# User Guide

## PMS Admin (Partner Admin)

**Partner Management Portal (PMP) is used by both; PMS Admin and Partner User.**

* Partner Administrator: Partner Admin
* Partners: Partner User
* **Partner User** - ‘Authentication Partners’ can use the new interface to perform all the activities mentioned under ’**[Authentication Partner Workflow](end-user-guide.md" \l "authentication-partner-workflow)’**
* **Partner Admin** - Partner Admin still will have to user the older ‘Partner Admin Interface to perform all the activities explained under’[**What all activities does a ‘Partner Admin’ perform for Authentication Partner?**](end-user-guide.md#what-all-activities-does-a-partner-admin-perform-for-authentication-partner)’. {% endhint %}

## 

## What all activities does a ‘Partner Admin’ perform for Authentication Partner?

Being a ‘Partner Admin’ you can perform following 3 activities to complete the end to end functionality pertaining to Authentication partner.

It should be noted that all these activities that you can perform as an admin you will still have to use the older ‘Partner Admin Interface’ as of now untill we complete its revamp which is already underway on a war footing.

* Upload Root CA and Sub CA Certificates
* Create Policy Group and Policy
* Approve/Reject Policy

### Upload Root CA and Sub CA

Only after you ‘Upload Root CA and Sub CA Certificates (From Older PMP Interface)’ that a Partner will then be able to ’Upload CA signed Partner Certificate.

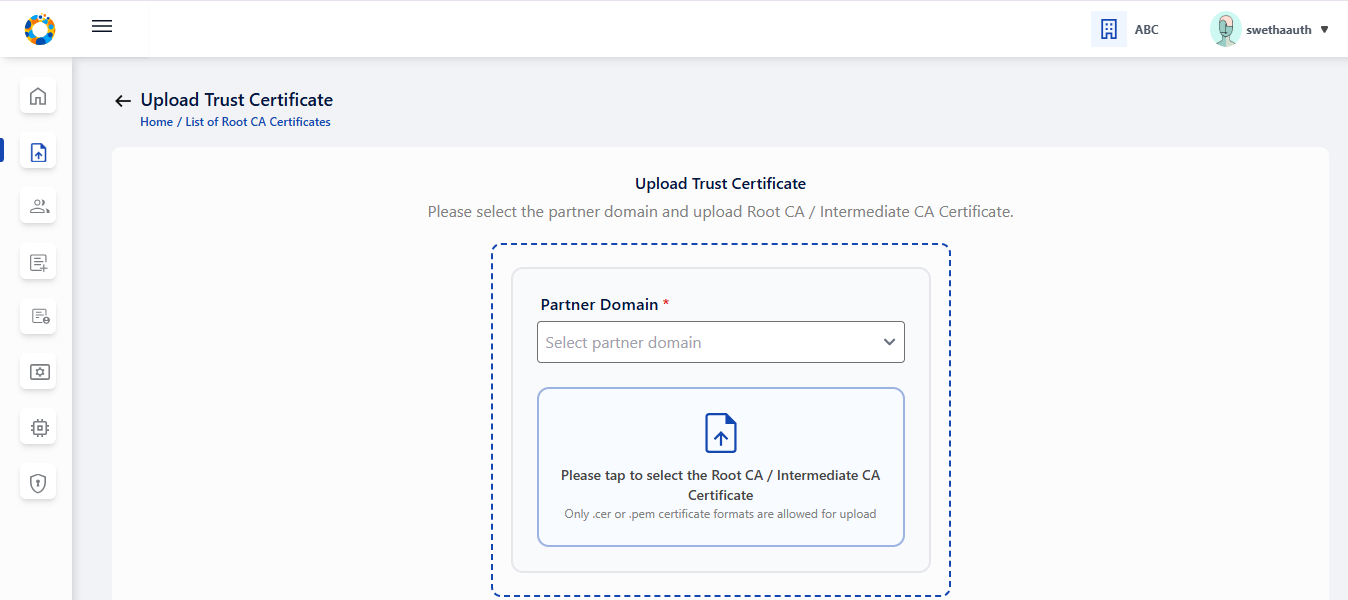
As a process of Partner onboarding onto PMP after successful registration, Partner is required to **Upload CA signed Partner Certificate** on behalf of their organisation which would be used to build a trust store in MOSIP to cryptographically validate that they are from a trusted organisation to perform authentication of citizens. Also this certificate is used to encrypt the response shared in e-KYC.

{% hint style=“warning” %} **Important:**

You will have to use older Partner Admin interface, Yes! you read it correct! before a Partner will be able to ‘**Upload ‘CA Signed Certificate**’ it is prerequisite that the ‘**Partner Admin**’ must upload the **Root CA** and **Sub CA** certificates and this you can do from ’**Older PMP Interface’**. {% endhint %}

#### To Upload Root CA and Sub CA Certificates

1. In ‘Certificate Trust Store’ click on ‘Upload Trust Certificate’.
2. Select the Partner Domain- AUTH in Upload Trust Certificate page.
3. Choose the **Root CA Certificate** to upload (only files with extensions as .cer or .pem).
4. Click Submit.
5. Similarly, sub/intermediate CA certificate should be uploaded by following the above steps (1-4).



image

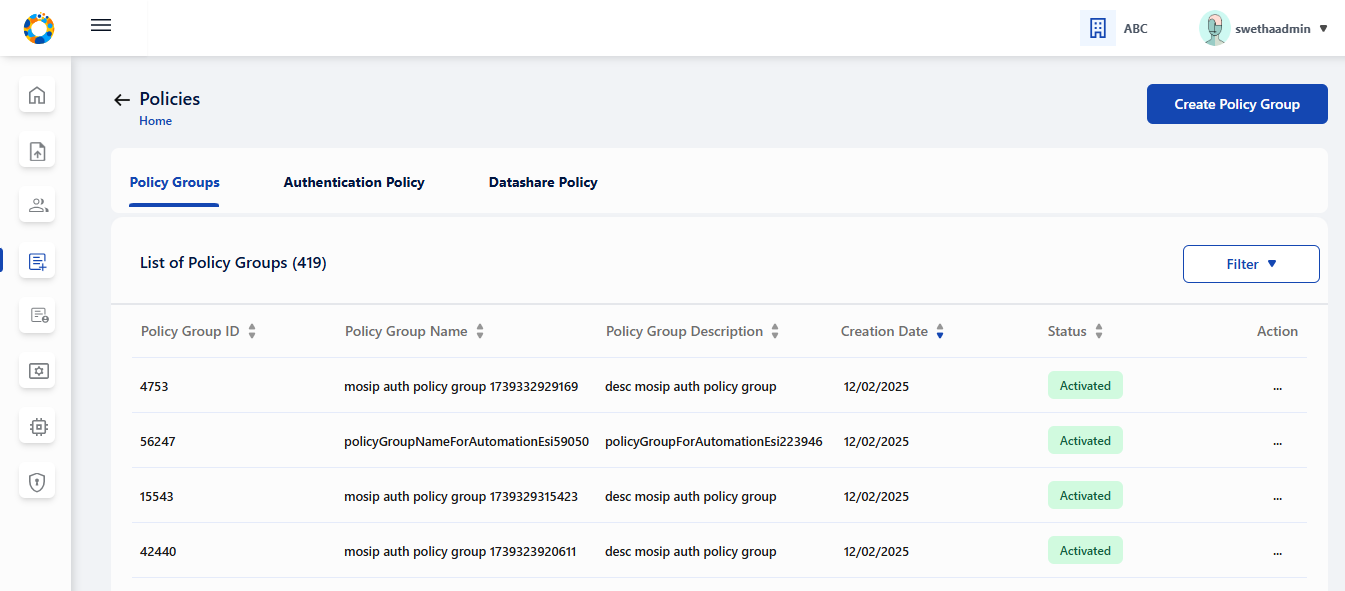
### Creating Policy Group and Policy

As Partner Admin you are required to ‘**Create Policy Group**’ and ‘**Create Policy(s)**’ which a ‘Partner’ will be able to select while self-registering on PMP.

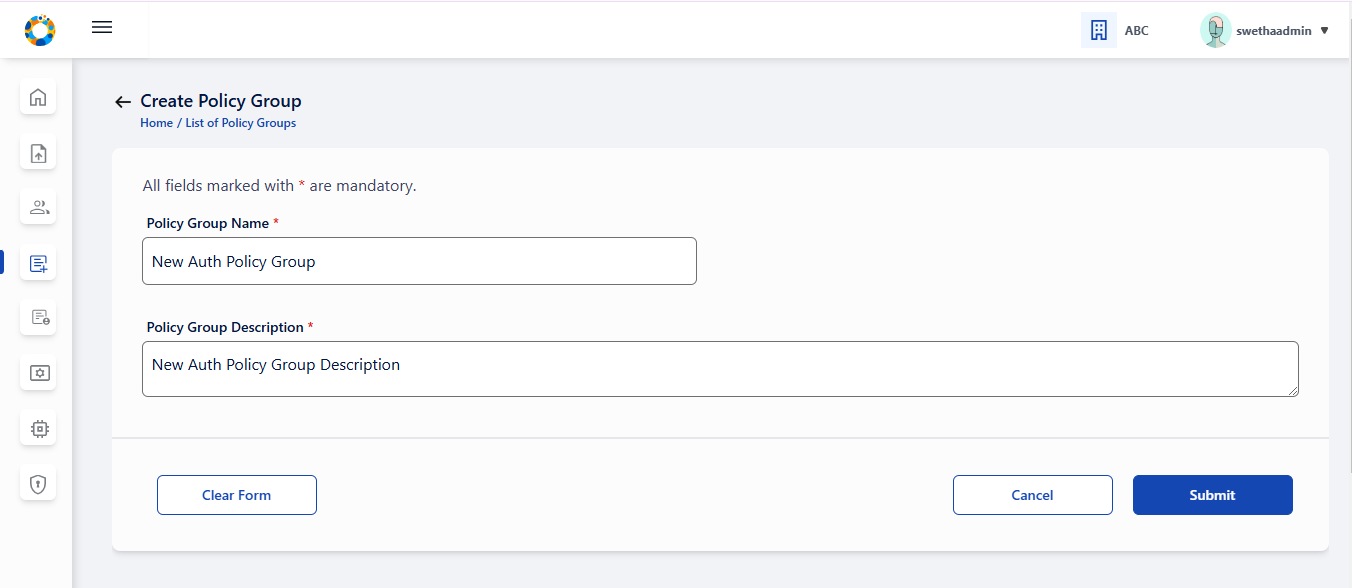
As an admin you will also have privilege to ‘**Approve Policy Request**’ when a Partner selects a Policy and it comes to you for approval, You can read more about this [**here**](end-user-guide.md#approve-policy-request).

#### Create Policy group

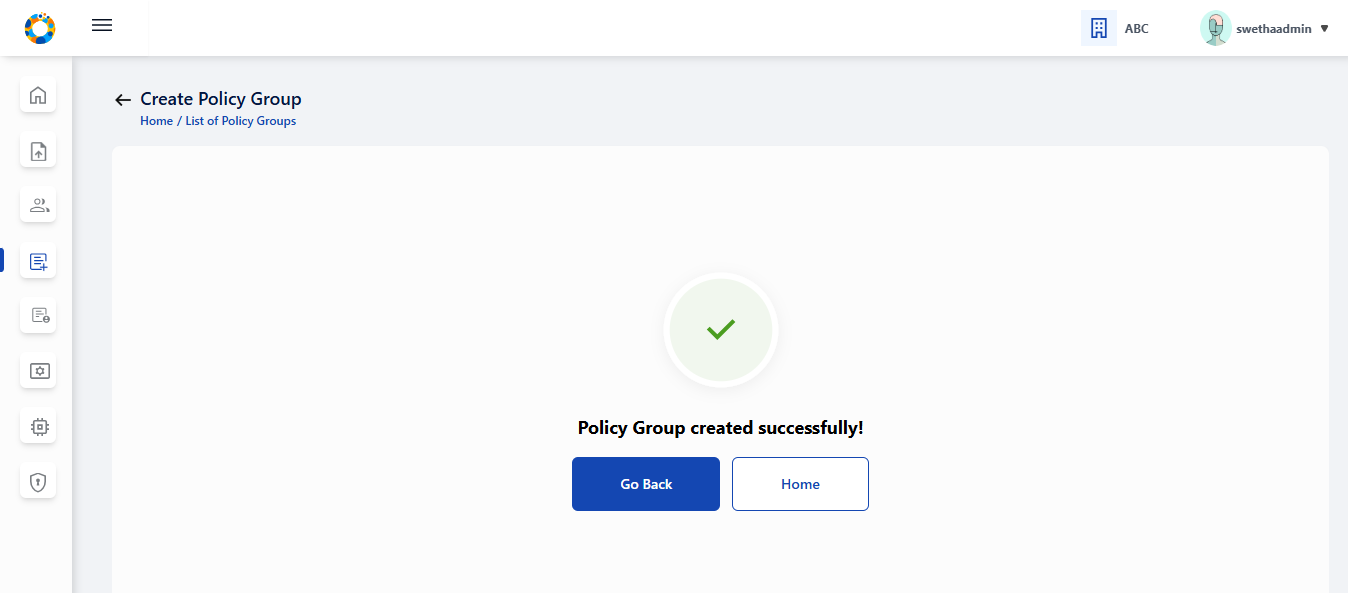
* Login as Partner Admin into the PMS portal (Older PMP Interface).
* All the policy groups created so far by Partner Admin/ Policy Manager are displayed on ‘List of Policy Groups’ page.



* On clicking the ‘Create Policy Group’ option on the top right of the screen, we can create a Policy Group by providing suitable name and description that is self explanatory for partners, who would be selecting them during Partner Policy Request to create API Key/ OIDC Client etc.



* On click of Submit, a success message appears.

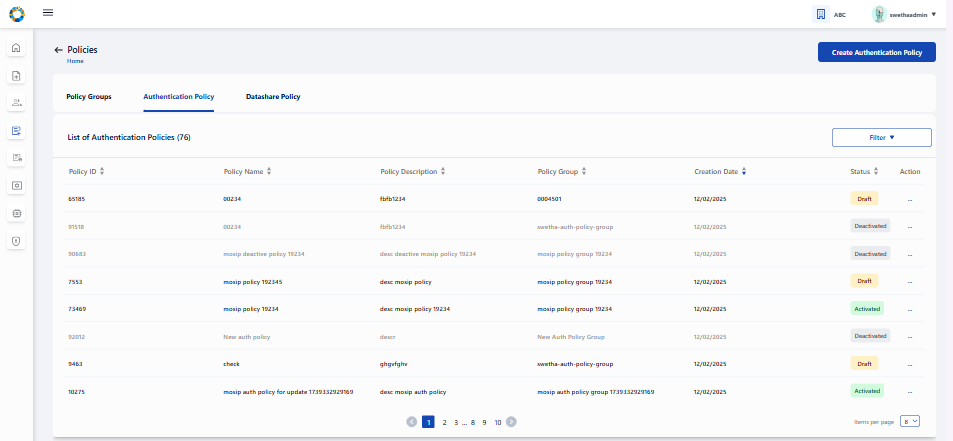


#### Create Auth policy

Once you ‘Create Policy’ you will also be required to activate it and then it will reflect when a Partner wants to select a policy. You can also change the status of **Policy Group** ( Deactivate) or edit it using the Action menu as shown below.

1. On clicking Authentication Policy tab, List of all previously created Authentication Policies are displayed.

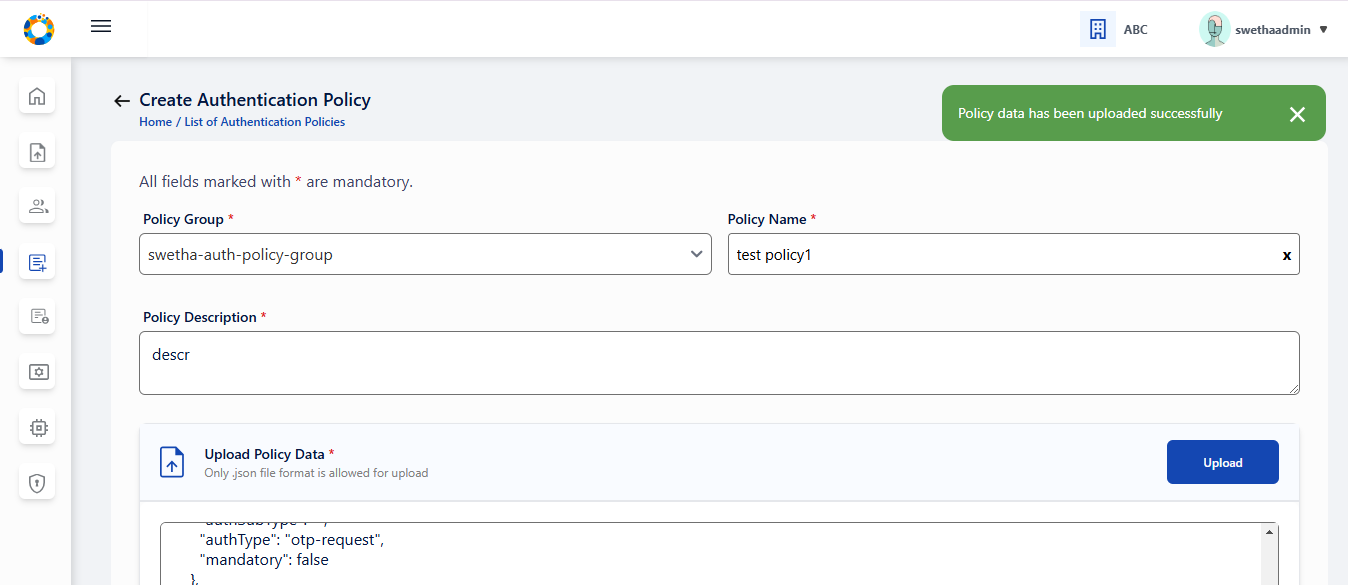
On clicking Authentication Policy tab, List of all previously created Authentication Policies are displayed.



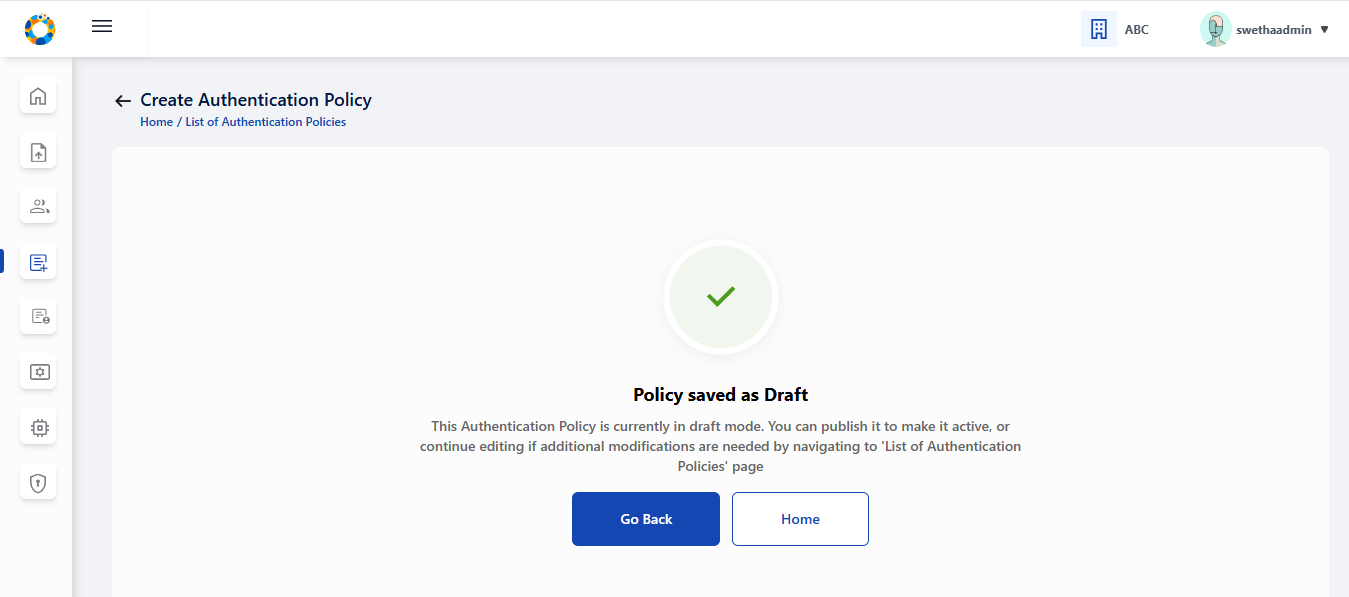
On clicking ‘Create Authentication Policy’ button, Partner Admin/ Policy manager is navigated to Create Authentication Policy page where details such as policy group, policy name, description etc will have to be entered

Note: Only active policy groups are available in the policy group dropdown.

click on the upload button to upload policy data . Only json files are allowed for upload.

