# JanParichay Offerings

## ACR

**Introduction**

Before any user can access an application, a service must specify the authentication settings known as the Authentication Context Class Reference, or ACR.
JanParichay makes sure that the service is only accessible to users who have the necessary ACR requirements.

The following is a list of ACR parameters that JanParichay complies with:

| 1. Password | 2. Aadhaar | 3. PAN | 4. DL | 5. State | 6. Email |
|---|---|---|---|---|---|

Users that comply with ACR will have frictionless access to the service throughout their subsequent logins. JanParichay provides a user-friendly endpoint that enables customers who have not yet met ACR requirements to comply with ACR standards and access services immediately.

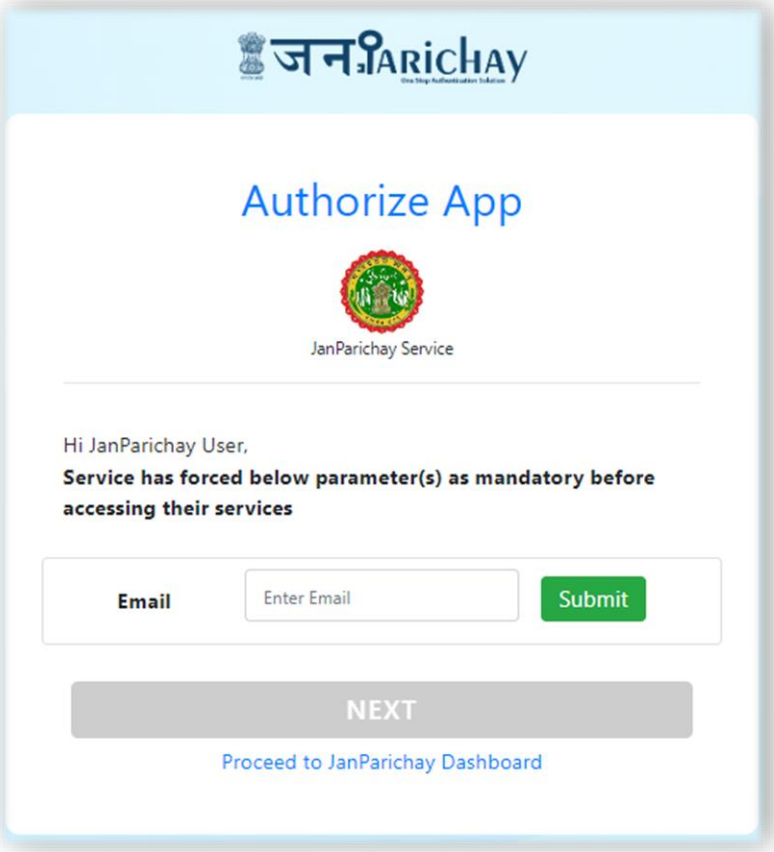



*Fig: JanParichay Portal for ACR Compliance*

**Need for ACR :**

As an SSO, JanParichay requires very little from users in order to facilitate a quick and safe registration procedure. When many users' accounts are onboarded from various sources, it could lead to a situation where a user isn't able to access some programme capabilities because he doesn't meet all the ACR requirements. When this happens, the user is sent back and must modify their profile and log in to the relevant service again. For services where customers can declare their expectations in a user profile before using their service, ACR is provided to enable smoother and more seamless operations between all applications and users.

**Advantages of ACR :**

The JanParichay Portal will only grant access to users who meet ACR requirements. This facilitates seamless operations between the SSO and integrated services.

Users don't have to update their profiles every time a disparity arises. Instead of having repeated calls, communication between the service and SSO occurs in a linear fashion.

**How to enforce ACR :**

Service owners can login on the JP Partners Portal and edit their service details with ACR.

Service owners will see a dropdown menu on the portal where they can select one or more ACR requirements for their service.
Once selected, click on 'Submit' to complete the process.

