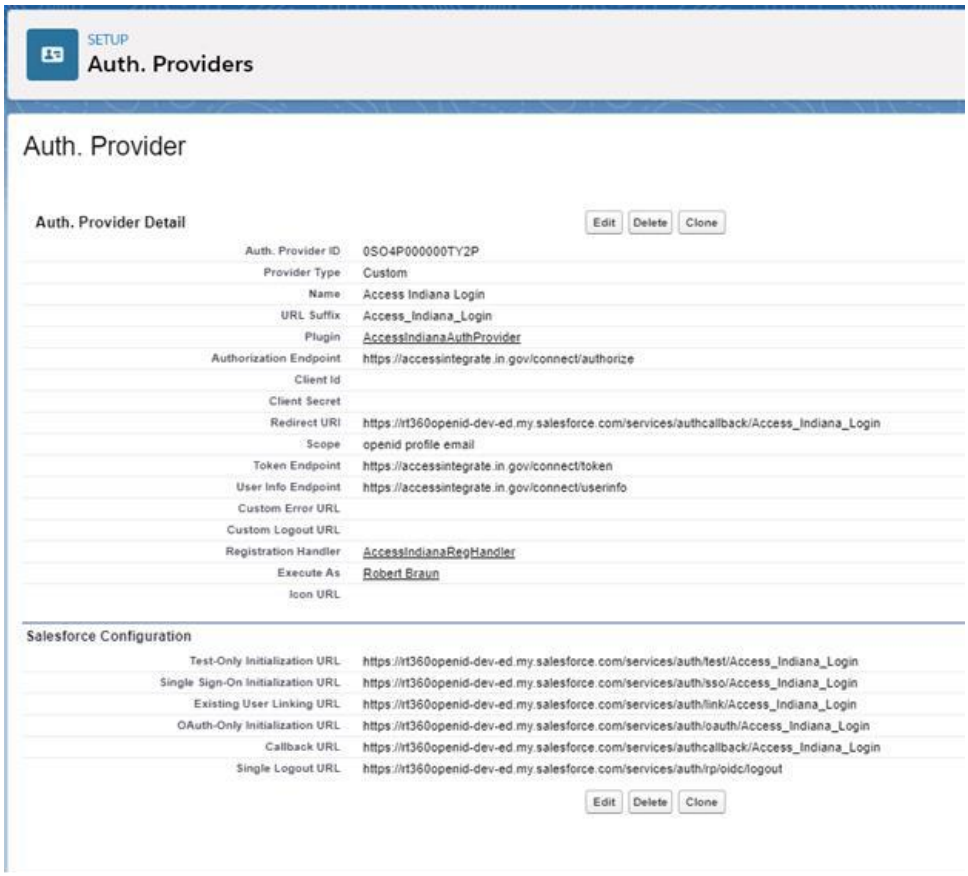
- In a browser, enter the following URL to see the Access Indiana well-known endpoints: https://accessintegrate.in.gov/.well-known/openid-configuration. Notice the URLs for the "authorization_endpoint", "token_endpoint", and "userinfo_endpoint".

```
{
  "issuer": "https://accessintegrate.in.gov",
  "jwks_uri": "https://accessintegrate.in.gov/.well-known/openid-configuration/jwks",
  "authorization_endpoint": "https://accessintegrate.in.gov/connect/authorize",
  "token_endpoint": "https://accessintegrate.in.gov/connect/token",
  "userinfo_endpoint": "https://accessintegrate.in.gov/connect/userinfo",
  "end_session_endpoint": "https://accessintegrate.in.gov/connect/endsession",
  "check_session_iframe": "https://accessintegrate.in.gov/connect/checksession",
  "revocation_endpoint": "https://accessintegrate.in.gov/connect/revocation",
  "introspection_endpoint": "https://accessintegrate.in.gov/connect/introspect",
  "device_authorization_endpoint": "https://accessintegrate.in.gov/connect/deviceauthorization",
  "frontchannel_logout_supported": true,
  "frontchannel_logout_session_supported": true,
  "backchannel_logout_supported": true,
  "backchannel_logout_session_supported": true,
  "scopes_supported": [
    "openid",
    "profile",
    "email",
    "offline_access"
  ],
  "claims_supported": [
    "sub",
    "name",
    "family_name",
    "given_name",
    "middle_name",
    "updated_at",
    "email",
    "email_verified",
    "email_updated_at"
```


- Copy each of the URLs for the endpoints listed above and paste into the “Authorization Endpoint, “Token Endpoint”, and “User Info Endpoint” fields, respectively. Your Auth. Provider should now look like below:



-
- Edit the Auth. Provider page again and enter “openid profile email” in the Scope field. Copy the Callback URL from the Salesforce Configuration section and copy it to the “Redirect URI” field. Your Auth. Provider should now look like this:



Register an application with Access

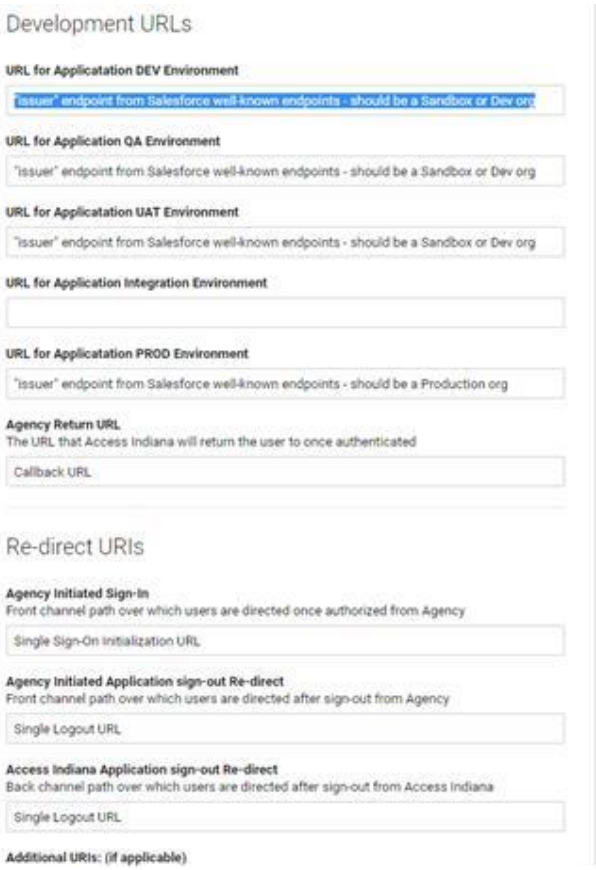
- To register your client application with Access Indiana, submit the online form located: https://app.smartsheet.com/b/form/472a5b71e31f455ebf14b39d9858f77b

- Complete the Agency information in the top part of the form. The Salesforce URL information can be found either in the Auth. Provider you just created, or in the Salesforce well-known endpoints.

- Provide the requested URLs so Access Indiana can create an application (tile) in Access Indiana that will collaborate with your Auth. Provider. Once this is set up, you will receive notice from Access Indiana along with a unique client id and client secret.

-
- Bring up a browser and navigate to your Salesforce org's well-known endpoints.
- Here is an example segment for the ingovtech openid Sandbox well-known endpoints: https://ingovtech--openid.cs33.my.salesforce.com/.well-known/openid-configuration)


```
{
  "end_session_endpoint": "https://ingovtech--OpenId.cs33.my.salesforce.com/services/auth/idp/oidc/logout",
  "frontchannel_logout_supported": true,
  "frontchannel_logout_session_supported": false,
  "issuer": "https://ingovtech--OpenId.cs33.my.salesforce.com",
  "authorization_endpoint": "https://ingovtech--OpenId.cs33.my.salesforce.com/services/oauth2/authorize",
  "token_endpoint": "https://ingovtech--OpenId.cs33.my.salesforce.com/services/oauth2/token",
  "revocation_endpoint": "https://ingovtech--OpenId.cs33.my.salesforce.com/services/oauth2/revoke",
  "userinfo_endpoint": "https://ingovtech--OpenId.cs33.my.salesforce.com/services/oauth2/userinfo",
  "jwks_uri": "https://ingovtech--OpenId.cs33.my.salesforce.com/id/keys",
  "registration_endpoint": "https://ingovtech--OpenId.cs33.my.salesforce.com/services/oauth2/register",
  "introspection_endpoint": "https://ingovtech--OpenId.cs33.my.salesforce.com/services/oauth2/introspect",
  "scopes_supported": [
    "visualforce"
```

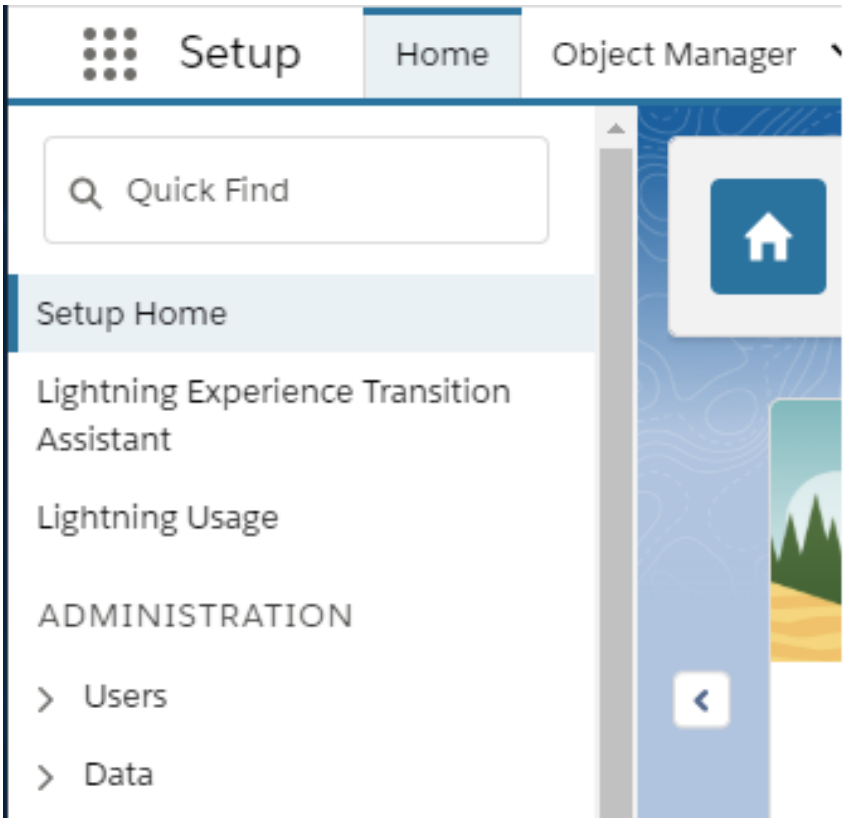
- Notice the "issuer" URL above. This is the URL for either the DEV, QA, UAT, or Integration environments. A Production org will not contain the Sandbox name in the "issuer" URL.
- The remaining URLs can be found in the Auth. Provider configuration you are setting up.
- For the "Agency Return URL" enter the "Callback URL", e.g.: https://rt360openid-deved.my.salesforce.com/services/authcallback/Access_Indiana_Login

-
- For the “Agency Initiated Sign-In” Re-Direct URL, enter the “Single Sign-On Initialization URL”, e.g.: https://rt360openid-dev-ed.my.salesforce.com/services/auth/sso/Access_Indiana_Login
- For the “Agency Initiated Application sign-out Re-direct and “Access Indiana Application sign-out Re-direct” Re-direct URLs, enter the “Single Logout URL”, e.g.: https://rt360openid-dev-ed.my.salesforce.com/services/auth/rp/oidc/logout

Submit the form and wait for your acknowledgement and client id and client secret.