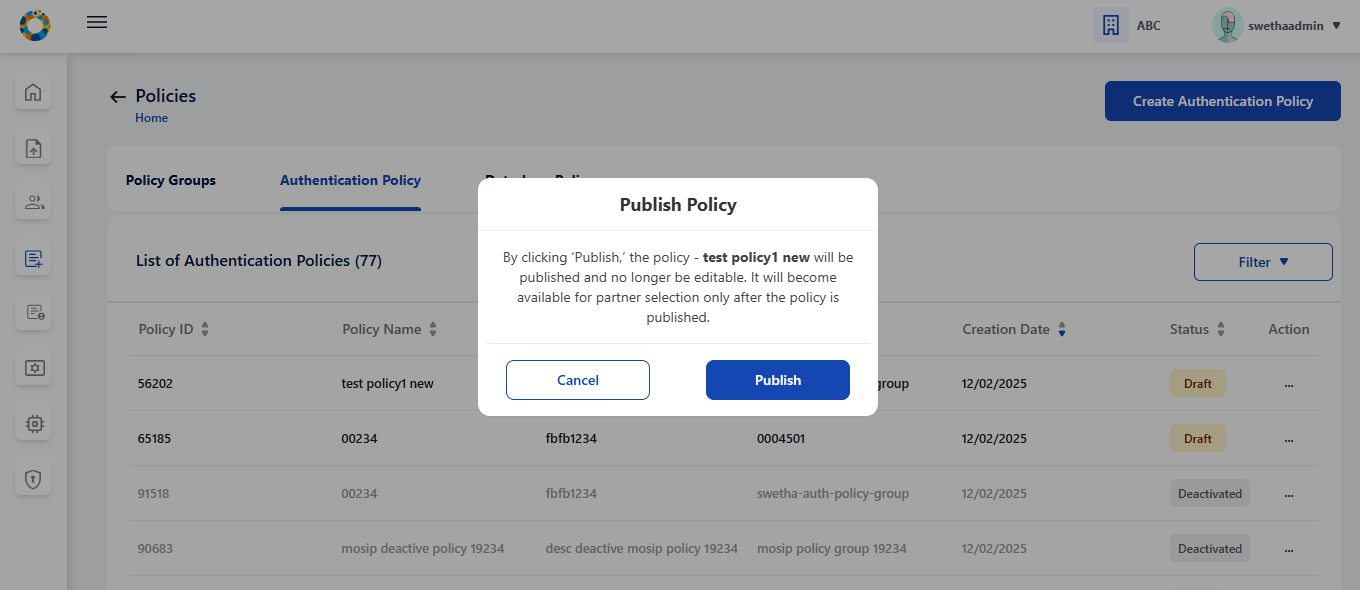


On clicking on Save as Draft, following success message appears .

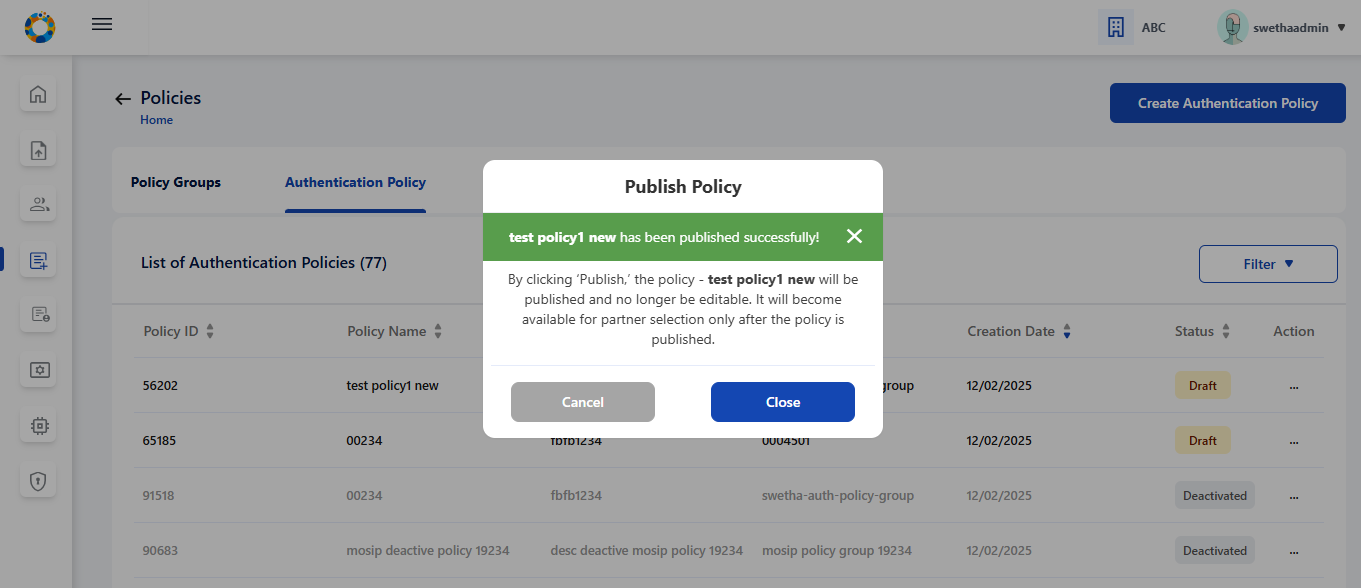


On clicking ‘Go Back’, admin is navigated back to tabular view where the policy is saved as ‘draft’ status.

To **publish policy** which is currently in draft status, click on ‘publish’ option in action menu. A popup window appears seeking for confirmation to publish.



On clicking Publish, a success message appears . Click on close to close the window.



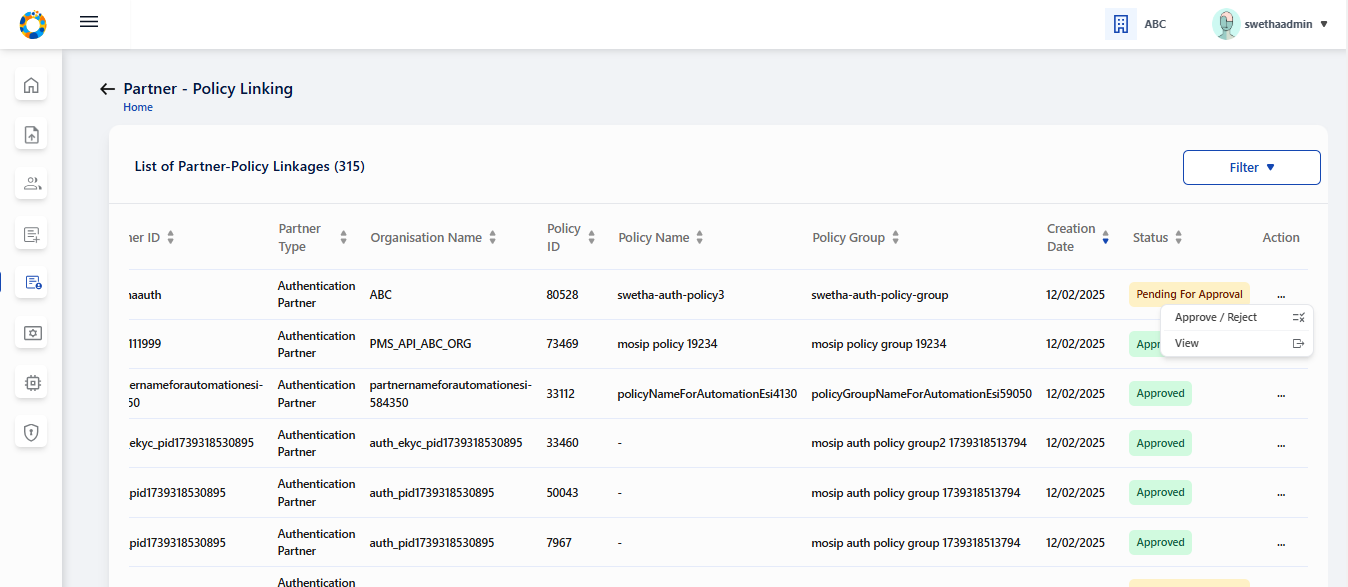
The given policy changes to ‘Activated’ status after being published. Once activated, the admin cannot edit the policy, hence the option is disabled.

Approve Policy Request

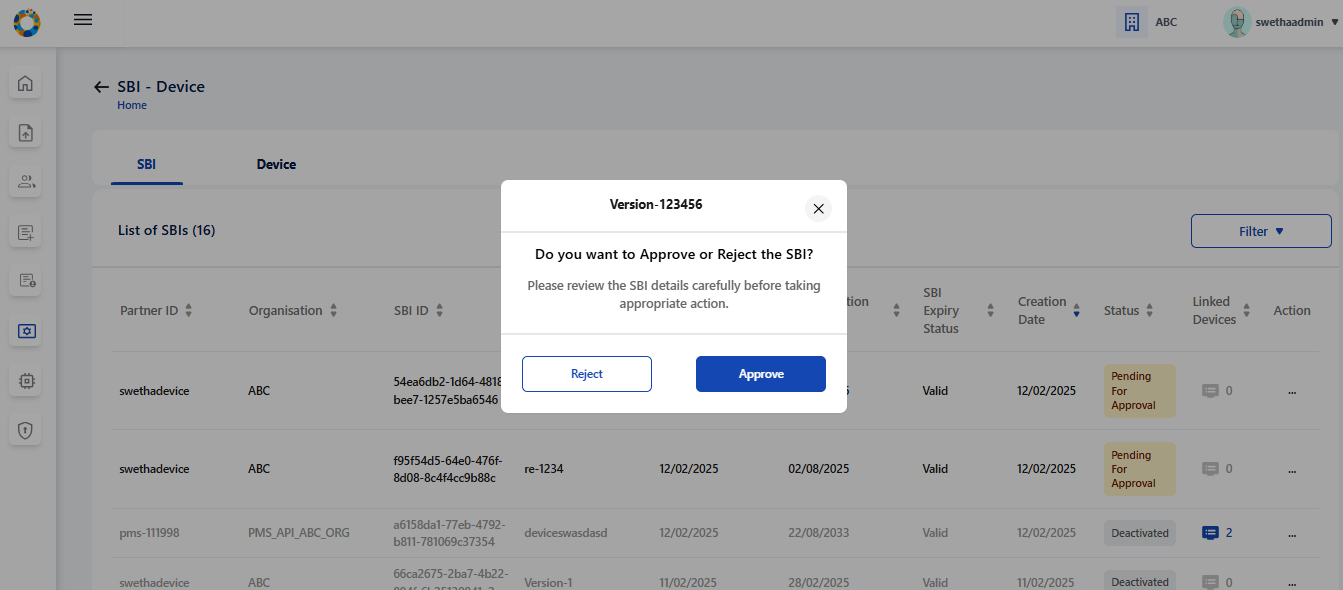
When a Partner have chosen a ‘Policy Group’ and the ‘Policy’, an approval request will come to you and you can approve or reject a ‘**Policy Request**’ using ‘**Request Policy**’ screen.

When a Partner have chosen a ‘Policy Group’ and the ‘Policy’ an approval request will come to you and you can approve or reject a ‘**Policy Request**’ using ‘**Request Policy**’ screen.

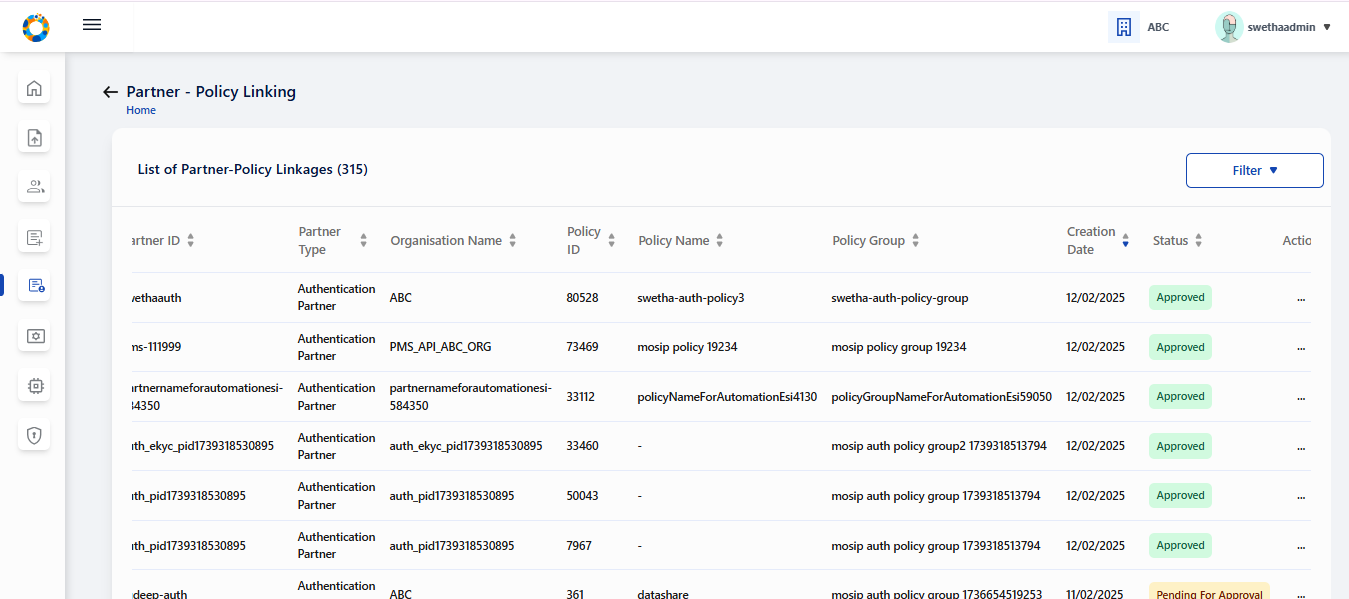
* Click on **Partner Policy Linking** in the admin dashboard.
* Select the policy mapping that needs an approval.The options provided for policy linking requests in ‘Pending for Approval’ are to Approve/ Reject. Also an option to view the policy request details is also provided.



On clicking the Approve/ Reject option, the window appears - and partner admin can click on either Approve or Reject to take appropriate action



The status- Approved / Rejected gets updated in the tabular view.



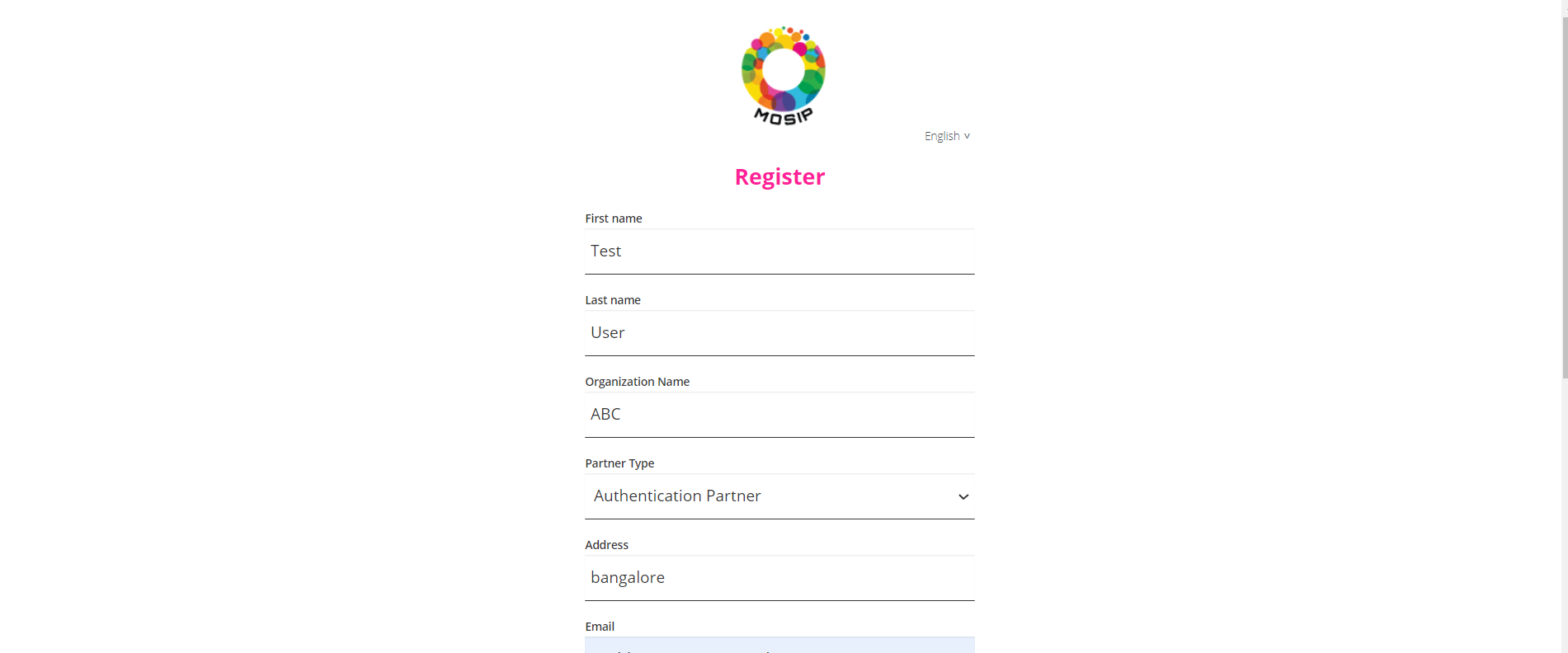
## Authentication Partner Workflow

To be able to access the services by PMP and to validate that the partner is from a trusted organisation, undergoing self registration on PMP and uploading CA signed certificate is necessary’.