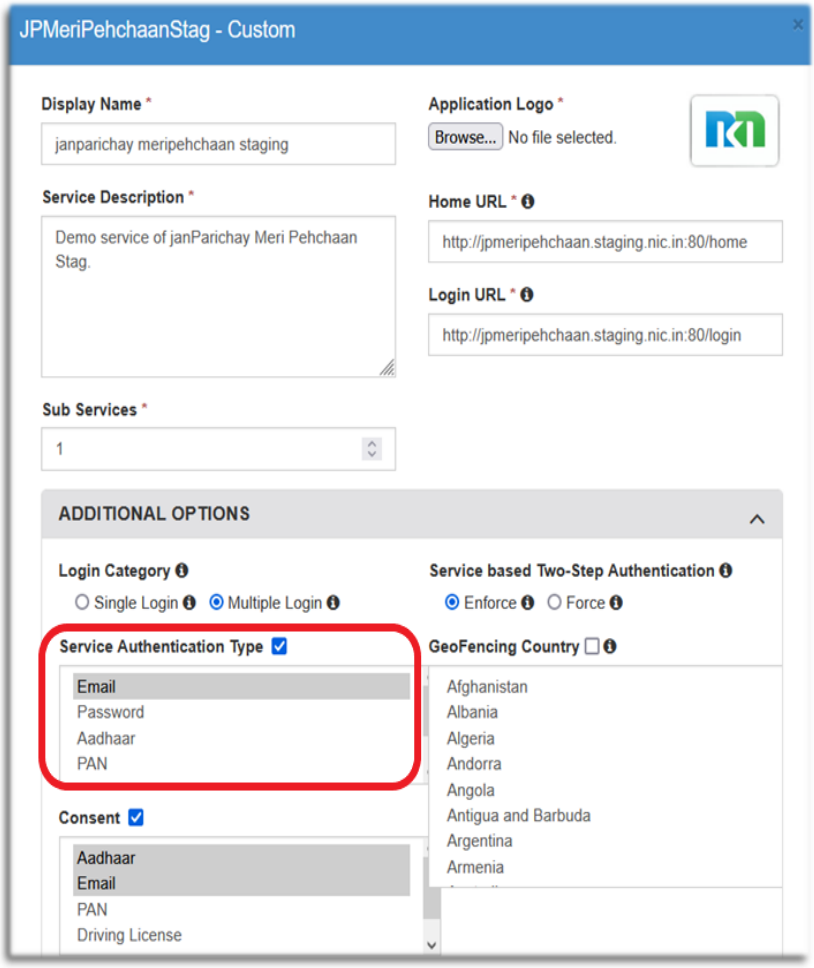



*Fig: JP Partners Portal to enforce ACR Compliance*

# SDL

**Introduction**

Conditional custom login interface, often known as Service Dynamic Login, or SDL for short. By using this interface, services can enable users to access their offerings on our SSO Portal using digital Aadhaar authentication.

In order to utilize the service, e-KYC users can use the interface to verify themselves and login using Aadhaar using either an OTP or finger biometric verification.

**Need for SDL :**

With a smooth linear flow, ACR was able to bridge the gap between the user's needs and the services requirements. However, in order to use the service, a user must log in to the JanParichay platform and employ two-factor authentication.

**Advantages of SDL :**

SDL guarantees session validation of an Aadhaar carrying user in the aforementioned problem statements. In addition, SDL supports services that require simply an eKYC validated user and do not require any additional ACR requirements.

Since users may log in to JanParichay immediately using their Aadhaar, they are not need to follow the regular login procedure.

Aadhaar login option is available on two verification parameters :

1. OTP Based Aadhaar Authentication
2. Finger Biometric Based Authentication

After authenticating successfully, the user is returned to their service.
If a user is already logged in, SDL makes sure that before they can use the service, they have to add Aadhaar to their user session. Thus confirming user session and authentication in the process.