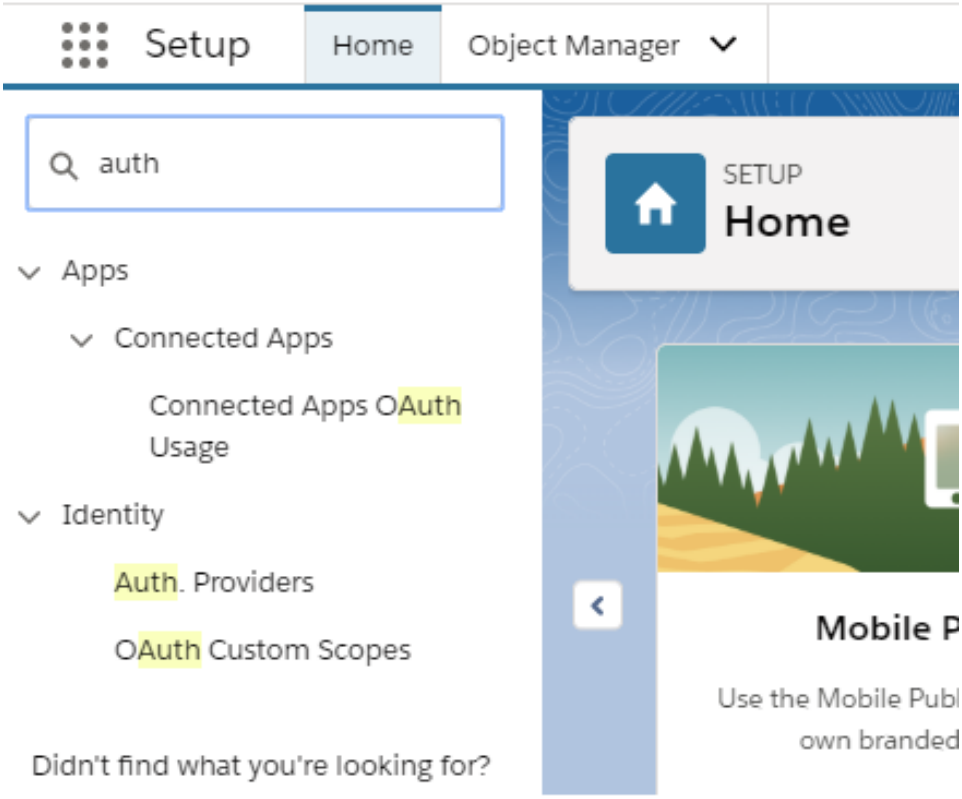
Final Configuration

- Once you receive your client id and client secret from Access Indiana, you will need to update your Auth. Provider configuration in your Salesforce org.
- Log into your Salesforce org and go to Setup.