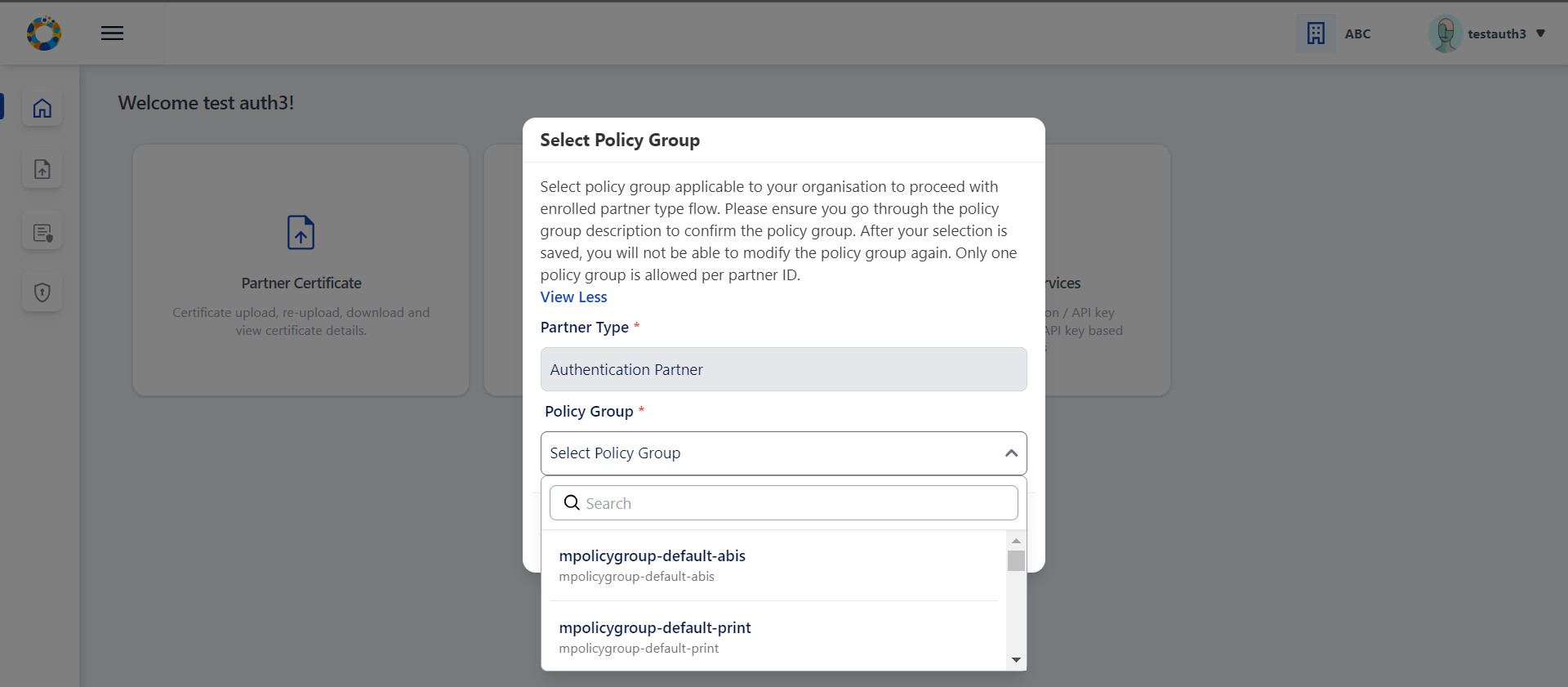
* Self Register on PMS Interface
* Upload CA signed Certificate

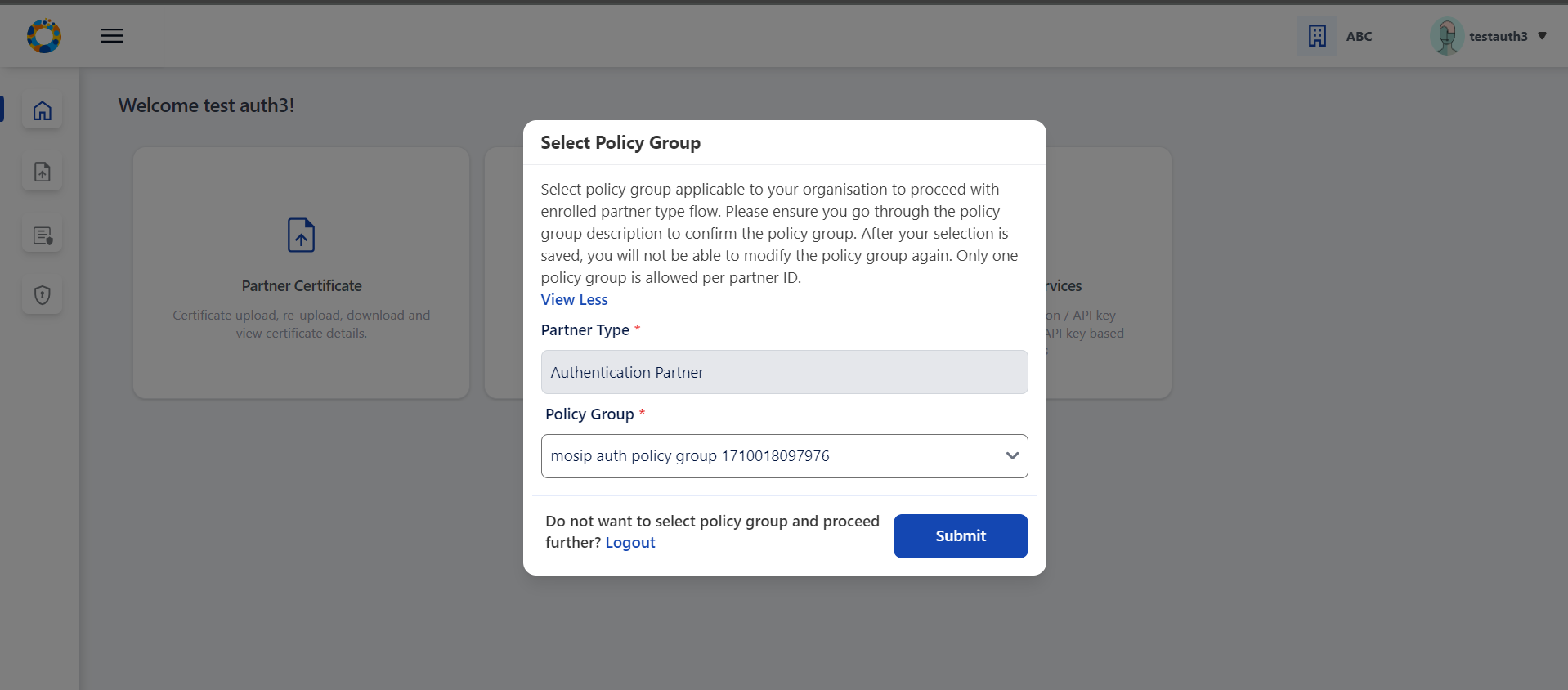
### Self-Register on PMP as Authentication Partner

1. The Authentication Partner can register themselves on MOSIP PMS portal by clicking **Register** on the Login Page, a form comes up.
2. Enter the Authentication Partner details:
   1. Partner type (Authentication Partner)
   2. First and Last name
   3. Organization Name
   4. Address, Phone number
   5. e-mail, Username and password

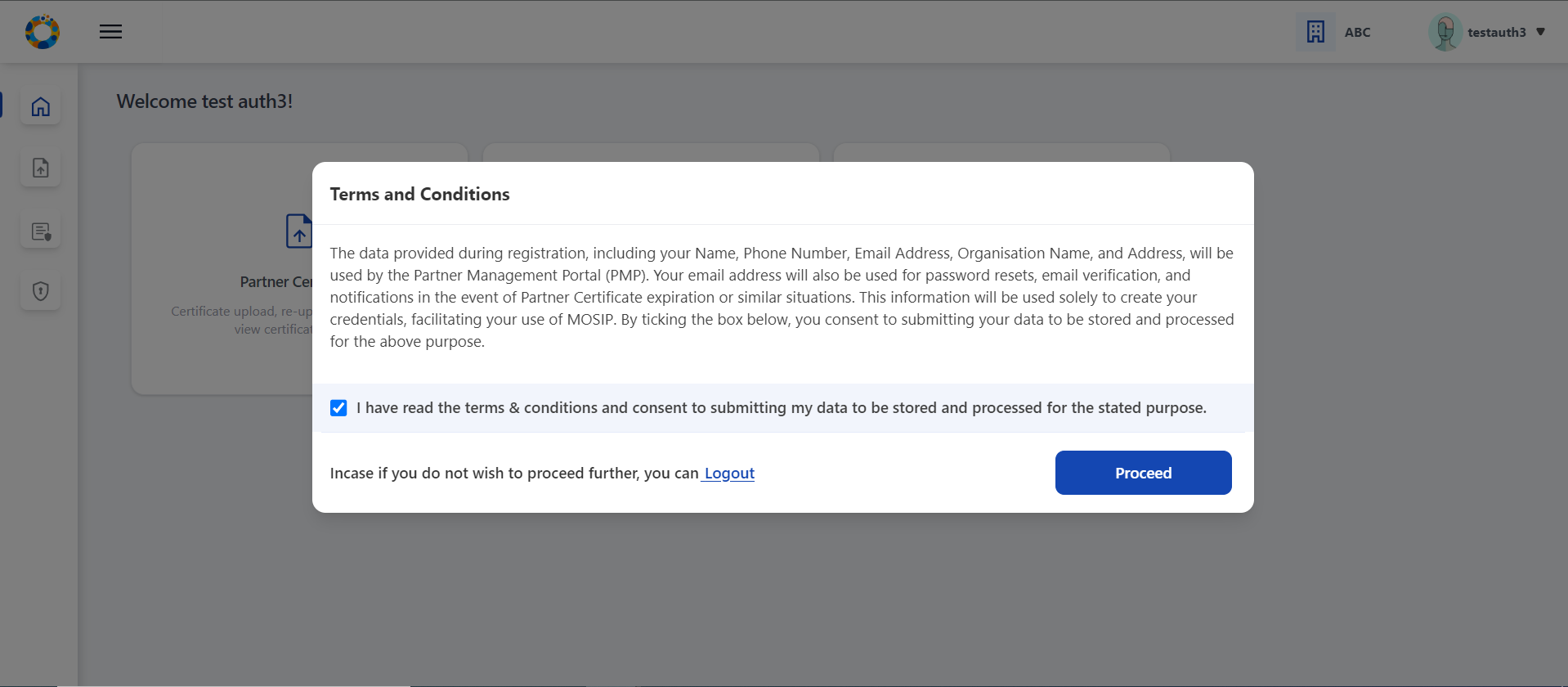
 ” alt=““>

1. **Click** on **Register**, a popup comes up which asks you to ‘**Choose a Policy Group**’ and seeks you to ‘**Agree to Terms and Conditions**’ before you can be considered as ’Authentication Partner.
2. Select the relevant/applicable **Policy Group** on **Select Policy Group** popup using **Policy Group** dropdown by reading through policy group description in dropdown.

 ” alt=““>

 ” alt=““>

1. On Submit it will ask you to read through ‘**Terms and Condition**’ and having carefully read through it you can agree and accept it.

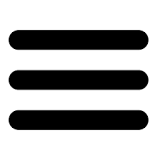
 alt=““>

{% hint style=“info” %} **Validations**:

* User can select only one **Policy Group** per **Partner Type**.
* Policy selected once cannot be edited later.
* Terms & Conditions: Partner consent refers to voluntary and informed agreement provided by a partner user on behalf of the Partner Organisation, to a specific action or process where the users have a clear understanding of what they are consenting to. User consent is important to ensure data privacy, where it is compliant to obtain explicit consent from partners before collecting, processing, or sharing their personal/ organisation level data.
* A detailed description explaining which of their personal and organisation data is used and for what purposes it will be used in PMP will be informed while seeking user consent. {% endhint %}

### CA Signed Partner Certificate Upload / Download or Re-Upload

User is now in [**Home Page/Dashboard**](end-user-guide.md#interface-overview) where the following features are provided to Authentication Partner: 1) Partner Certificate, 2) Policies and 3) Authentication Services: OIDC Client and API Key generation.

These features can also be accessed by clicking on side panel (in the form of icons) or clicking on the hamburger menu  on the top left which is available across all screens of PMP to help user to easily navigate.

Once registered, as a process of Partner onboarding onto PMP after successful registration, user is required to perform upload CA signed Partner Certificate on behalf of their organisation which would be used to build a trust store in MOSIP to cryptographically validate that they are from a trusted organisation to perform authentication of citizens. Also this certificate is used to encrypt the response shared in e-KYC.

{% hint style=“info” %} **Tips**:

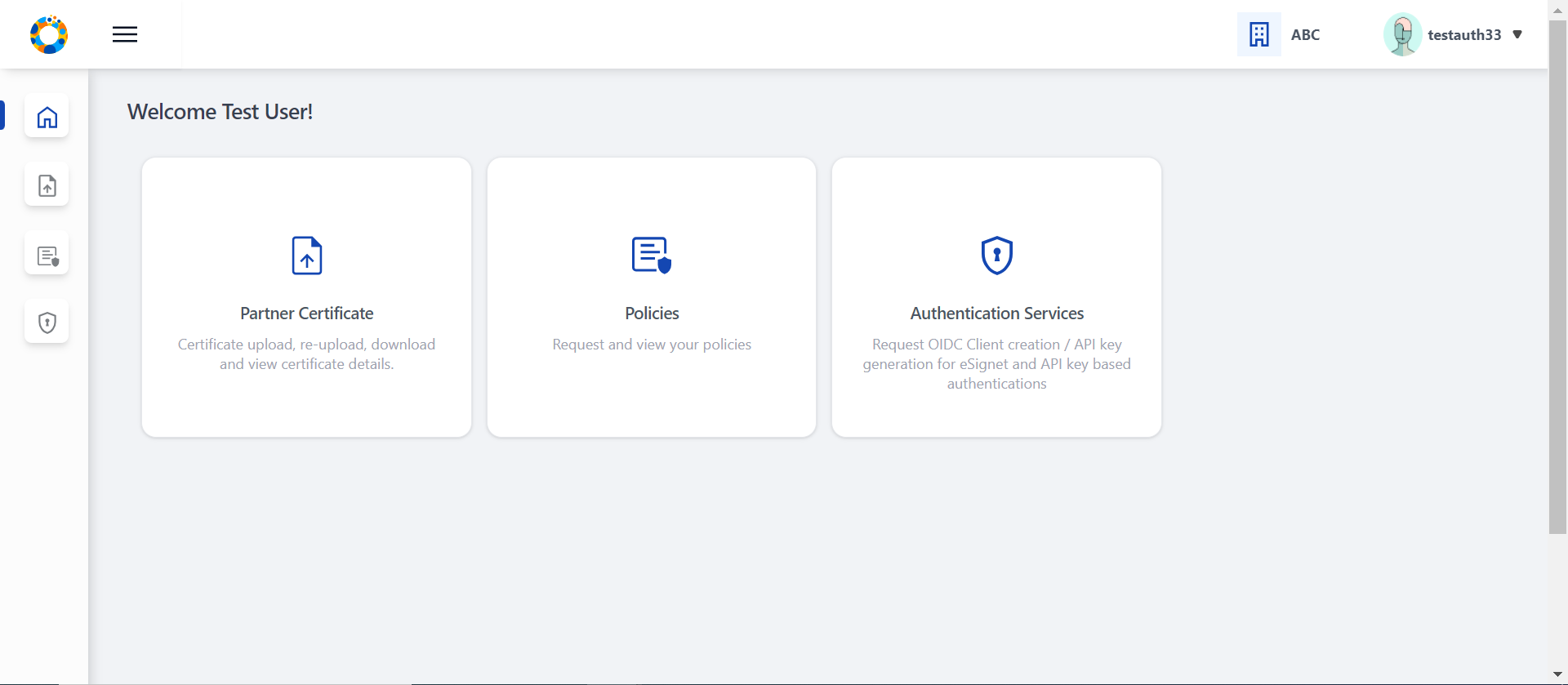
Later when required a Partner can also ‘Download Certificate’ and ‘Re-Upload Certificate’ (As the need may be). {% endhint %}

{% hint style=“info” %} Important:

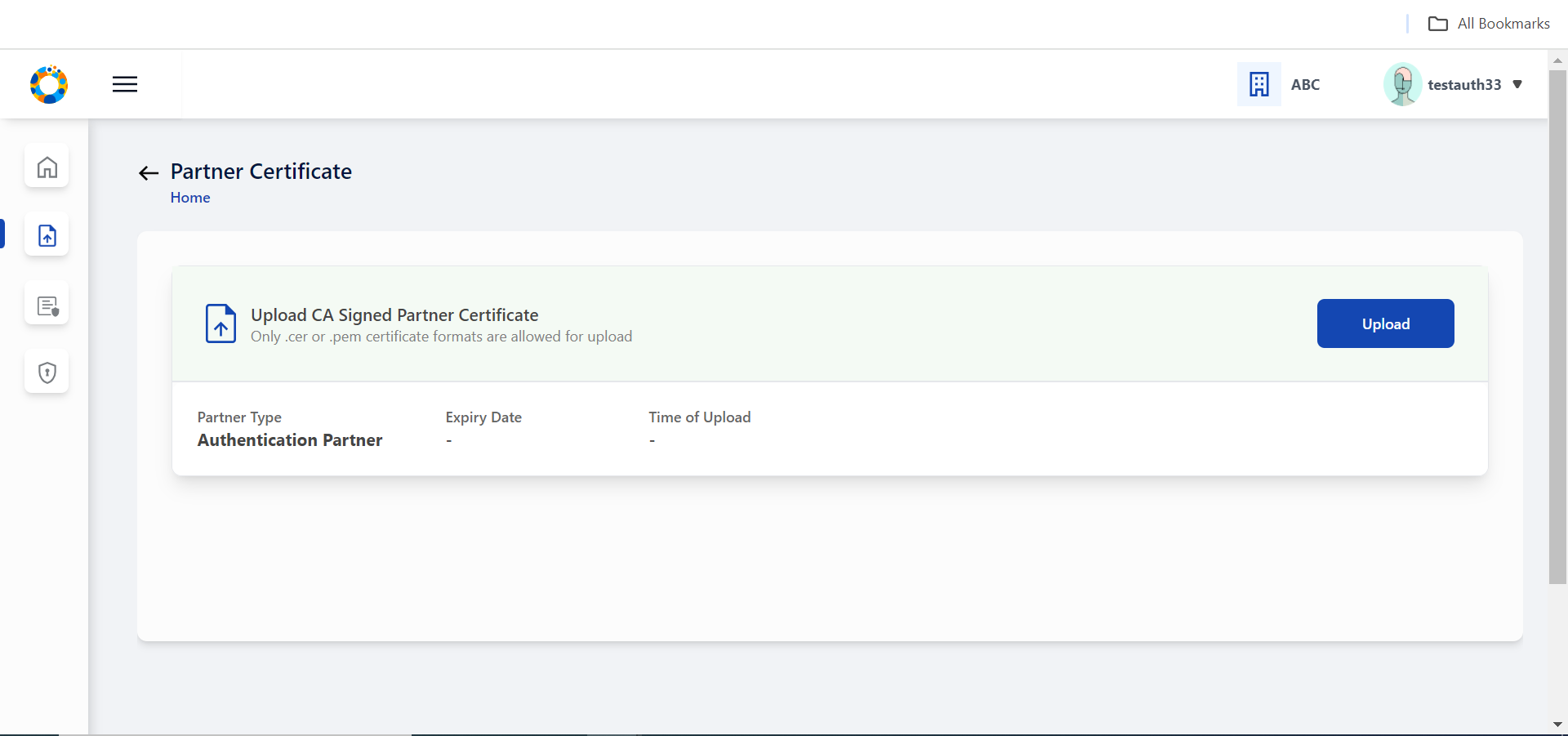
Before a Partner can upload a ‘CA Signed Certificate’ it is prerequisite that the ‘Partner Admin’ should have already had uploaded the **Root CA** and **Sub CA** certificates (From older PMP interface). {% endhint %}