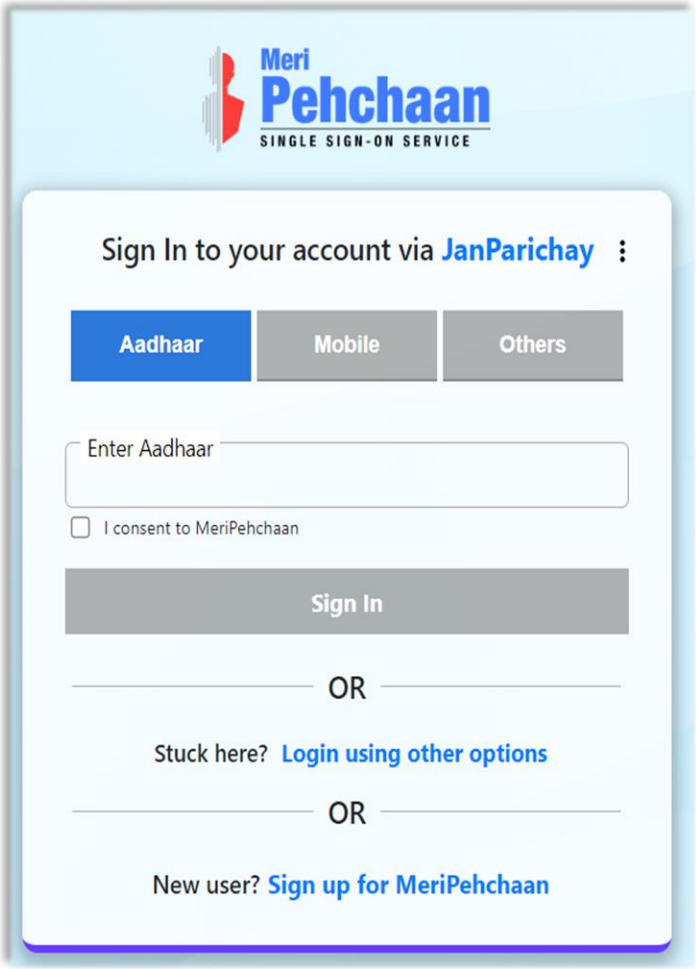



*Fig: JanParichay SDL Page*

**How to enforce SDL :**

Services can enforce SDL during service registration process. Integrated services can contact support to get this feature enabled. The feature will soon be made live on the JP Partners Portal and can be modified from the portal itself.

# Consent

**Introduction**

Services can mention user data to be added to the consent screen for which they are requesting consent from the users.

JanParichay consent page displays the values for which services need user's consent. Services will be sent only the values for which the user has consented on the consent page.

**Need for Consent :**

It allows you to collect and use data ethically while assuring users that their information is respected. By obtaining user consent, you can also ensure they are complying with legal requirements such as GDPR and other privacy laws.

**Advantages of Consent :**

It offers transparency , user's trust , giving user greater control, compliance with GDPR and other legal requirements and privacy laws.