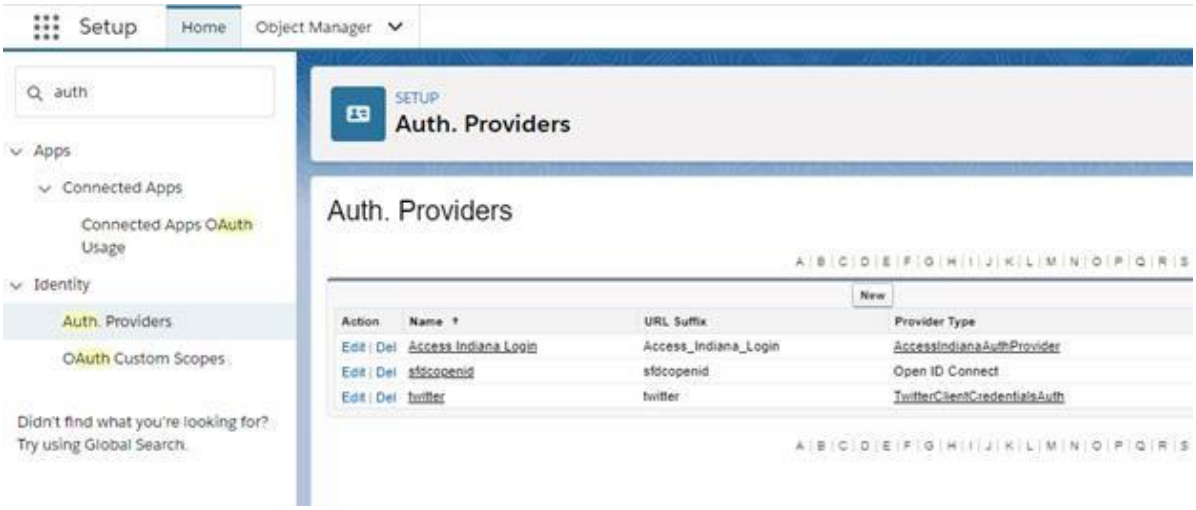


-

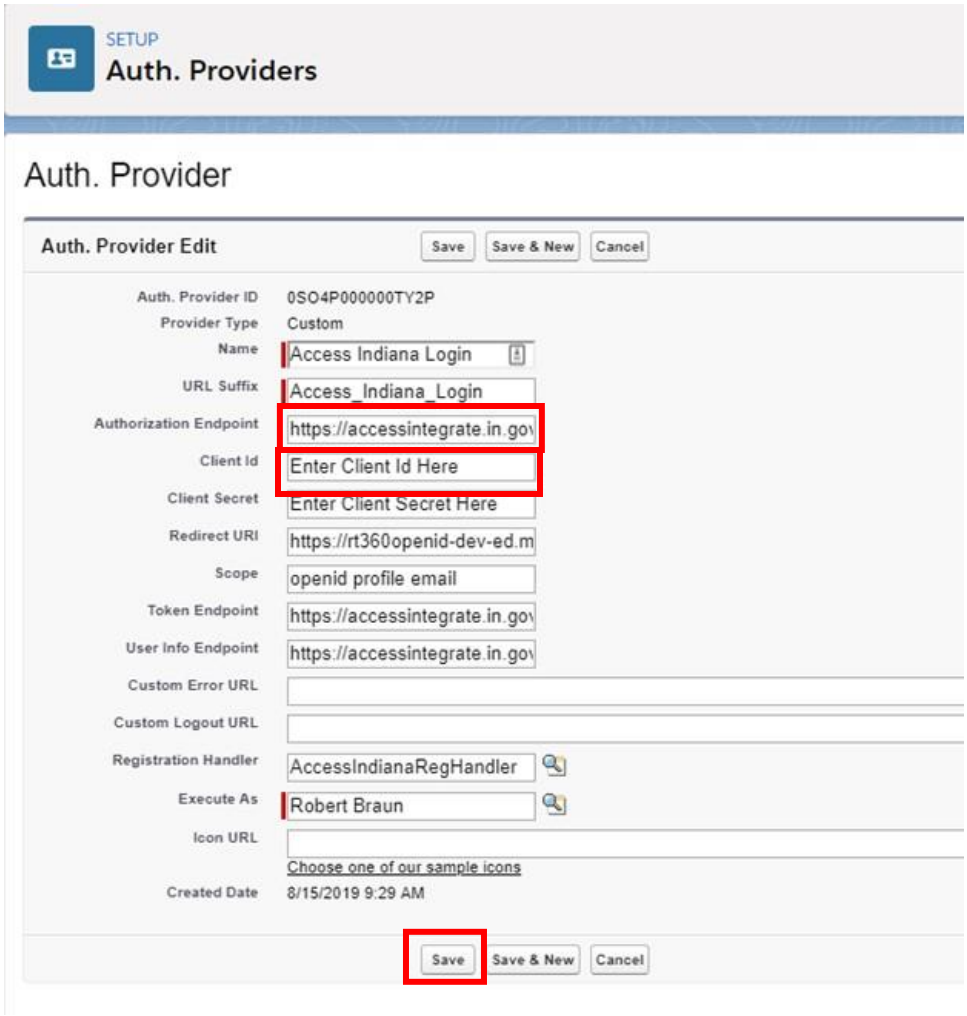
In the Quick Find search field, type “auth” and click the Auth. Providers link.



- You should now be at the SETUP Auth. Providers home page.

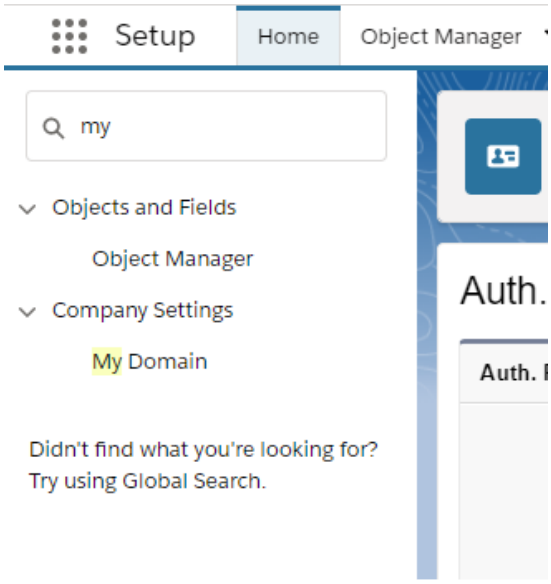


Edit your Auth. Provider to add the Client Id and Client Secret. Enter the Client Id and Client Secret values you received from Access Indiana into the Client Id and Client Secret fields, respectively. Save your configuration by clicking the Save button at the bottom of the page.