#### To Upload CA signed Certificate

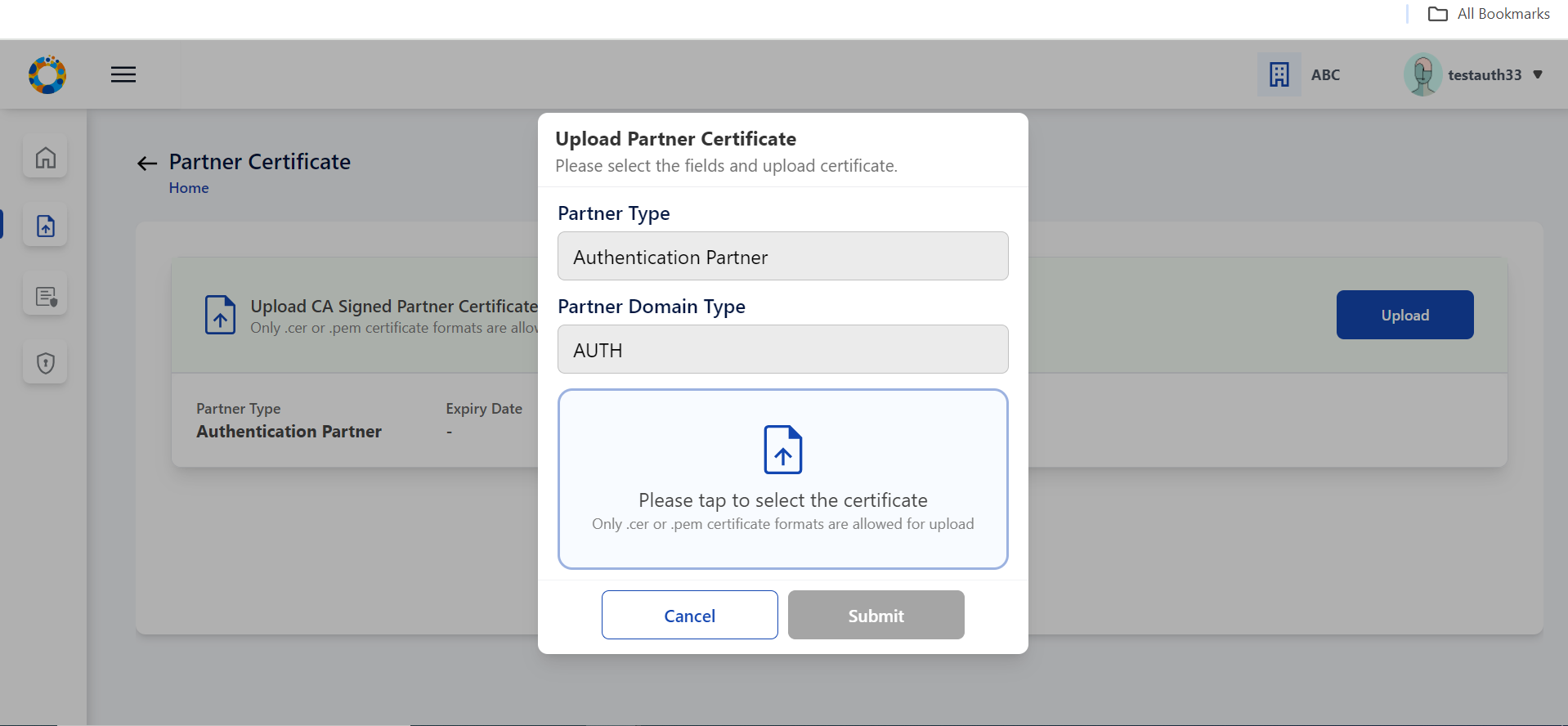
1. Go to **Authentication Partner** (New UI) -> **Dashboard.**

 ” alt=““>

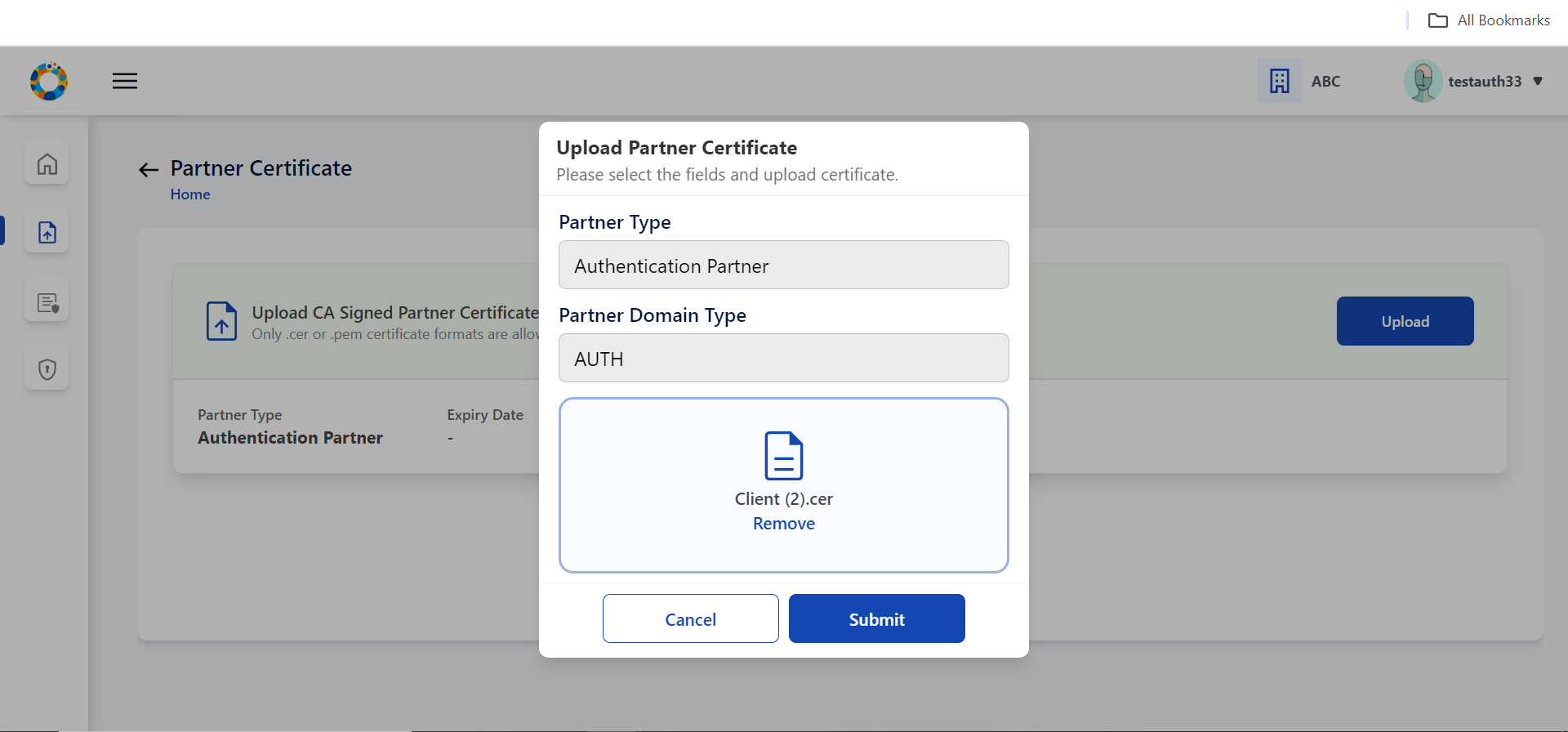
1. Click on **Partner Certificate** option, Click on the **Upload** button to upload the partner certificate signed by CA.

 ” alt=““>

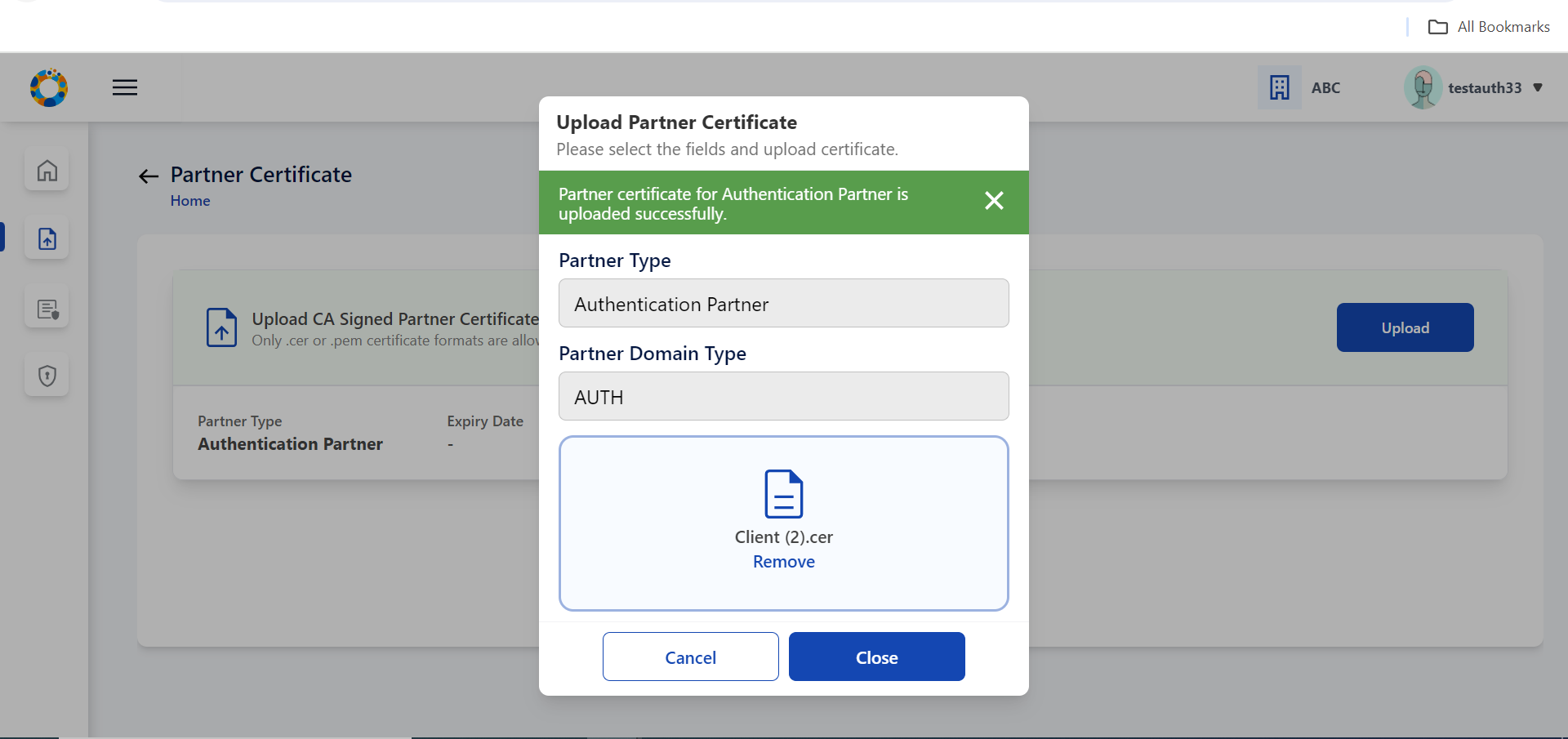
1. Select the CA signed partner certificate from local system by tapping on the upload section (blue area).

 ” alt=““>

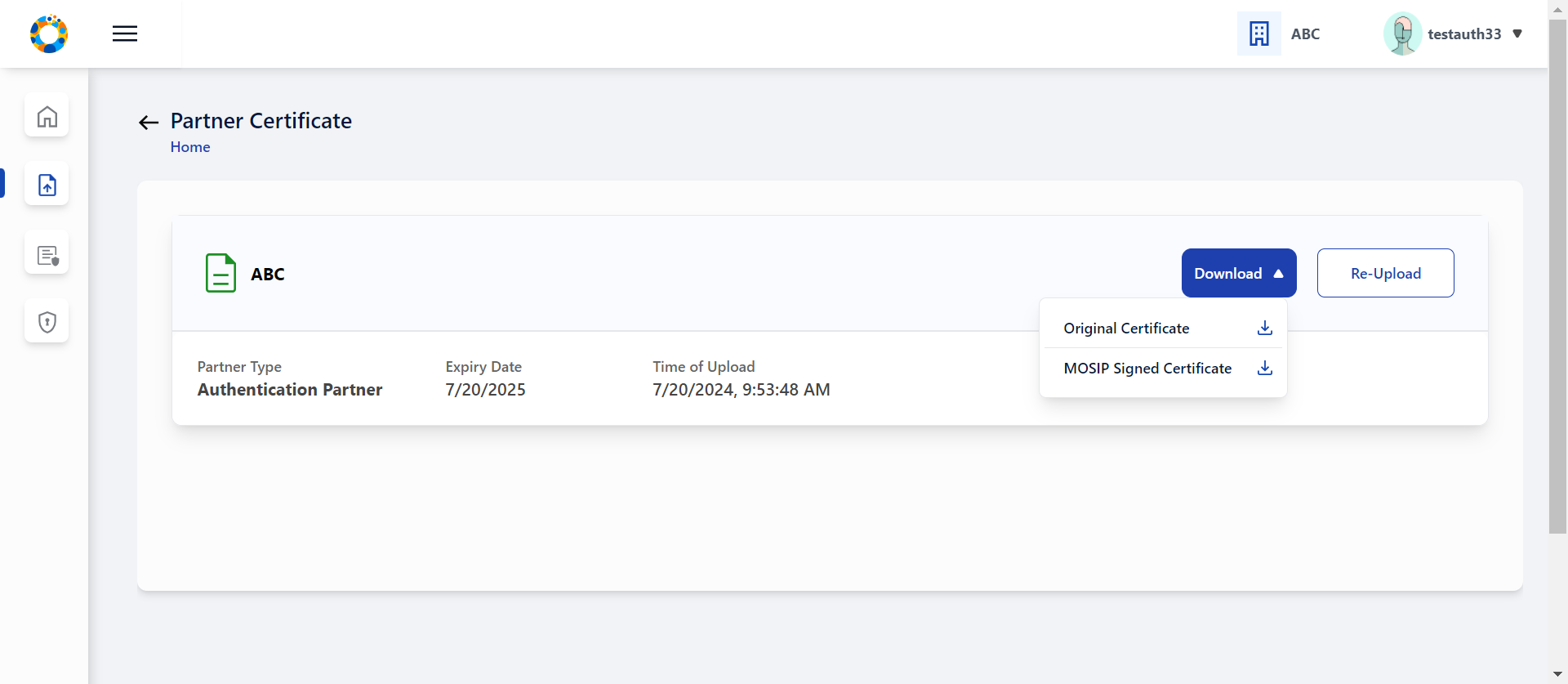
1. Certificate is successfully fetched from local system.

 ” alt=““>

1. Click on **Submit**, Partner Certificate is uploaded successfully.

 ” alt=““>

1. On closing the popup, The user can view the uploaded certificate details in the form of a list view.

 ” alt=““>

#### Download Certificate

There is also an option to download initially uploaded CA signed certificate and also the MOSIP Signed Certificate.

#### Re-Upload Certificate

Reuploading certifacte is required in cases when MOSIP Signed Certificate gets expired after one year.

{% hint style=“info” %} **Note:**

’MOSIP Signed Certifcate has a validity of 1 year from the time of Partner Certificate Upload. {% endhint %}

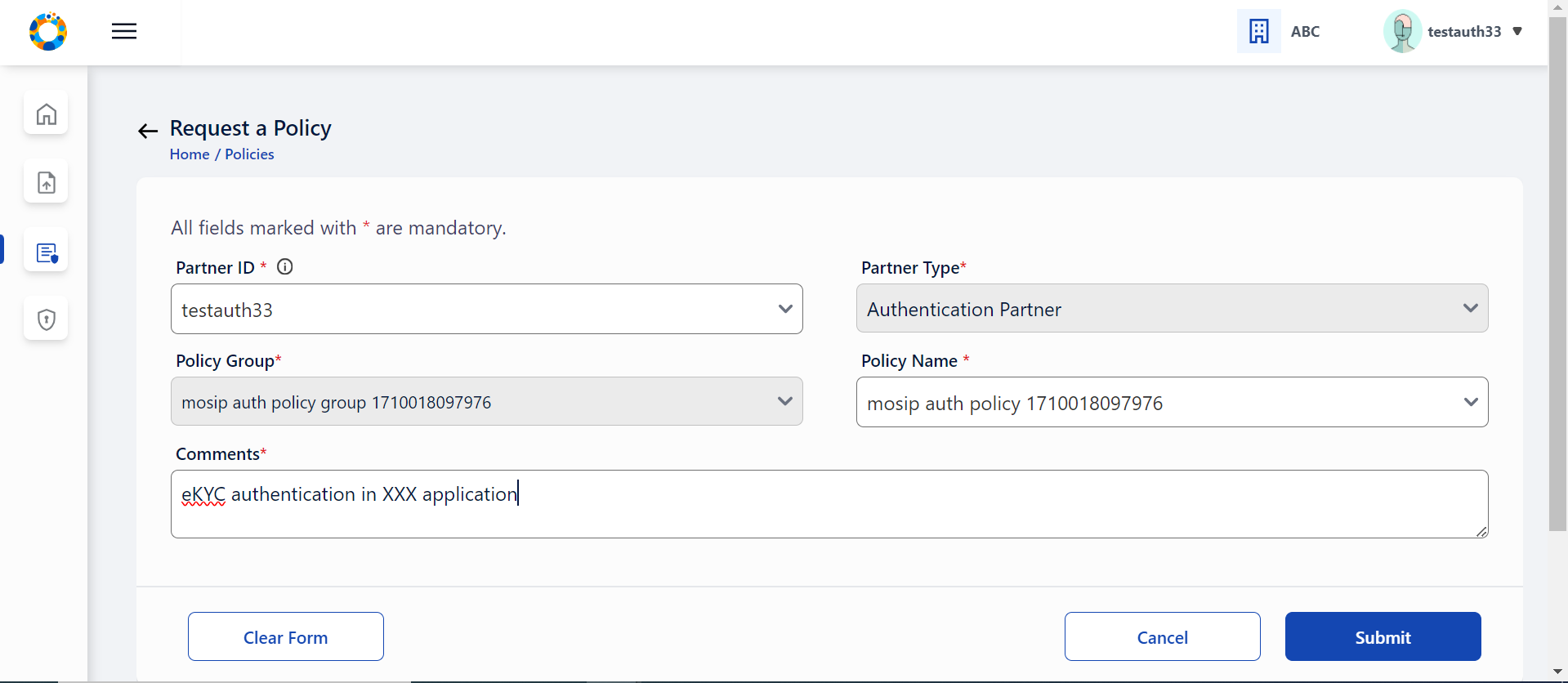
You must ensure that you re-upload the partner certificate again so that new MOSIP signed certificate can be generated and other functionalities such as Request Policy, Authentication Policies can function.