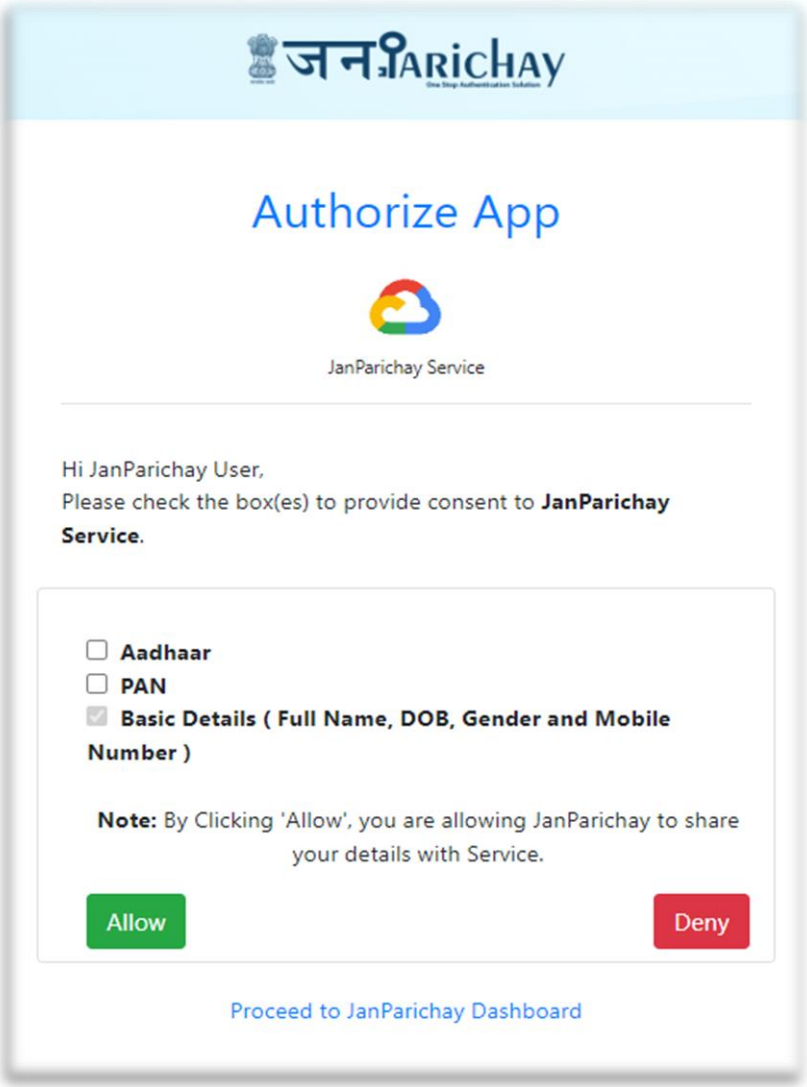



*Fig: JanParichay Consent Page*

**How to enforce Consent :**

Service owners can login on the JP Partners Portal and edit their service details with Consent Scopes.

Service owners will see a dropdown menu on the portal where they can select one or more Consent Scopes requirements for their service.

Once selected, click on 'Submit' to complete the process.