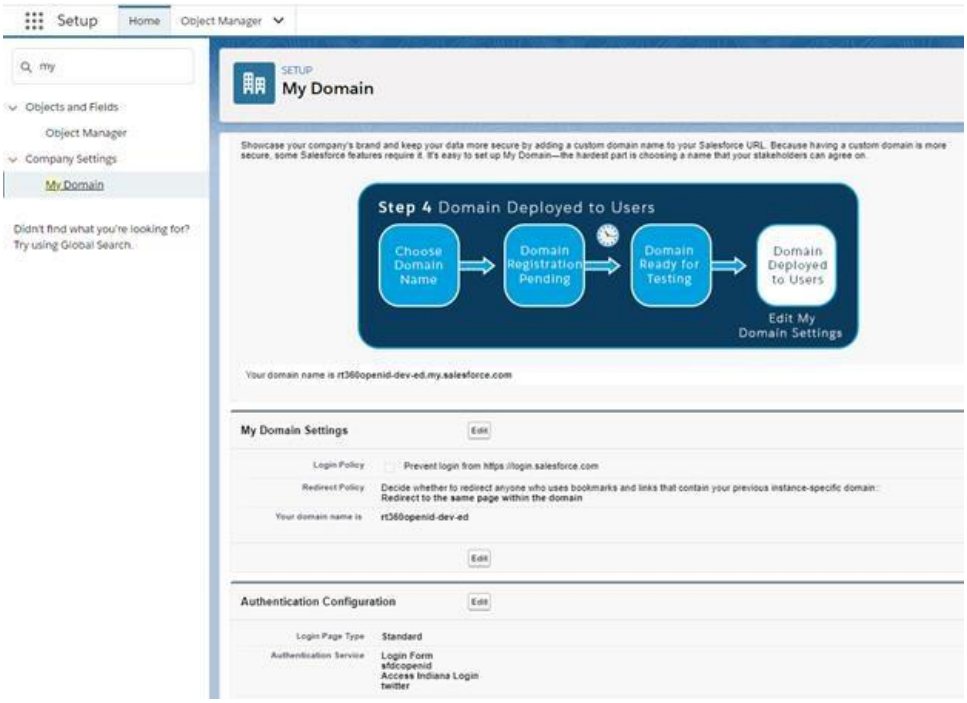


- At this point, your Access Indiana custom Auth. Provider is fully configured. Now, we need to make sure Users can access this authentication. To do this, we add the Auth. Provider you just created to the sign-in page as a button.

Type “my” in the Setup Quick Find field and select the “My Domain” link.

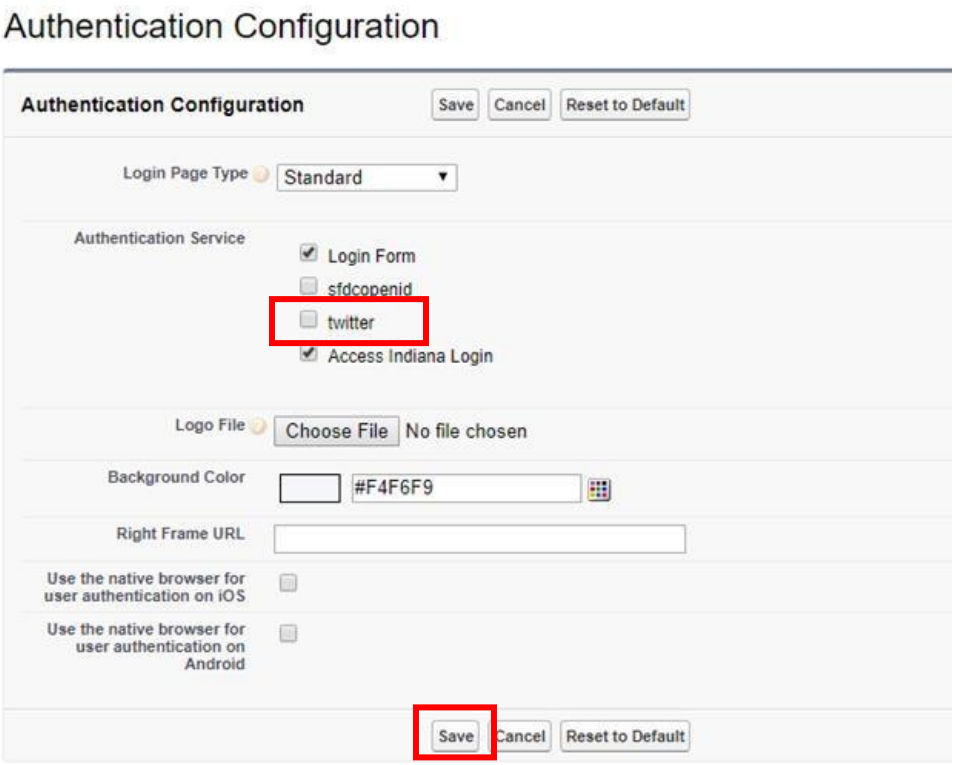


- This navigates you to the My Domain SETUP home page.



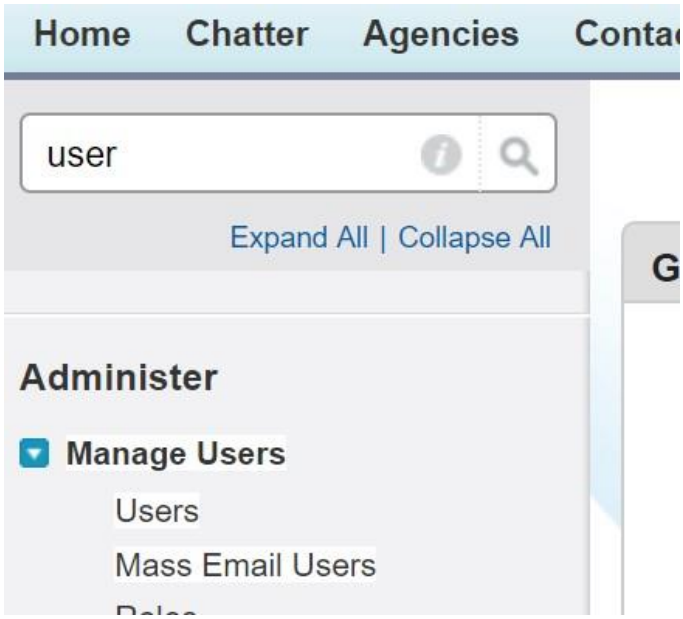
- Notice the “Authentication Configuration” section. Click the Edit button for this section. You will see an Authentication Service for the “Access Indiana Login” Auth. Provider you just created. Check the checkbox next to it to add that button to the login page.