### Request Policy

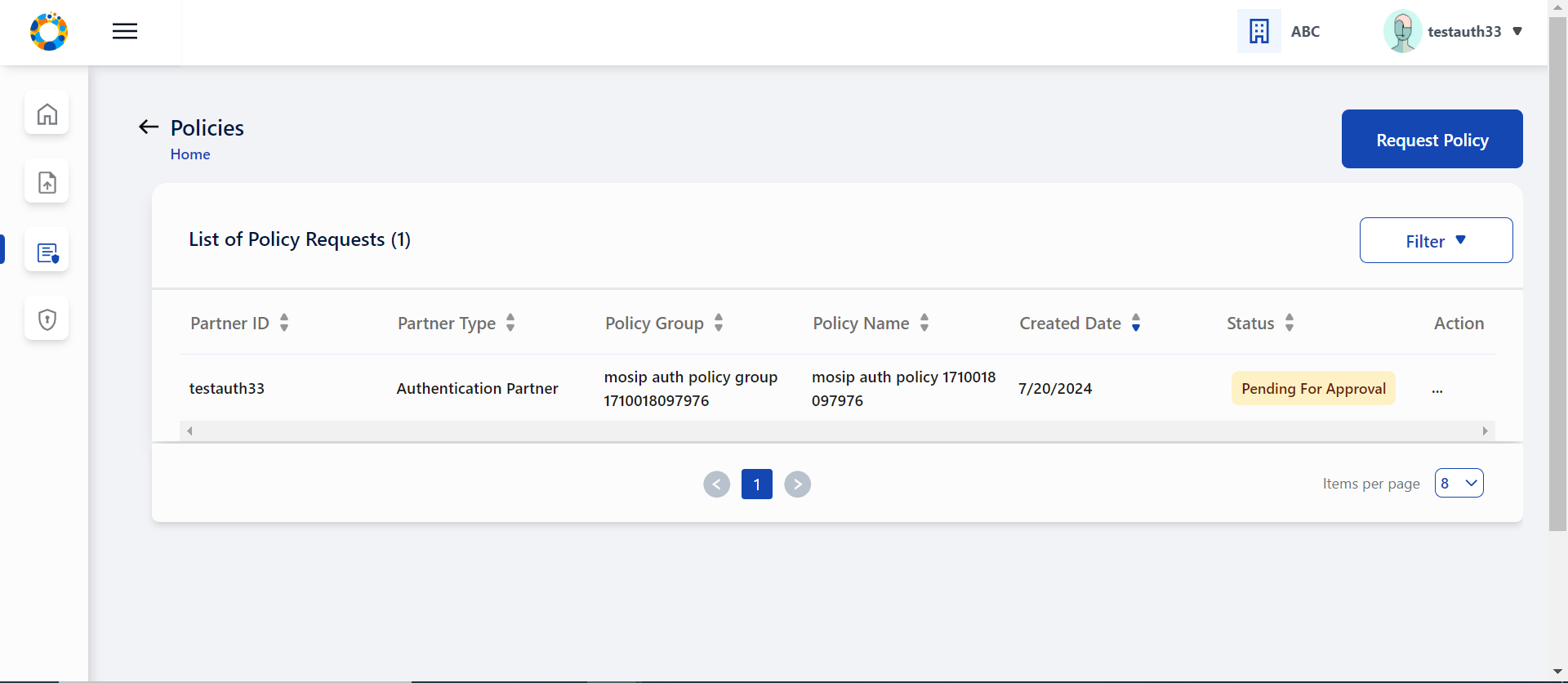
**Pre-Requisite**: **Policy Manager** (in our case ‘**Admin**’) must have created a [**Policy Group**](end-user-guide.md#create-policy-group) and then created a [**Policy**](end-user-guide.md#create-an-auth-policy) within it for the Partner to be able to ‘**Request a Policy**’.

#### To Request a Policy

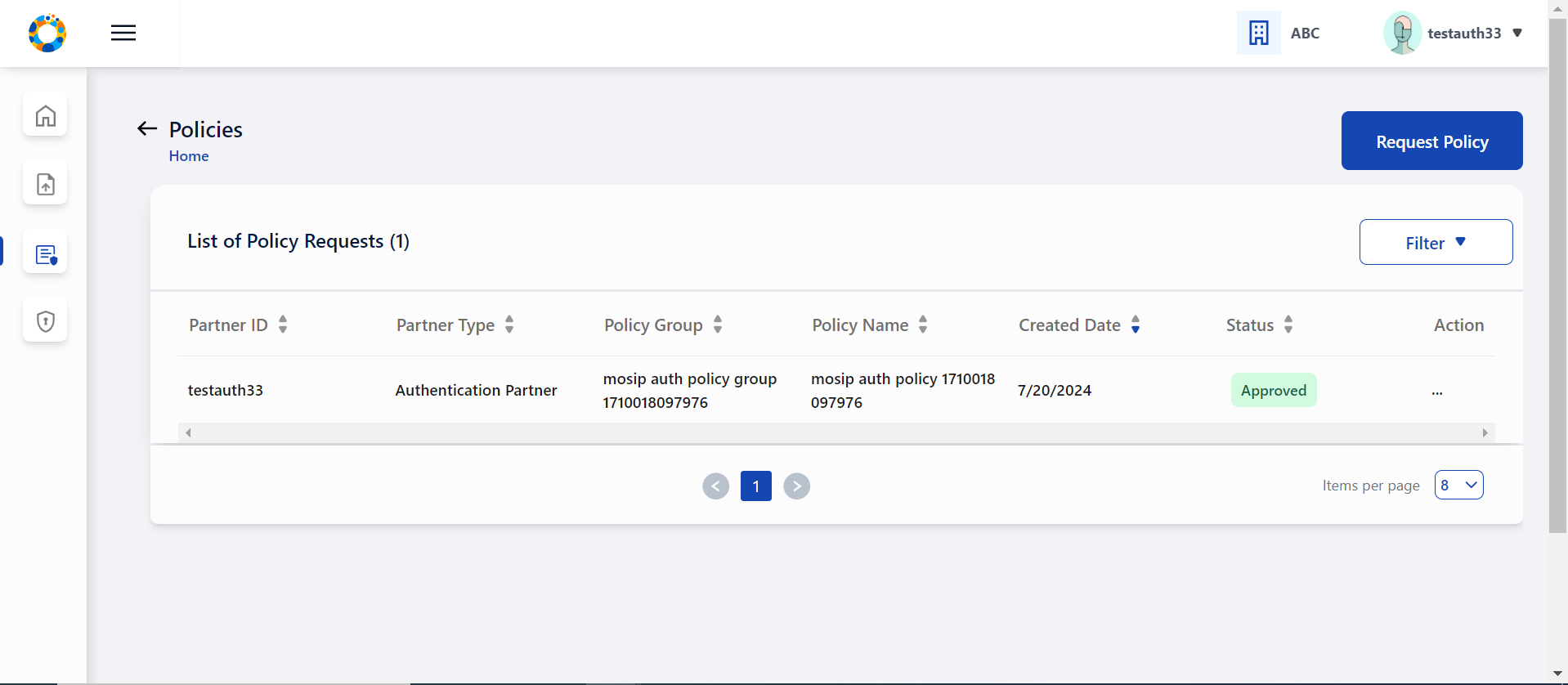
1. Click on the ‘Request Policy’ option in User homepage/dashboard.
   1. Each policy name is provided with policy description, You can make a suitable policy selection. You can provide appropriate request comments and submit the policy request details. A message conveying Policy request submitted successfully to admin is displayed.

 ” alt=““>

1. This newly created policy request will be in ‘Pending for Approval’ status. You can also click on action menu to see all the submitted policy details irrespective of its status.

 ” alt=““>

1. Once the request is approved (Partner Admin will [**Approve Policy Request**](end-user-guide.md#approve-policy-request)). Once the request is approved you can view the status turns to ‘Approved’ status.

 ” alt=““>

## Authentication Service

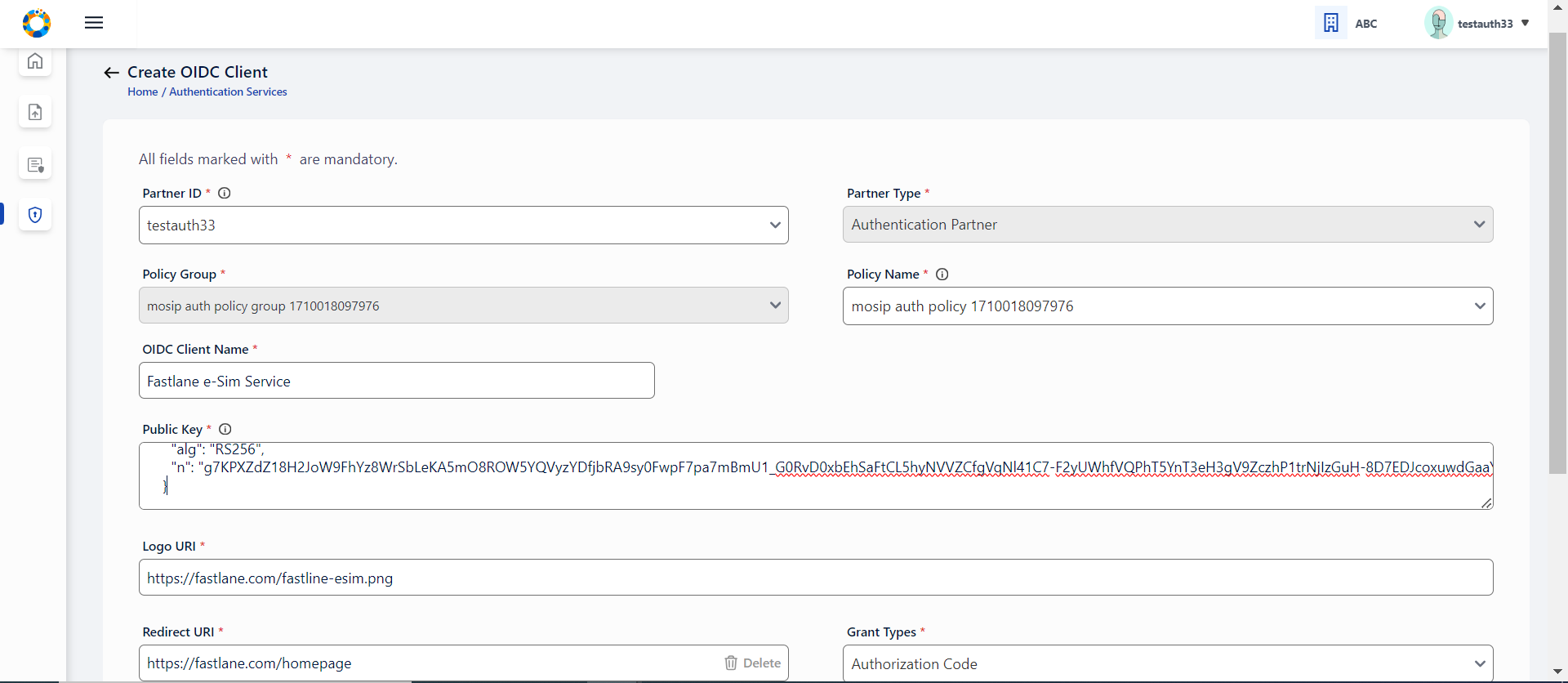
After the partner has selected a policy group, uploaded partner certificate, requested for policy and also got admin approval - partner can now perform ‘Authentication Services’:

* OIDC Client: Create OIDC Client for approved policy
* API Key : Generate API Key for approved policy

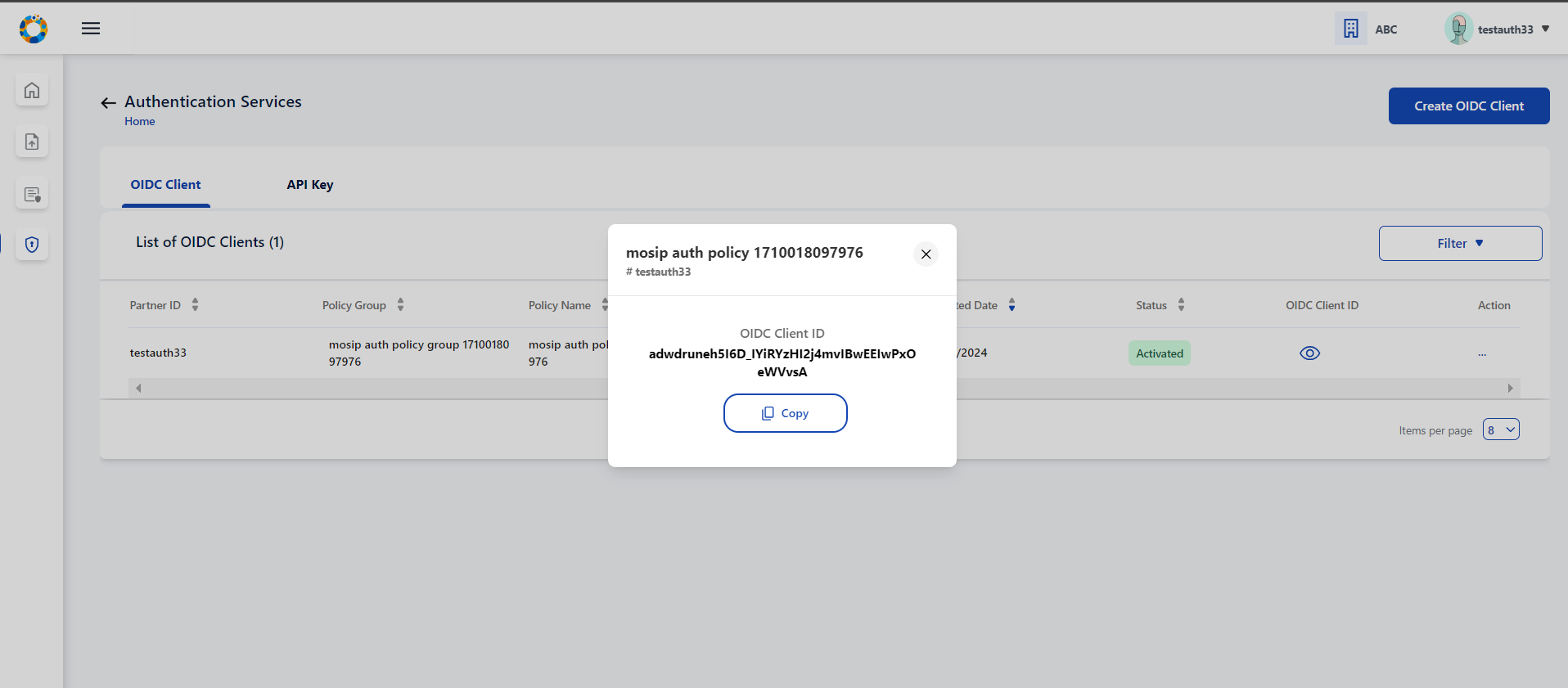
**Prerequisites**: Policy requested by the **Partner** must be already approved by **Policy Manager** (Read More [**here**](end-user-guide.md#approve-policy-request)).

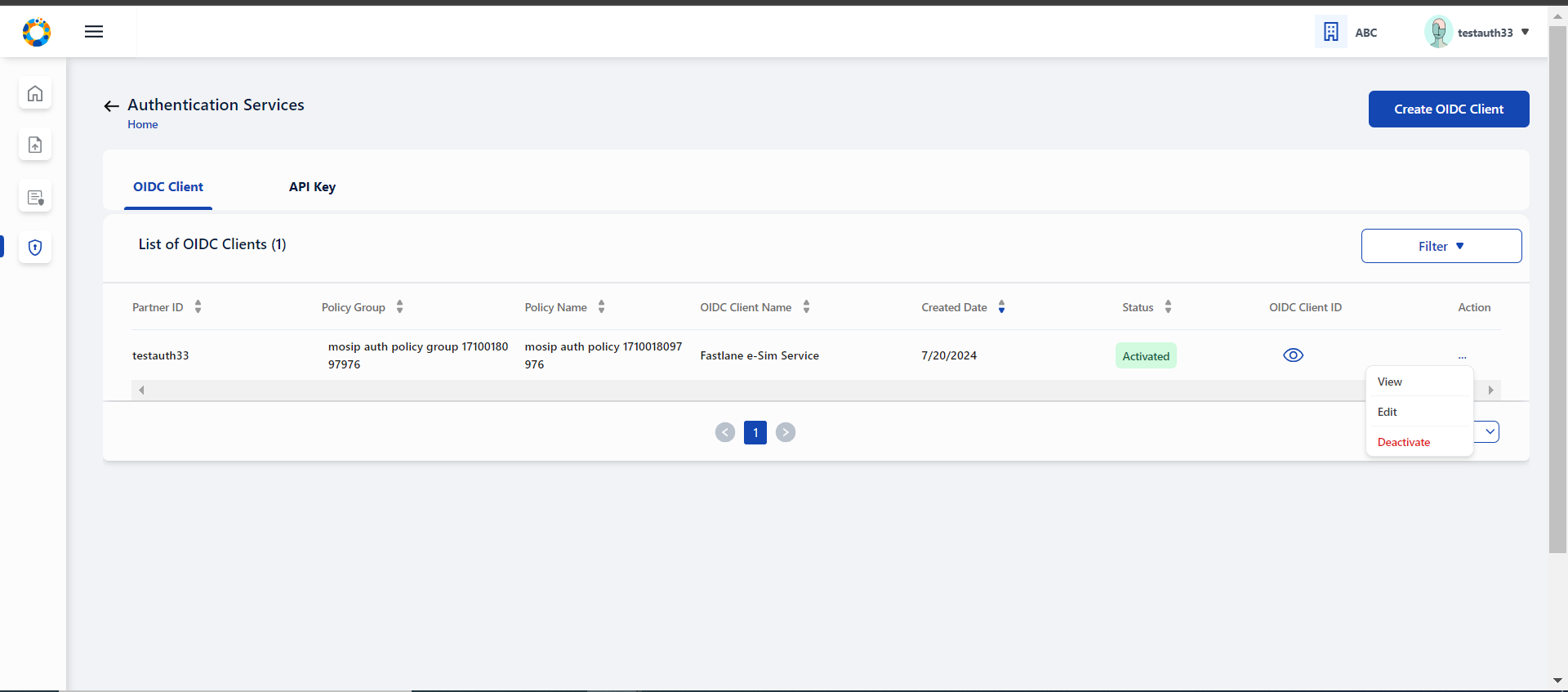
#### Creating OIDC Client

* The authentication partner needs to provide the following details to create OIDC Client
  + Select suitable Authentication policy for OIDC Client creation. Only the policies that are APPROVED by admin will be available in dropdown for selection.
  + Enter the public key in JWK format, name or label for OIDC Client, LogoURI and one or more Redirect URI.
  + On successful submission, user can find this record in tabular list of submitted OIDC Client details in ‘Activated’ status. Tabular list and individual view of submitted OIDC Client details along with OIDC Client ID, Edit OIDC Client details and Deactivate OIDC Client can also be seen from here.