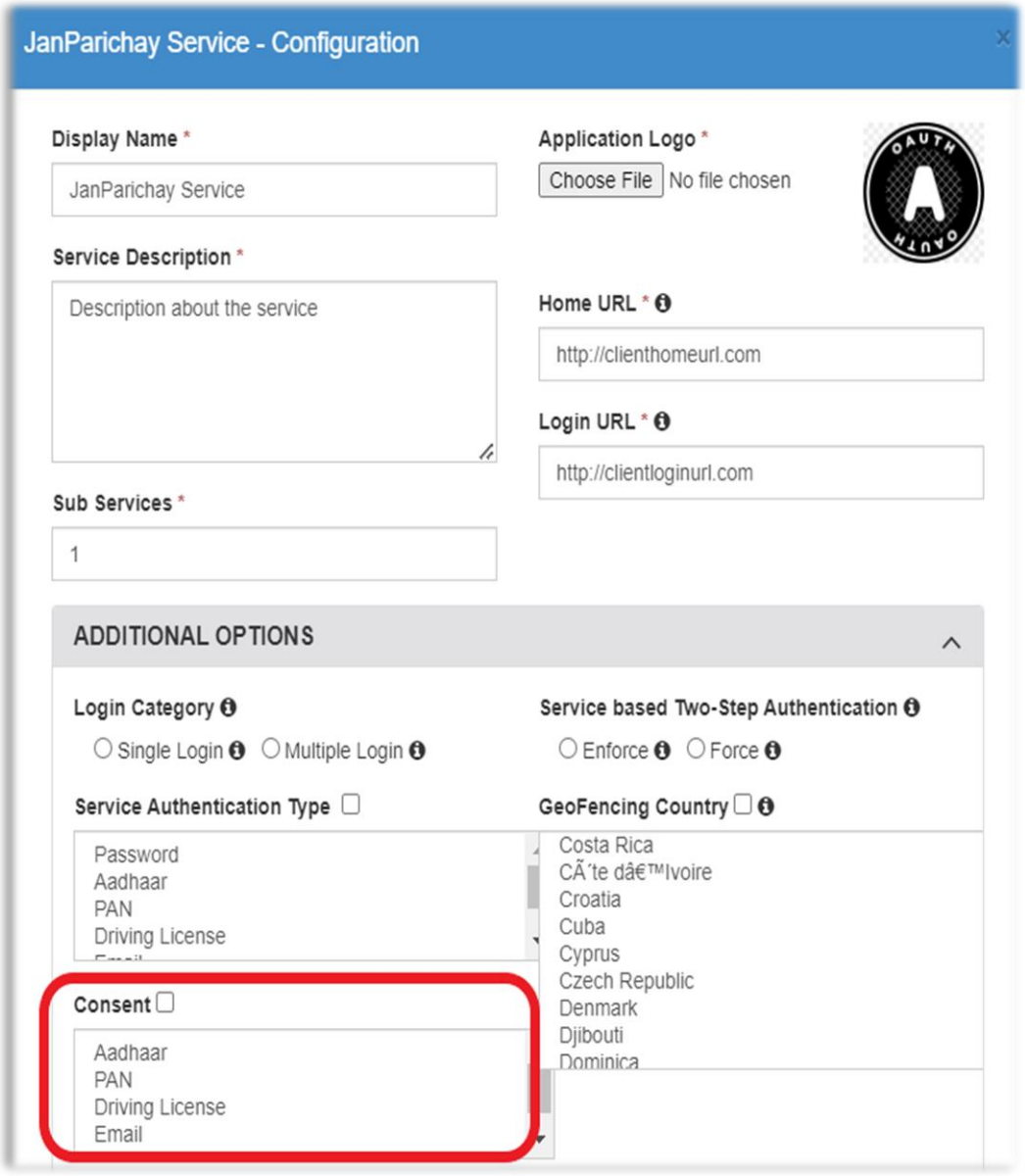



*Fig: JP Partners Portal to enforce Consent Scopes*

# GeoFencing

**Introduction**

GeoFencing in JanParichay is used to enhance cybersecurity, enforce access restrictions and prevent unauthorized access to sensitive information.

This personalized feature enables users to manage the accessibility to their account. Users can opt to either Per-user Global Authorization or Per-user Per-service Authorization as per their requirements.

**Need for GeoFencing :**

By leveraging geolocation — the geographical location of devices connected to the Internet — geofencing allows marketers to create virtual boundaries around brick-and-mortar business locations (geofences), and deliver alert and notifications when consumers enter them.

**How to enable geofencing:**

GeoFencing can be enabled by both the service and the user.

**For Users**

Users can enable the functionality from the Account Settings Page on the JanParichay Page.

GeoFencing can be enabled either Globally or for a particular service as well.

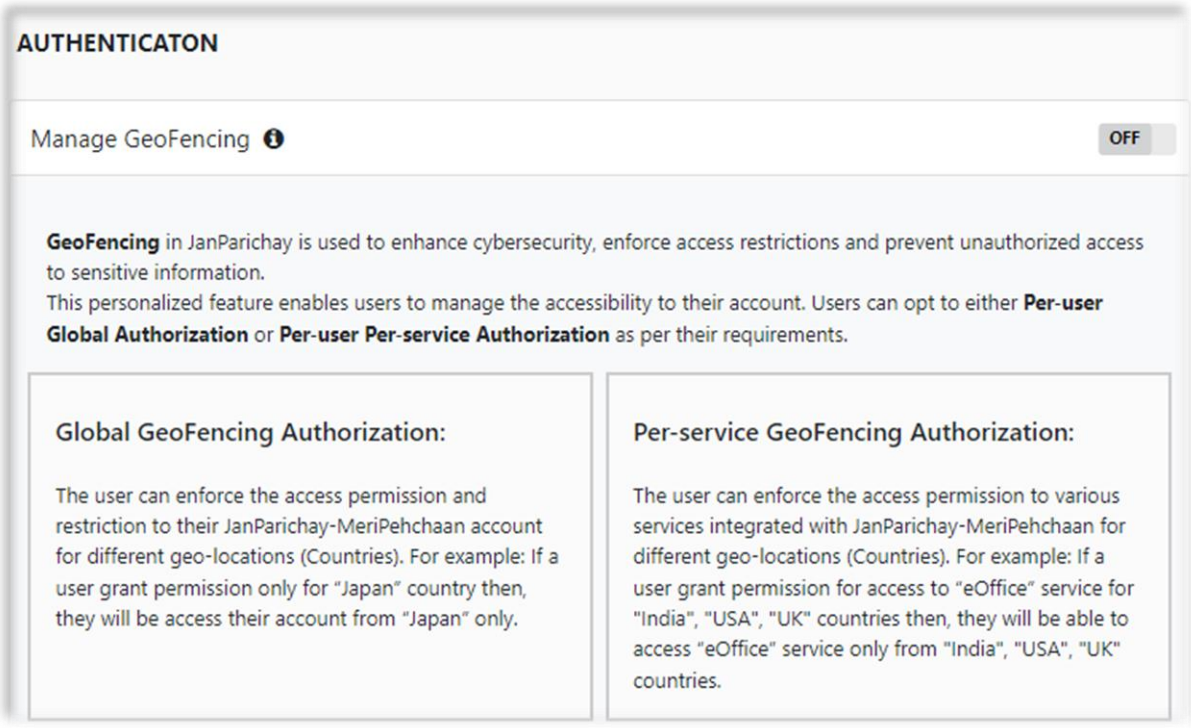
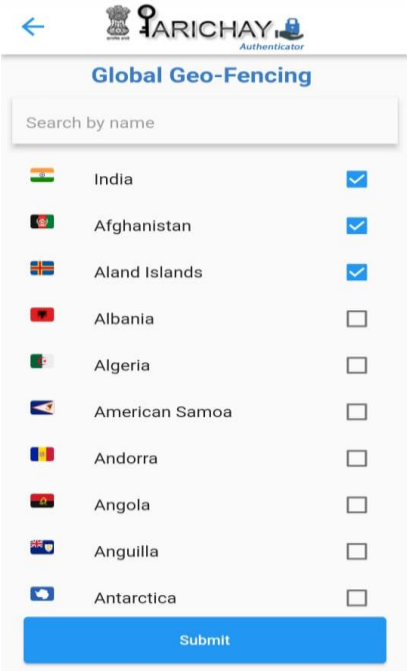
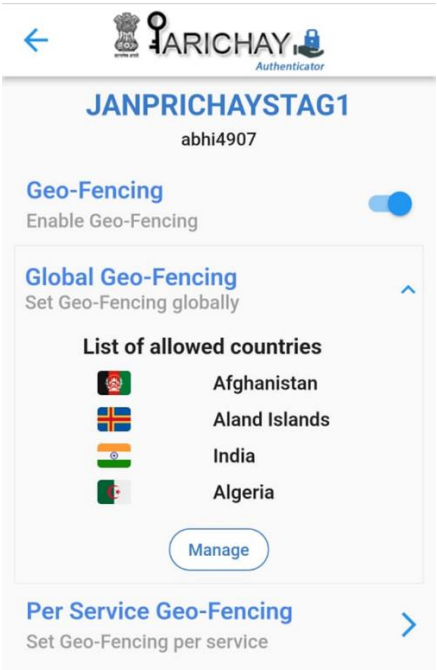