- Click the Save button at the bottom of the page to save this configuration.

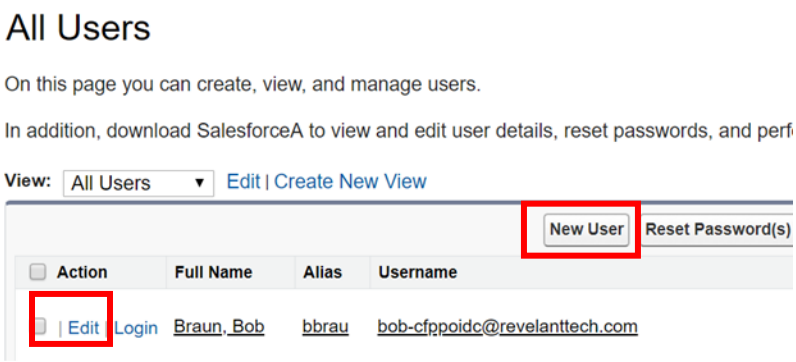


Set up a User

- In the Setup Quick Find field, type “user”.

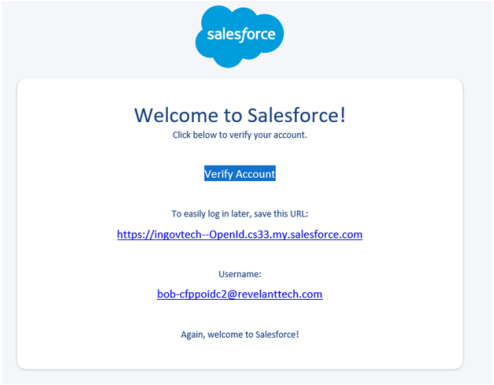


- Click the Users link to go to the All Users page.
- Either create a new User or edit an existing User. In this example, I am editing the Braun, Bob User by clicking the Edit link.



- Scroll down in the edit page to the “Additional Information” section. Enter the “Access Indiana Email” into the Access Indiana Email field.

- Your User should receive an email from support@salesforce.com with a link to “Verify your account”.

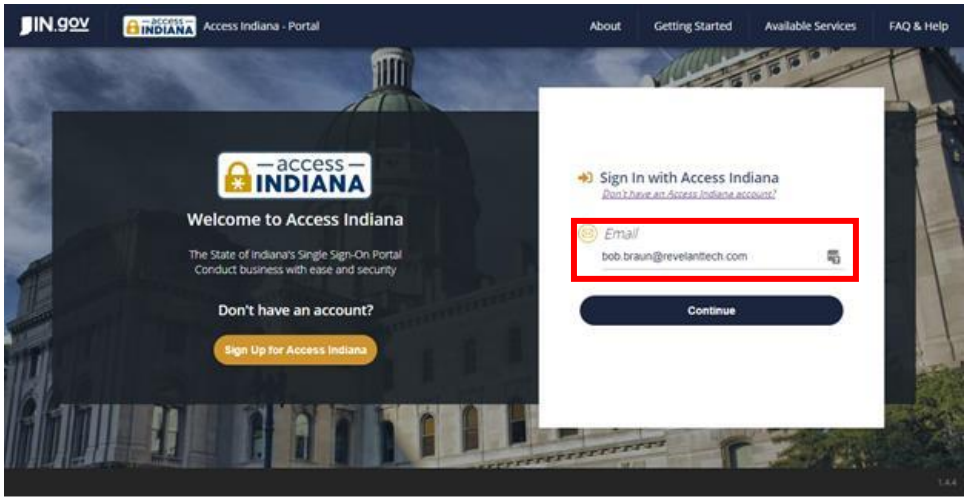


- Once the user ha clicked on the Verify Account link, the user is now ready to log in via Access Indiana.

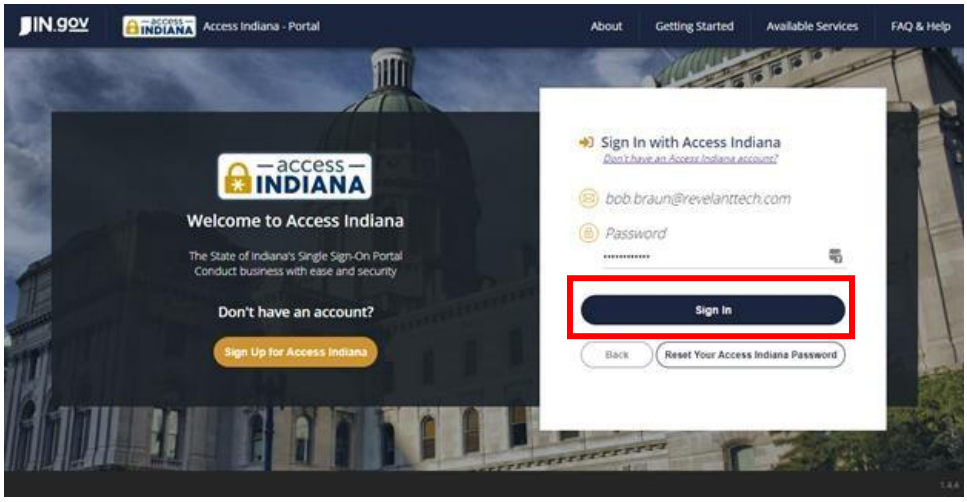
Test Your App

To test your application, log in to Access Indiana. In a browser, enter this URL: https://accessintegrate.in.gov