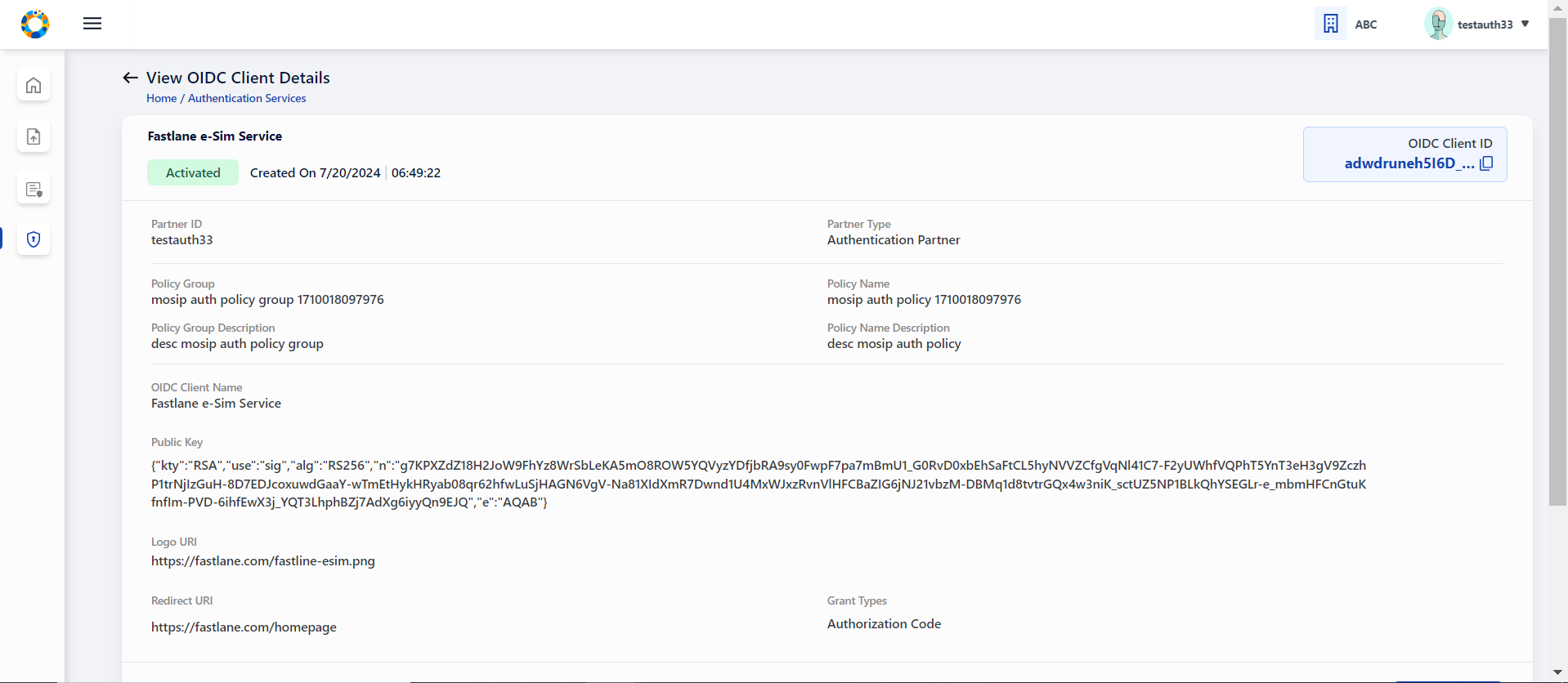
 alt=““>

* Once the details are in Activated status, user will be able to view the OIDC Client ID generated, by clicking on the eye icon  . clicking on the OIDC Client ID eye icon, opens a popup window which displays the Client ID and a copy button.
* This Client ID can then be consumed in eSignet to perform authentication. Client ID can be accessed by clicking on eye icon.
* User can utilize this OIDC Client ID to perform eSignet based authentication of citizens

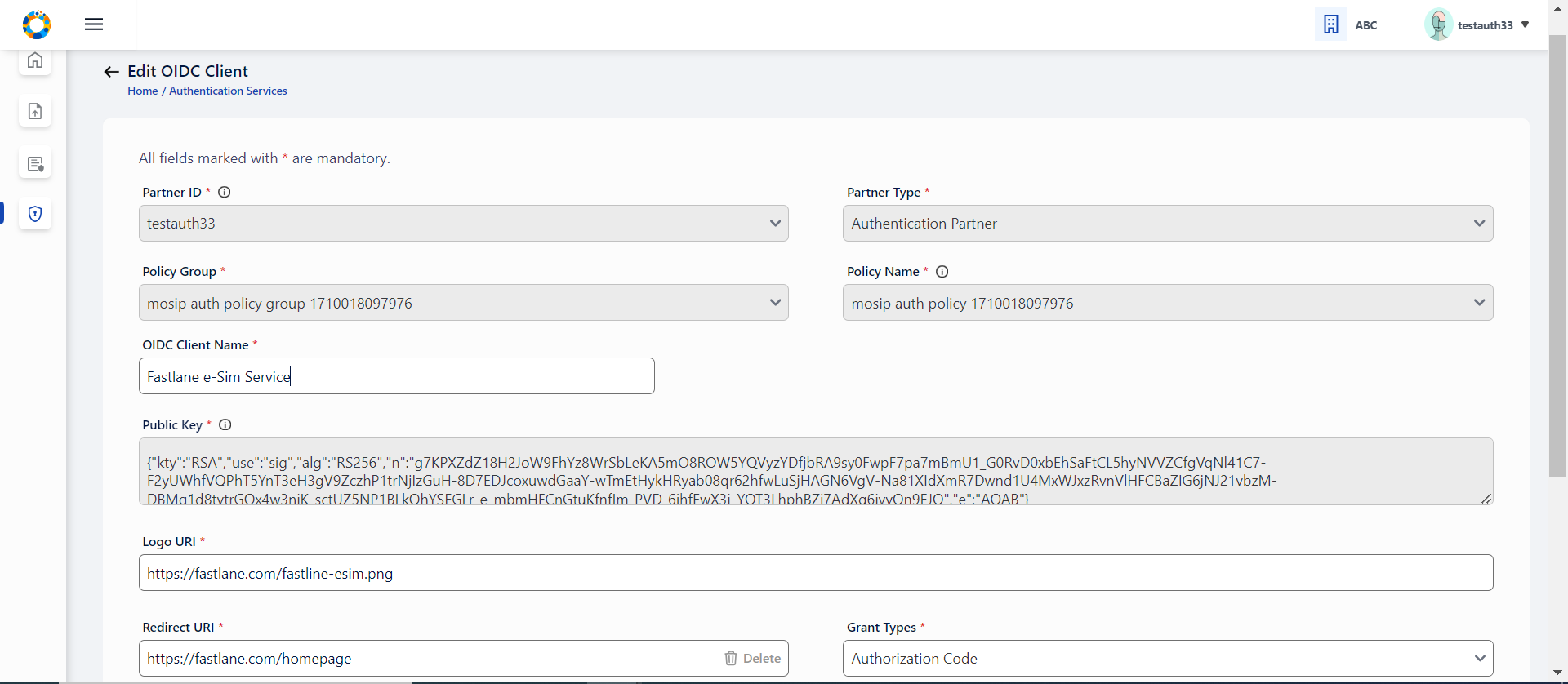
 ” alt=““>

 ” alt=““>

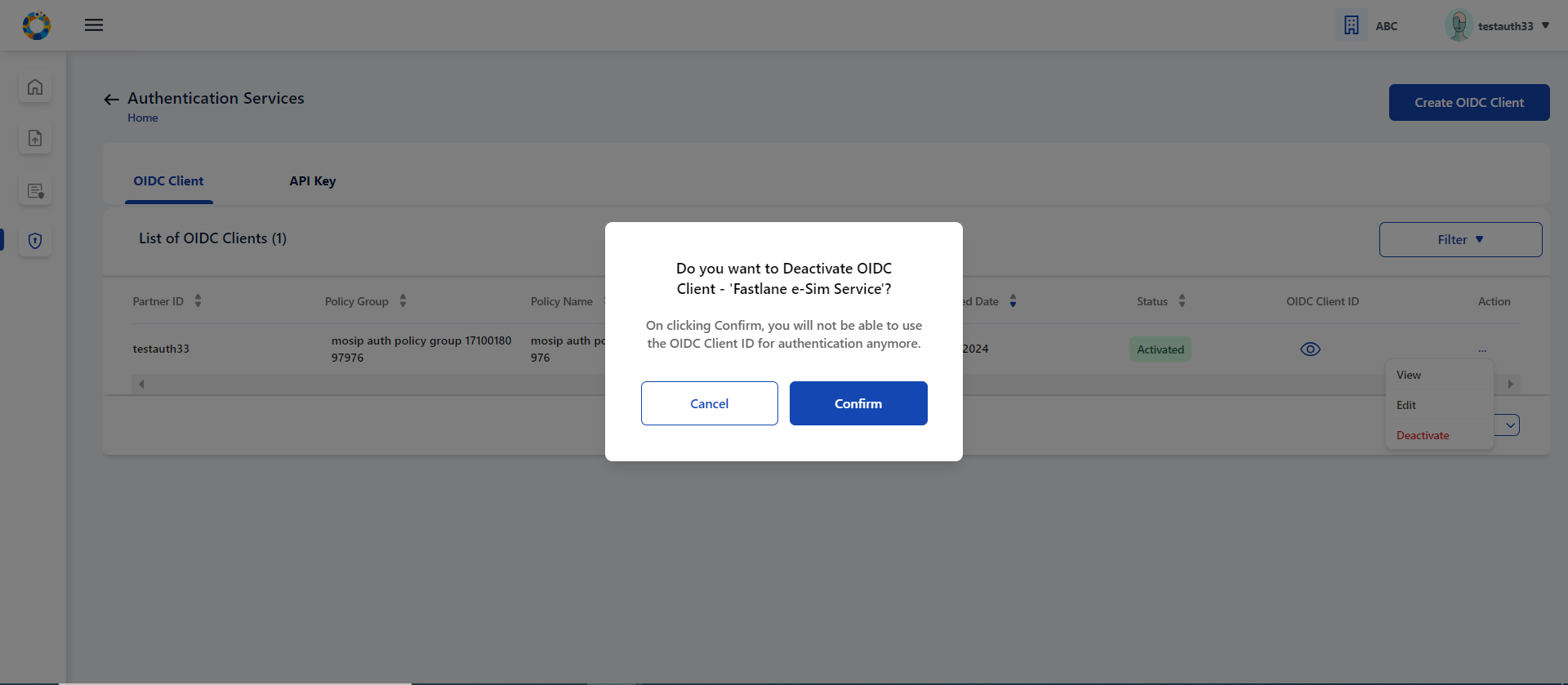
* The user can also view every OIDC Client detail individually using the View option

 ” alt=““>

* The user can also edit the OIDC Client details in Activated status (only OIDC Client Name, LogoURI and RedirectURI are editable) by selecting the edit option in Action Menu.

 ” alt=““>

* User can deactivate the OIDC Client ID by clicking on deactivate option . The deactivate popup window appears and on clicking confirm, the OIDC Client record is changed to Deactivated status. **Once deactivated, the client ID can not be used anymore for authentication**.

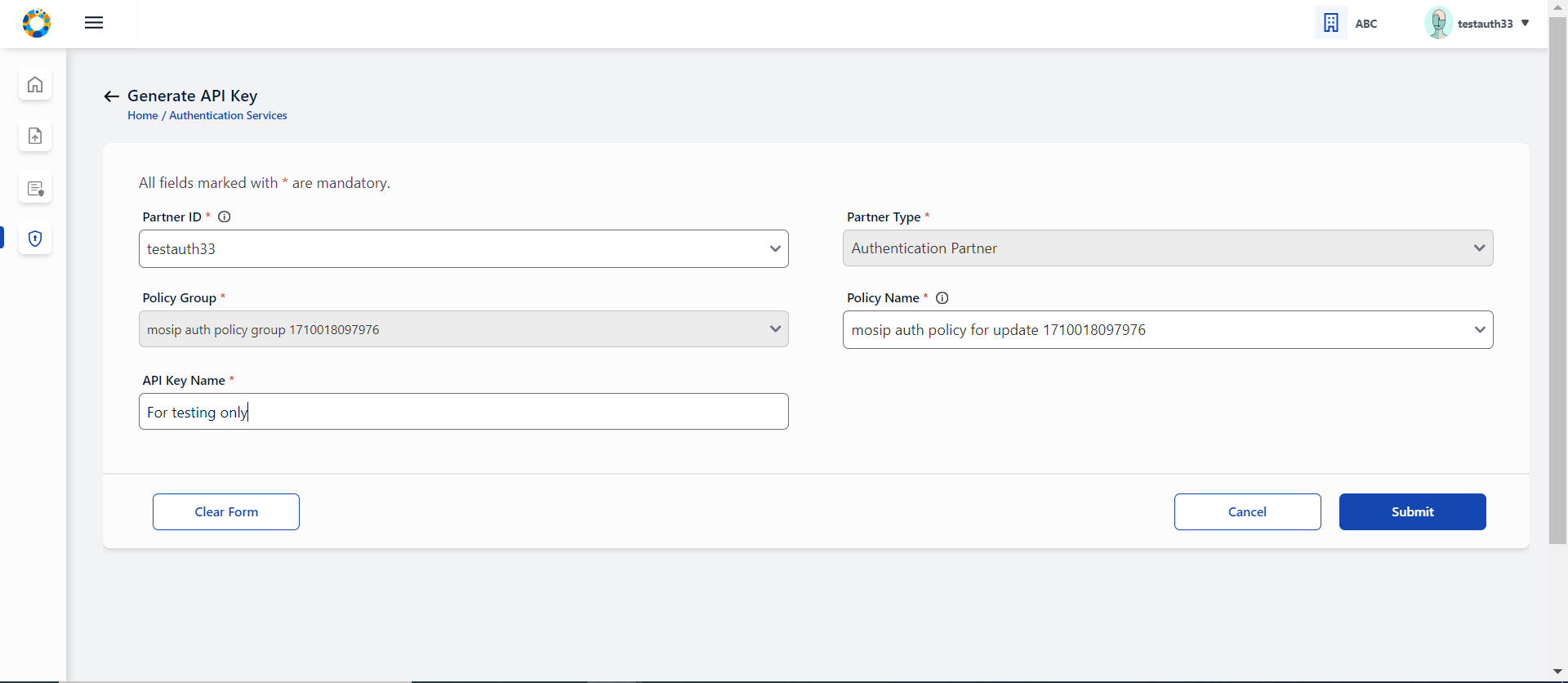
 ” alt=““>

#### API Key Generation

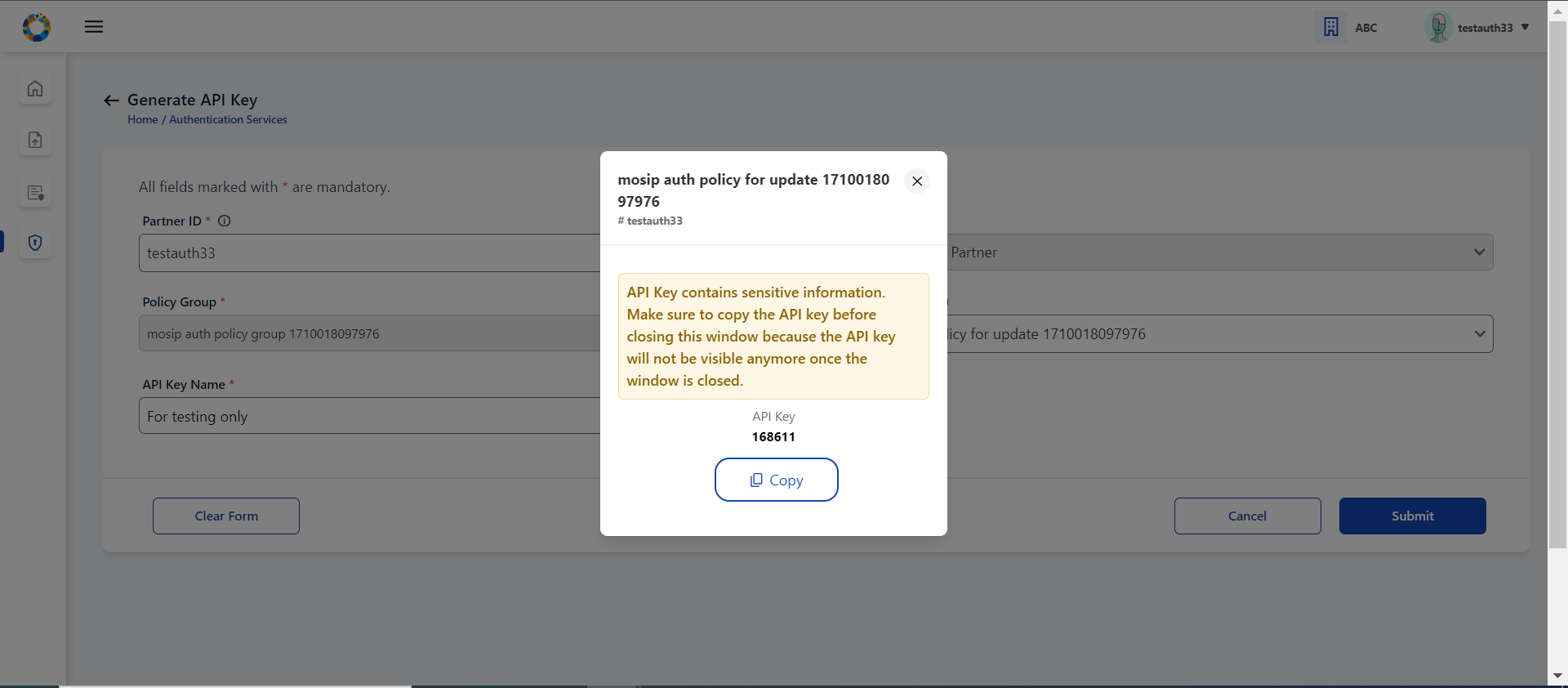
The authentication partner needs to provide the following details to generate API Key

* Select suitable Authentication policy for API Client. Only the policies that are **Approved** by admin will be available in dropdown for selection.

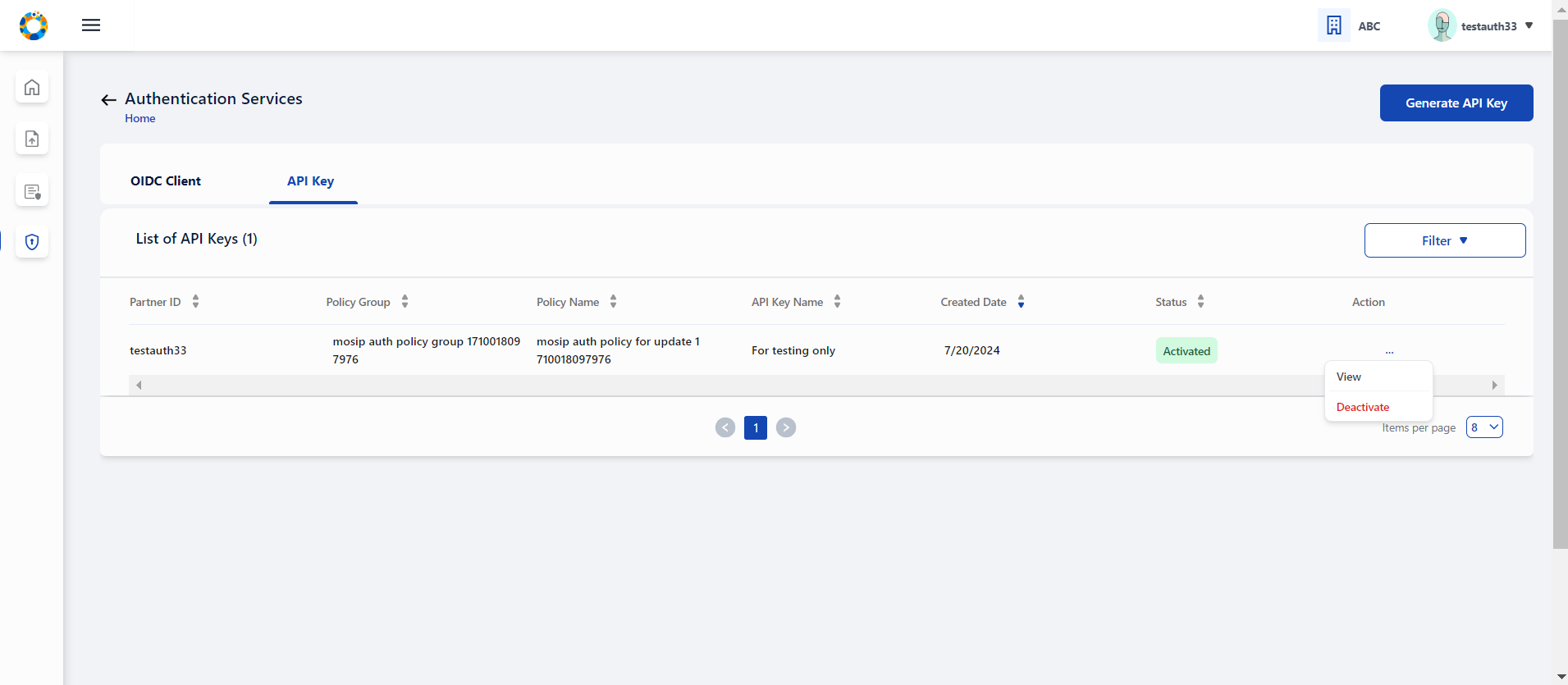
1. Enter an appropriate name or label for API Key to be generated and submit, On successful submission, a popup window displays API Key along with a copy button.