*Fig: Enable GeoFencing from the JanParichay Account Settings Page*

Users can also enable GeoFencing from the Parichay Authenticator Mobile App.




**For Services**

Service owners can login on the JP Partners Portal and edit their service details with GeoFencing.

Service owners will see a dropdown menu on the portal where they can select one or more country to apply GeoFencing for their service.

Once selected, click on 'Submit' to complete the process

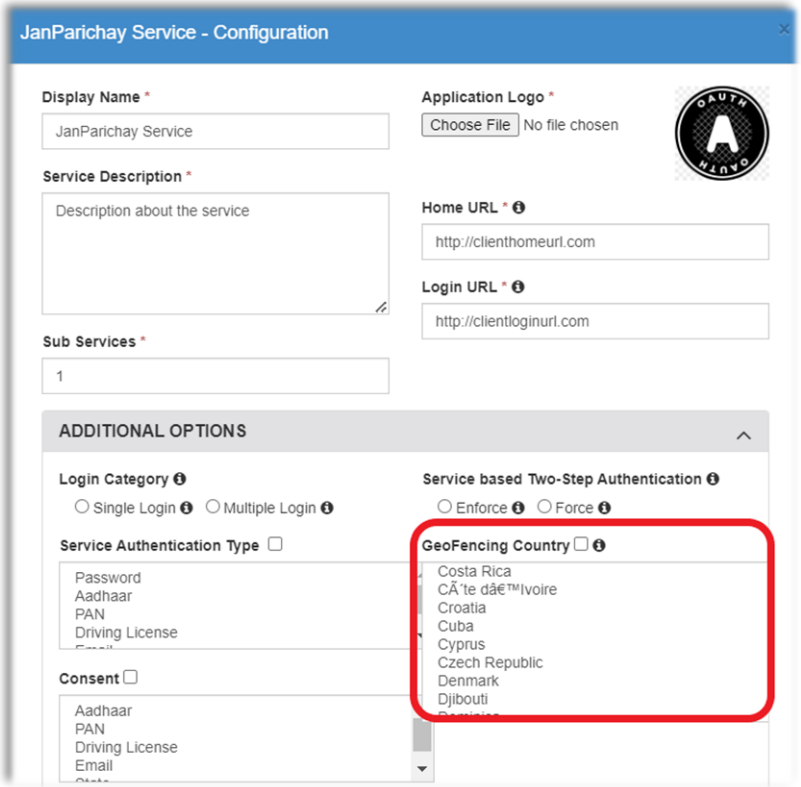



*Fig: Enable GeoFencing from the JP Partners Portal*