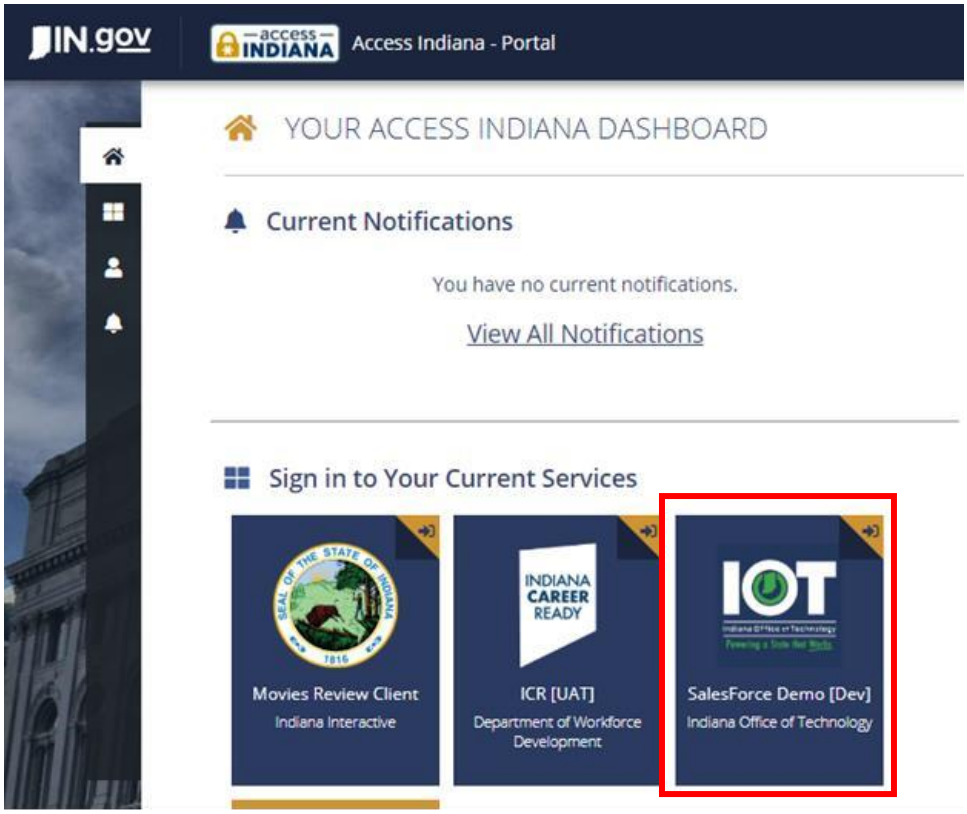
- Enter your Access Indiana Email address and click Continue (or click the “Don’t have an Access Indiana account?” link to create an account.)



- Enter your Access Indiana Password and click the Sign In button.



- You are now in the Access Indiana – Portal.



- Find the tile for your Access Indiana application. In this example, it is the IOT Salesforce Demo [Dev] tile. Click that tile to log into your Salesforce org.

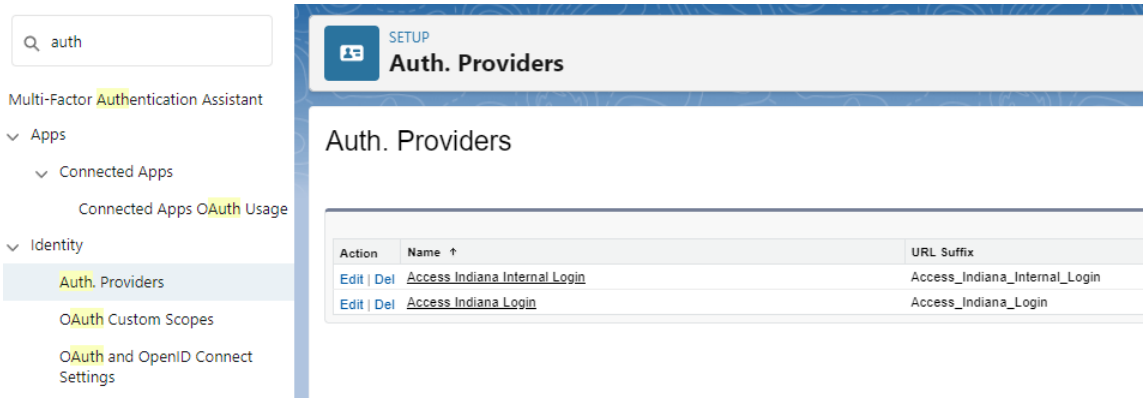
Sandbox Creation/Refresh Configuration

Once your sandbox is ready for use updates will be required in SFDC for Auth Providers and Remote Site Settings to leverage Access Integrate, https://accessintegrate.in.gov/, for the sandbox environment. If the environment was previously configured with Access Integrate the Client ID and Secret can be re-used without engaging with Access Indiana as outlined in 'Register an application with Access' section above.

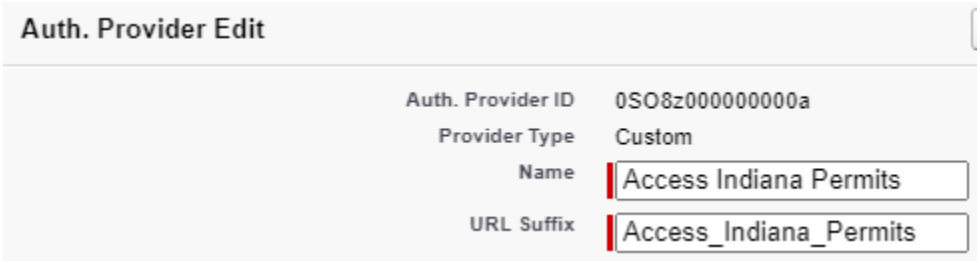
For Sandbox instances that have been configured with Access Integrate the Client ID and Client Secret should be stored securely by the Administrator Staff or values should be copied prior to starting refresh process for later configuration.