 ” alt=““>

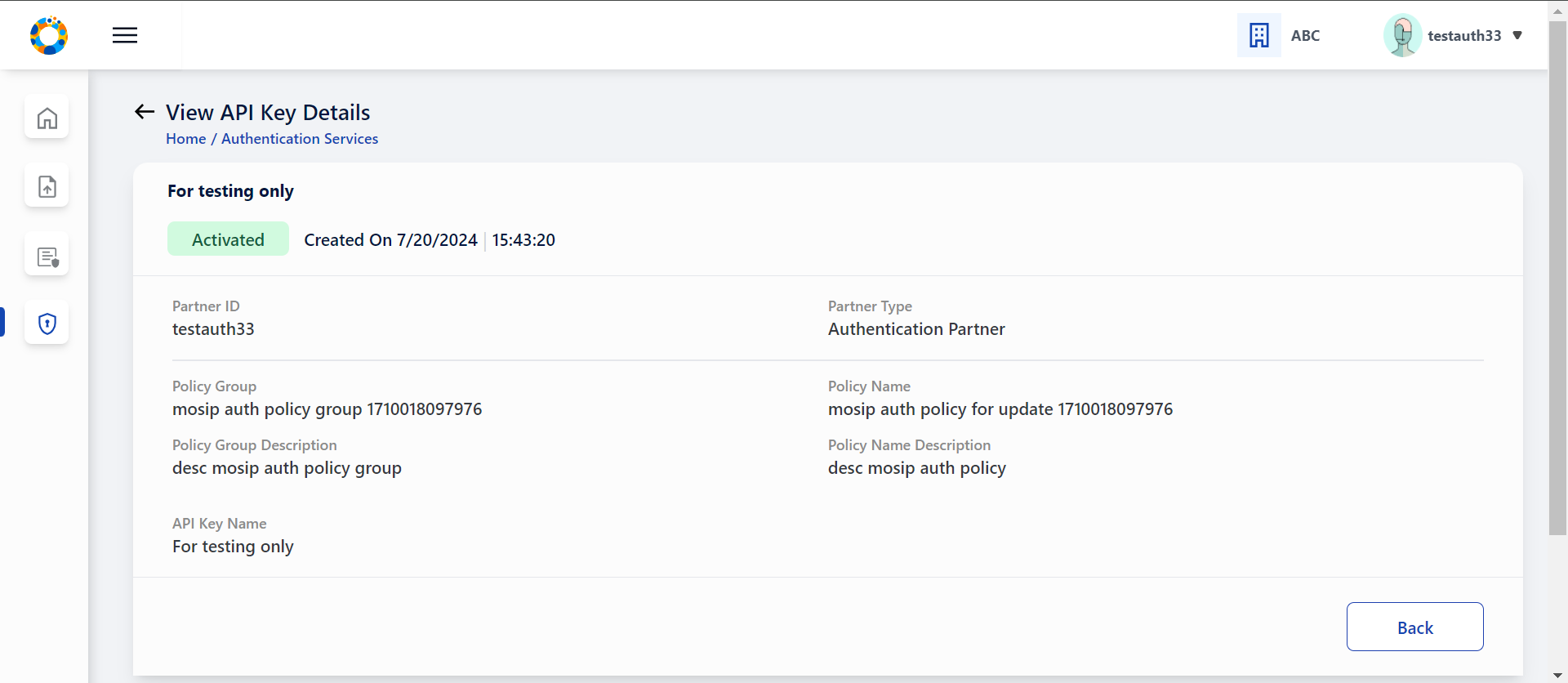
1. This API Key can be viewed by user in PMS application only once due to security reasons, hence the user is well notified with an appropriate message in the same API Key popup window to avoid closing the window unless user has not copied the API Key.\

*  ” alt=““>

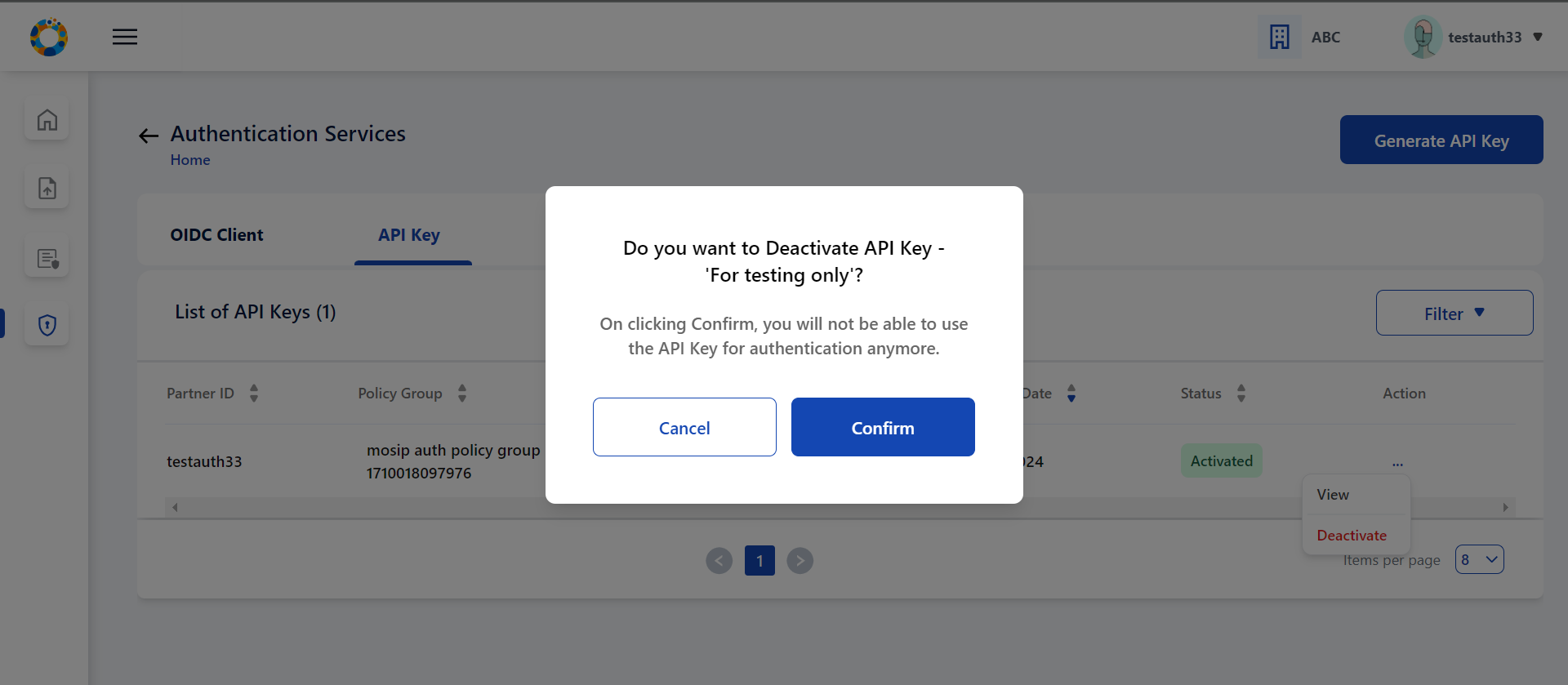
1. User can find this record in tabular list of submitted API details in ‘Activated’ status.

*  ” alt=““>

1. User can either view individual API Key entries or view the consolidated list in tabular view.

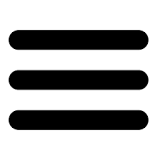
 ” alt=““>

1. You also have an option to deactivate an API Key, which thereafter cannot be used for authentication. On clicking confirm, the API Key record is changed to Deactivated status. Once deactivated, it cannot be activated again. You may need to generate a new API key as per requirement.

 ” alt=““>

## Interface Overview

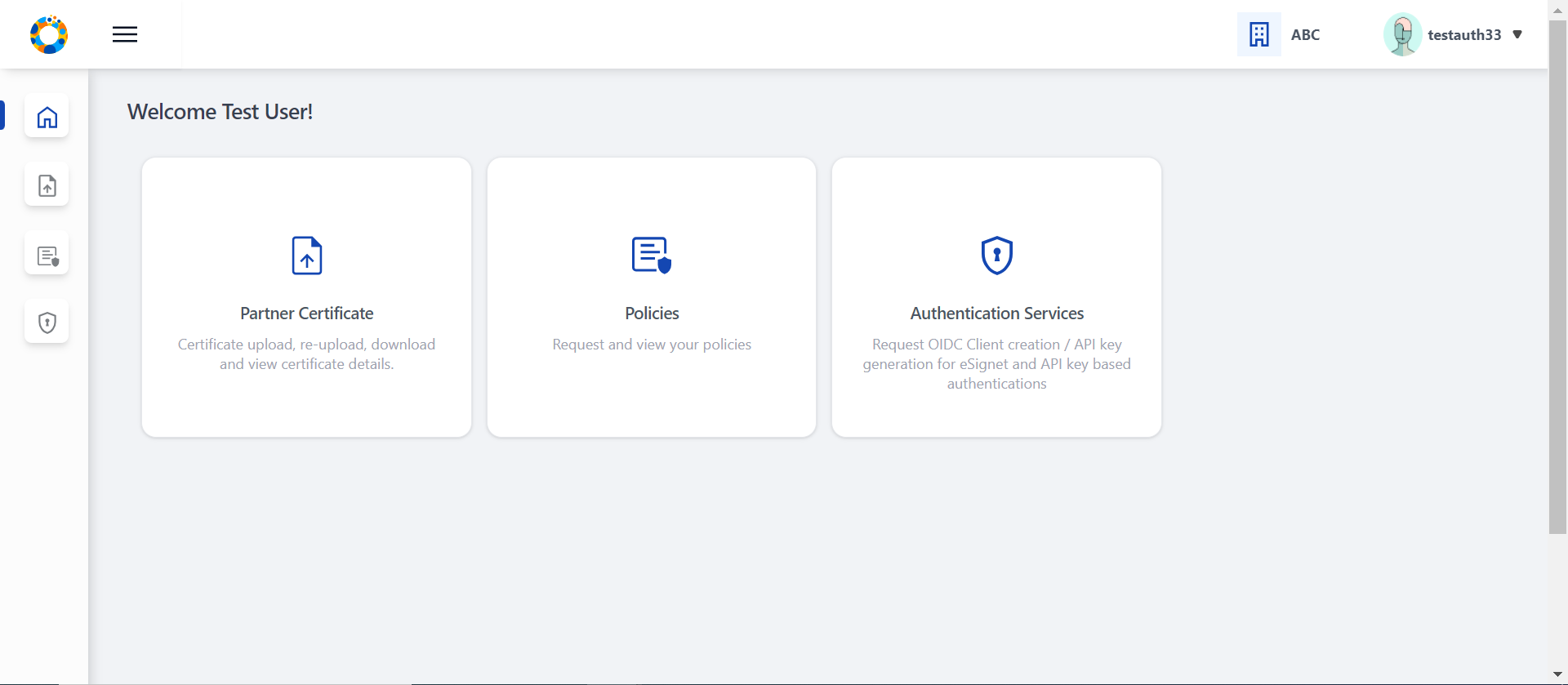
PMP (Partner Management Portal) is going under a comprehensive overhaul. This revamp includes improving usability and elevate the overall user experience (UX). The focus is to bring user centered design to PMP, make the PMP more intuitive, efficient, and aligned with our partners’ evolving needs.

The PMP Interface ‘Card View’ for ‘Authentication Partner’ presents you with following features, These features can also be accessed by clicking on side panel (in the form of icons) or expanding the hamburger menu (  on the top left which is available across all screens of PMP to help user to easily navigate.

Card view presentation is there for each functionality with brief description to help you understand the services offered in Partner User Dashboard.

After successfully registering you can access the Home Page / Dashboard. You will be able to view the features and functionalities on the dashboardand based on your Partner Type.

Note: You can access the partner dashboard only when you are duly registered and have selected the ‘Policy Group’.

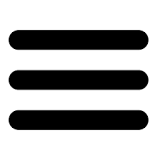
 ” alt=““>

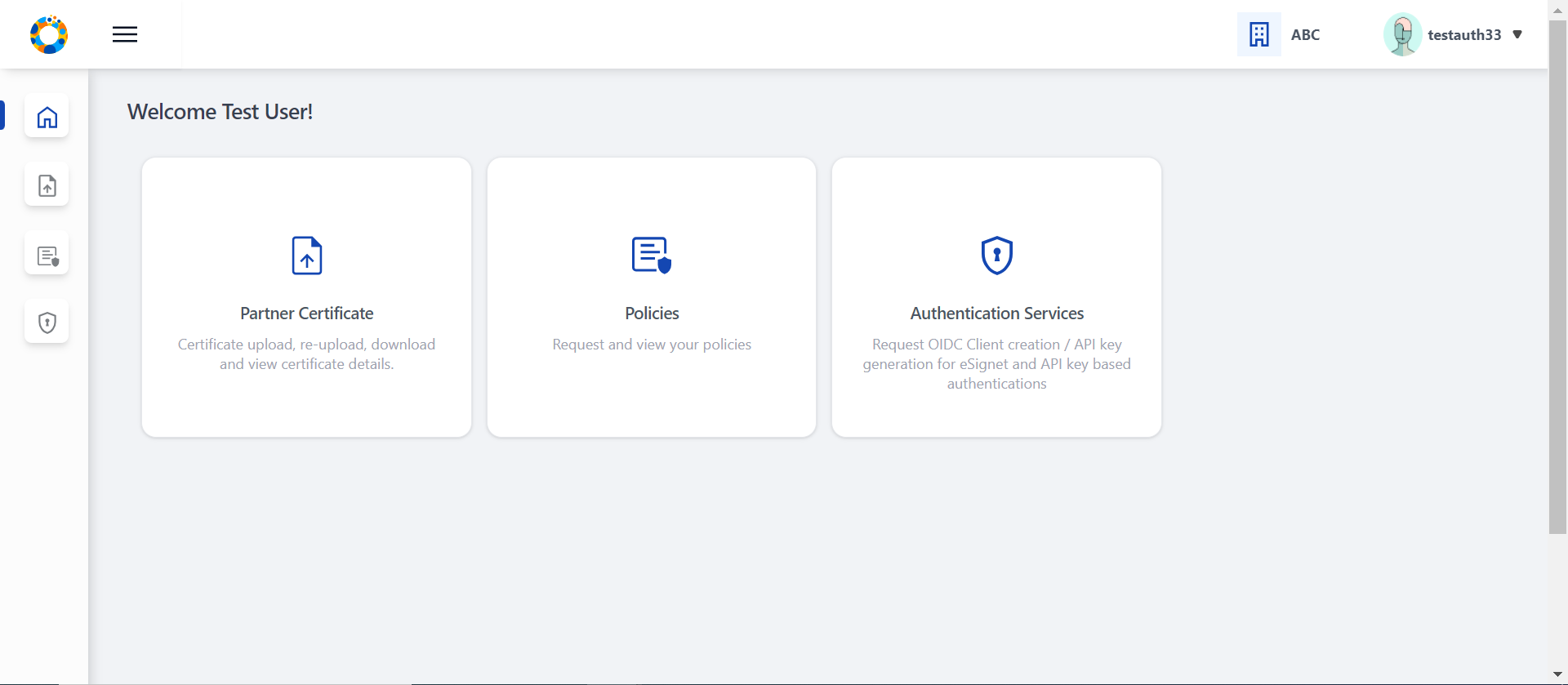
Each functionality that the user can perform is displayed in each card so that there is independent navigation for each tasks.

* Partner Certificate: Upload or Reupload CA Signed Partner Certificate and Download CA Signed Partner Certificate & corresponding MOSIP Signed Certificate
* Policies: Request for a policy within the selected policy group, tabular list of requested policies along with status of admin approval, view requested policy details along with admin comments/status.
* Authentication Services:
  + OIDC Client : Create OIDC Client for approved policy, tabular list and individual view of submitted OIDC Client details along with OIDC Client ID, Edit OIDC Client details and Deactivate OIDC Client
  + API Key : Generate API Key for approved policy, tabular list and individual view of submitted API Key details and Deactivate API Key.

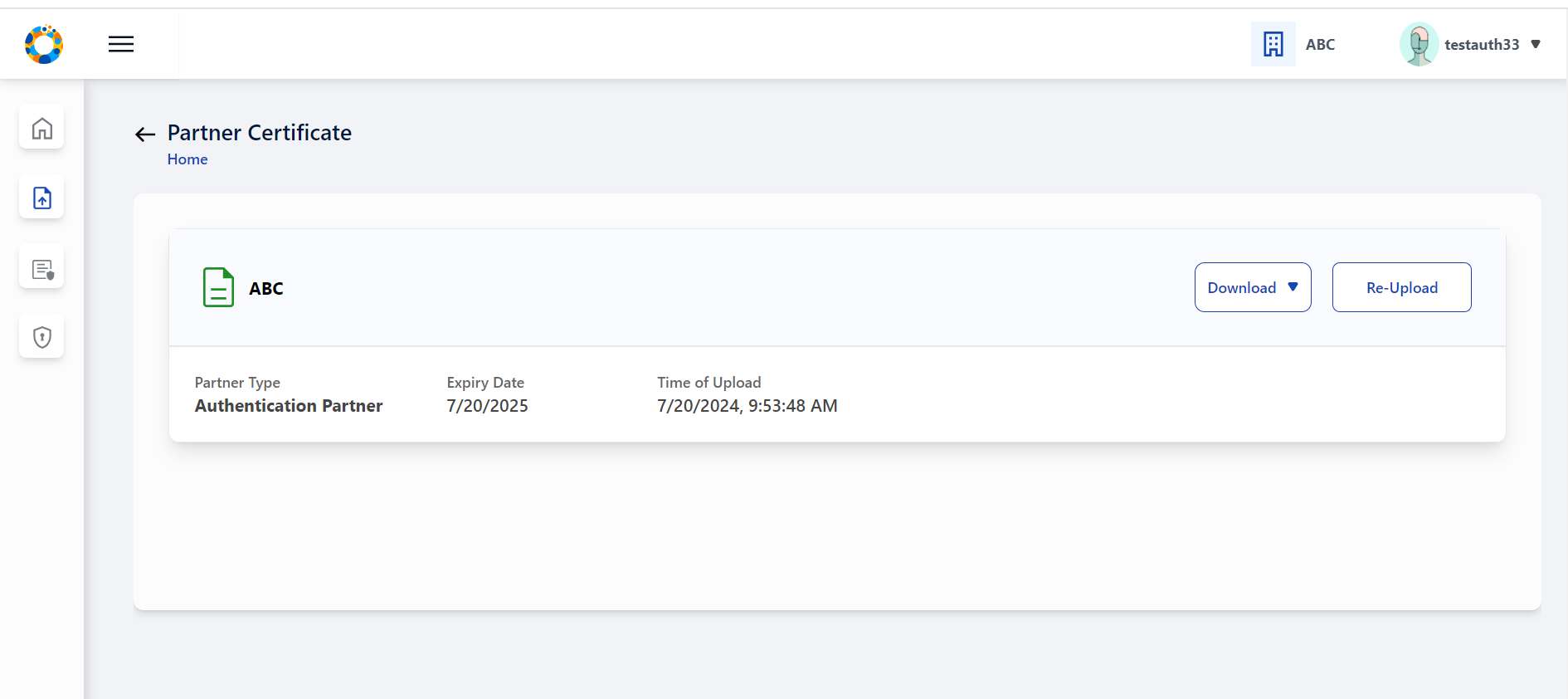
You can view your organisation name and username on the top right called ‘User Profile’, logout options is also placed here only.