Auth Providers

- In the SFDC Setup menu search for Auth. Providers. Which should reference 'Access Indiana Internal Login' for internal staff access and 'Access Indiana Login' for external users accessing the new PSP Portal Site.



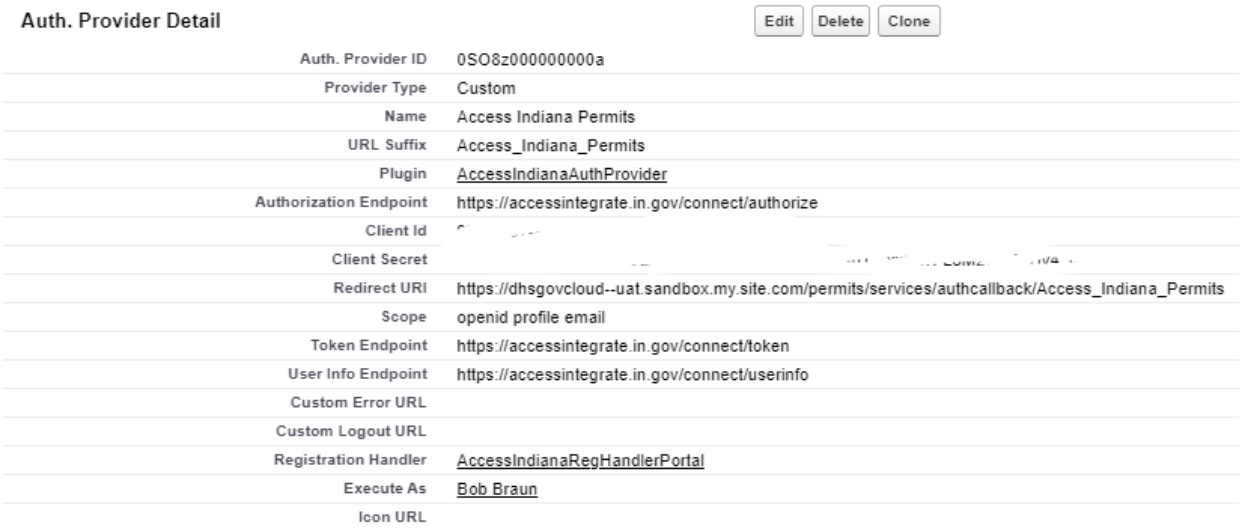
- ***Skip step unless working with Full copy sandbox 'UAT'
  If working with the full copy sandbox 'UAT' the name and URL Suffix for 'Access Indiana Login' should be updated to reflect 'Access Indiana Permits' to align the configuration with Access Integrate.



- For the selected Auth Provider update Endpoints referencing access.in.gov to accessintegrate.in.gov and the Redirect URL based on the Auth Provider configuration. Covered in detail in earlier section 'Initial configuration of Access Indiana custom Auth. Provider in your Salesforce org'.

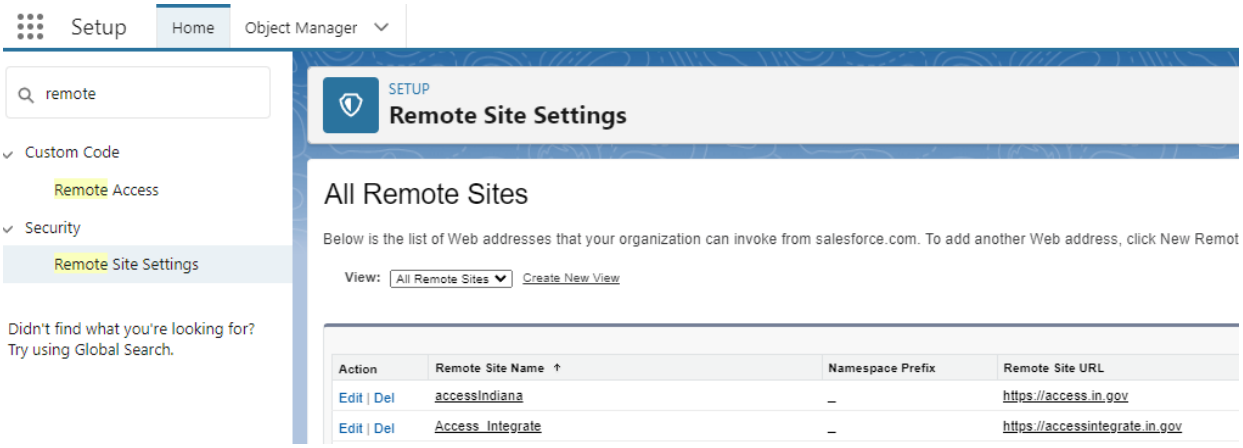
- Update the Client ID and Client Secret from the retained values from Access Integrate.

- Auth Provider configured for accessintegrate.in.gov should look similar to this.



Remote Site Settings

- In Setup search for Remote Site Settings



- Locate the Remote Site Name accessIndiana and delete this record. Doing this will help stop a sandbox from inadvertently accessing Prodction.

- Then create a new Remote Site entry. Remote Site URL should equal https://accessintegrate.in.gov. The Remote Site Name is only used in reference within the UI for users. This allows for external access of Access Integrate/Access Indiana.