## Reupload a new partner certificate through the following steps

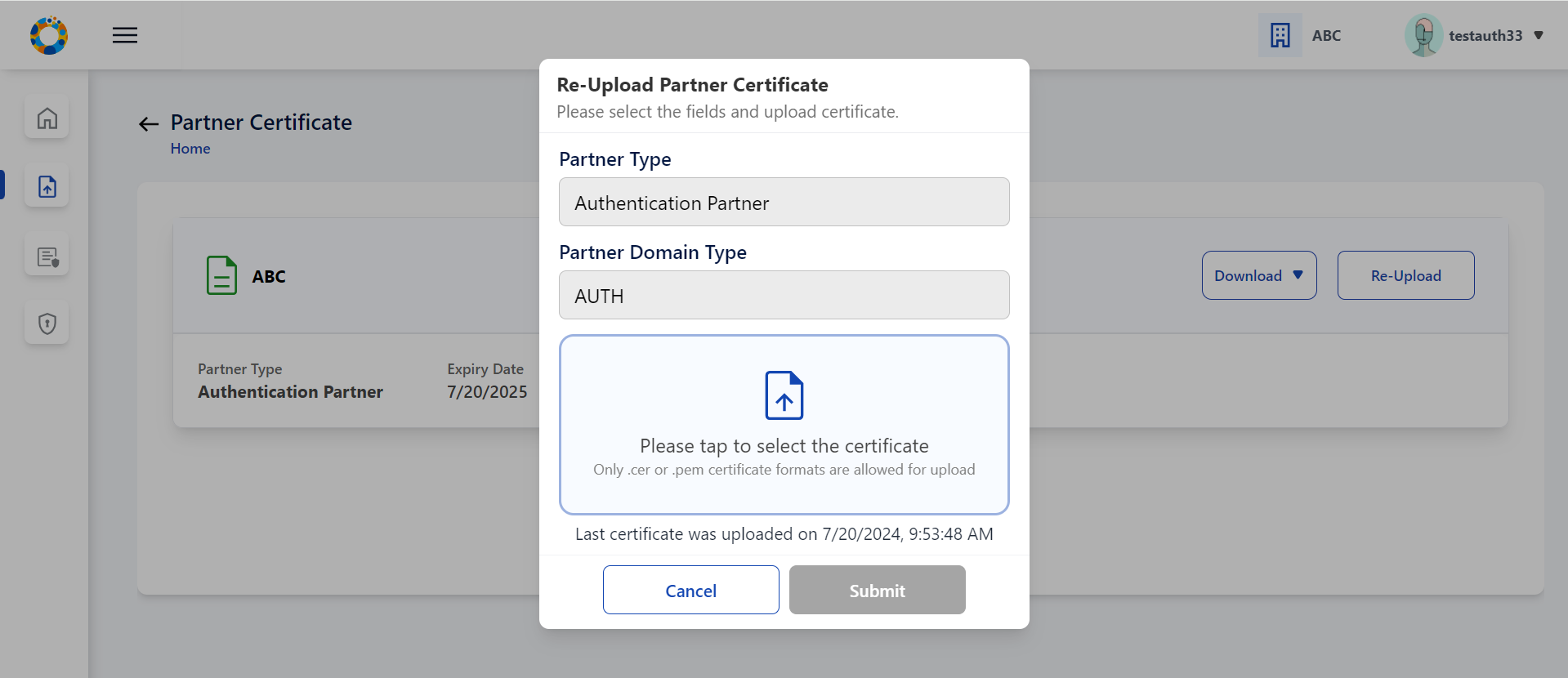
1. Login to PMP and Go to Dashboard.
2. Click on Partner Certificate option in the dashboard / side panel / hamburger menu , you will be redirected to list view of partner certificate.

 alt=““>

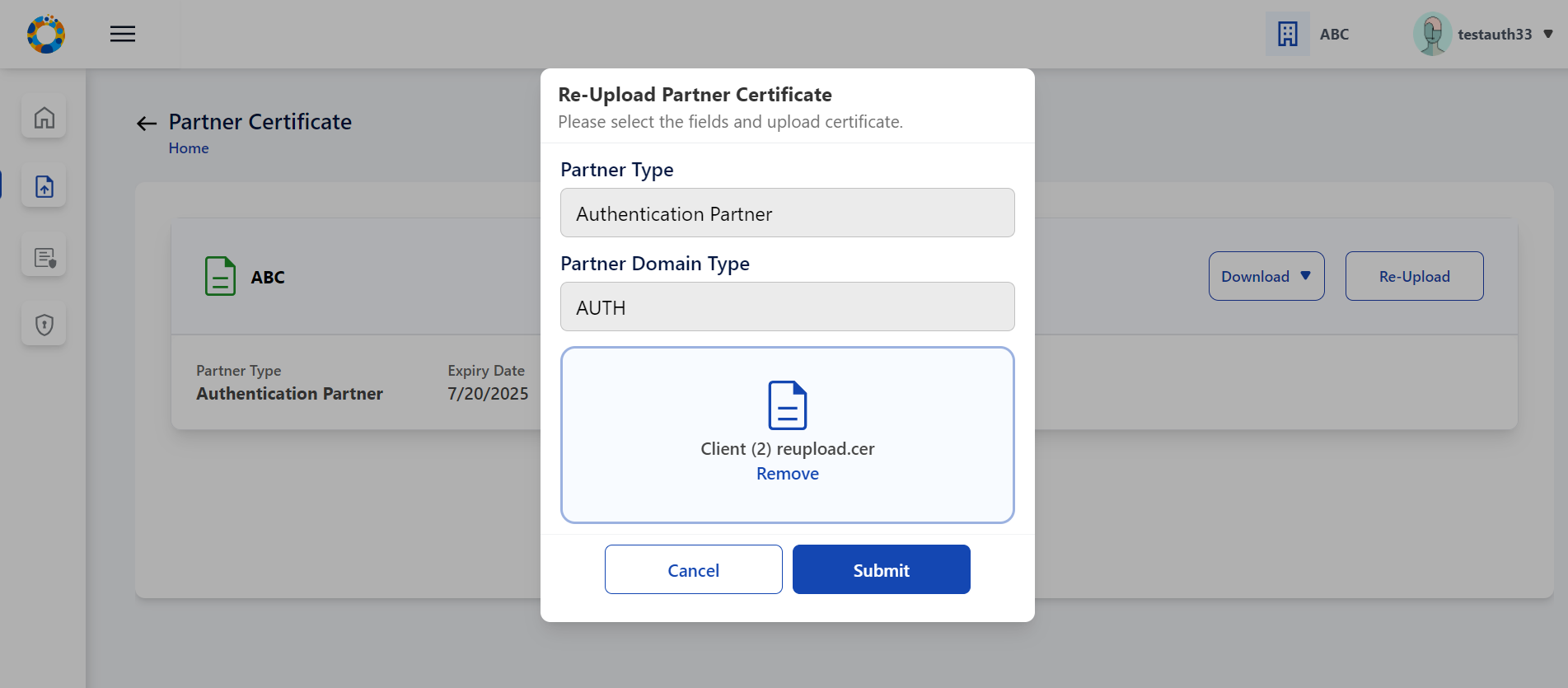
1. Click on Re-Upload button of Authentication Partner Type.

 alt=““>

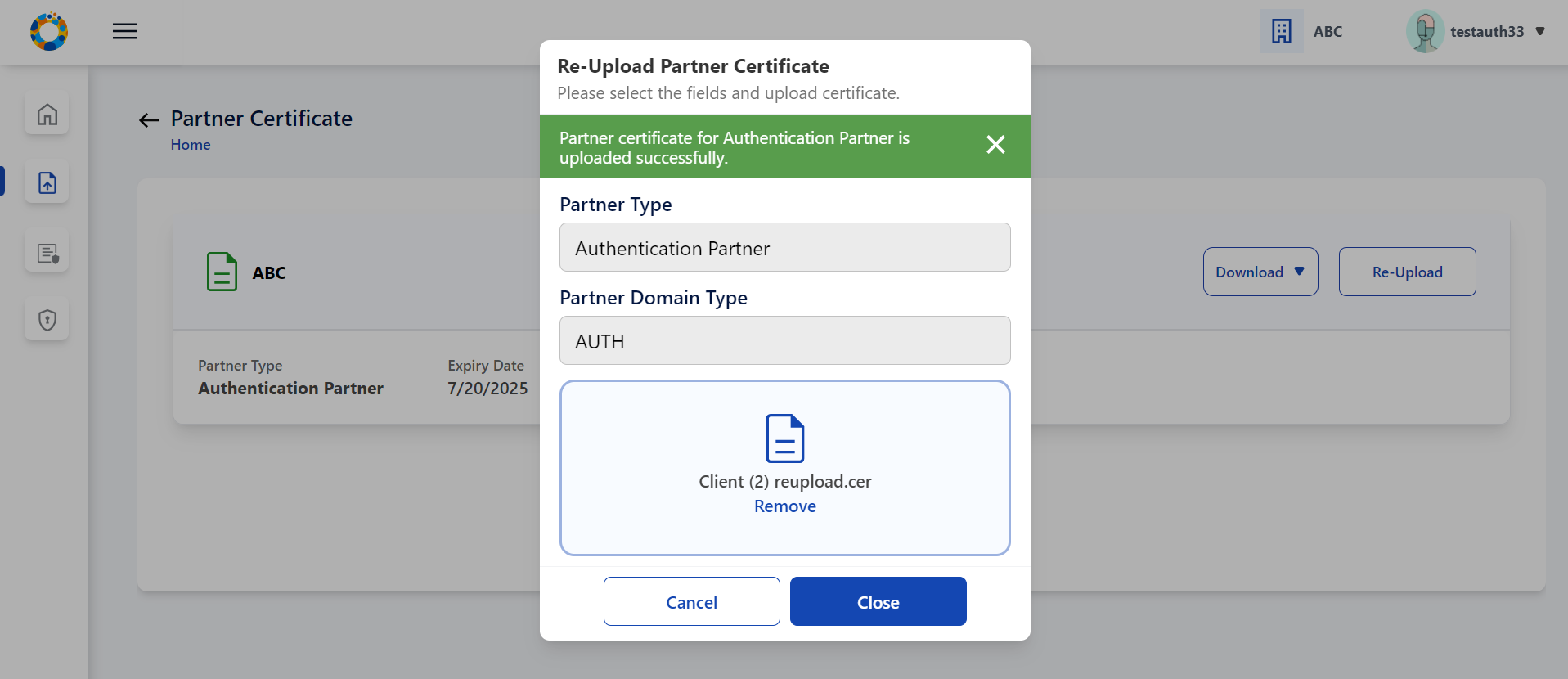
1. Re-upload certificate pop-up window appears. The time and date of previous certificate upload is also displayed for user reference. Click on the certificate upload section (blue area) to upload a new partner certificate from the local system.

 ” alt=““>

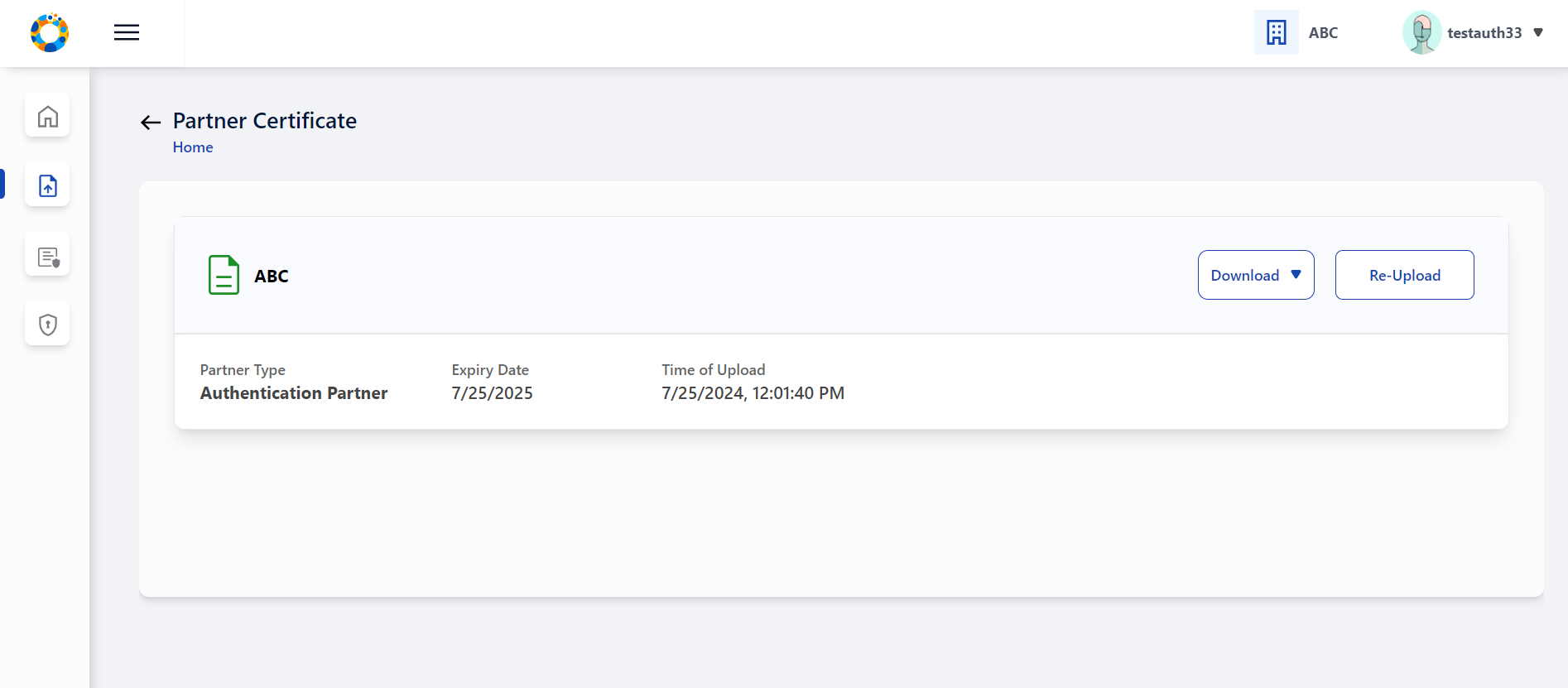
1. After selecting the certificate from local system, the fetched certificate name is displayed.

 ” alt=““>

1. Click on Submit, Partner certificate upload success message is displayed.

 ” alt=““>

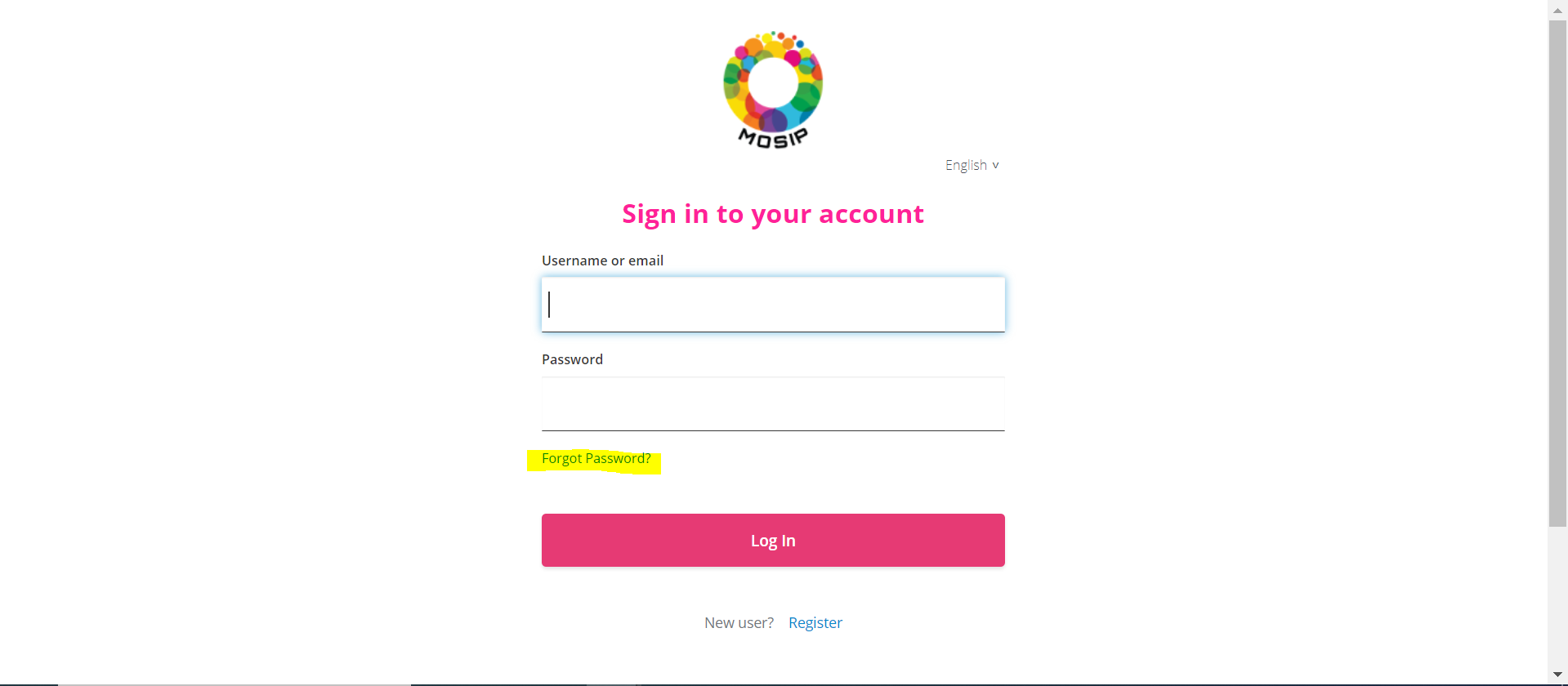
1. Click on Close to come back to list view of partner certificate.

 ” alt=““>

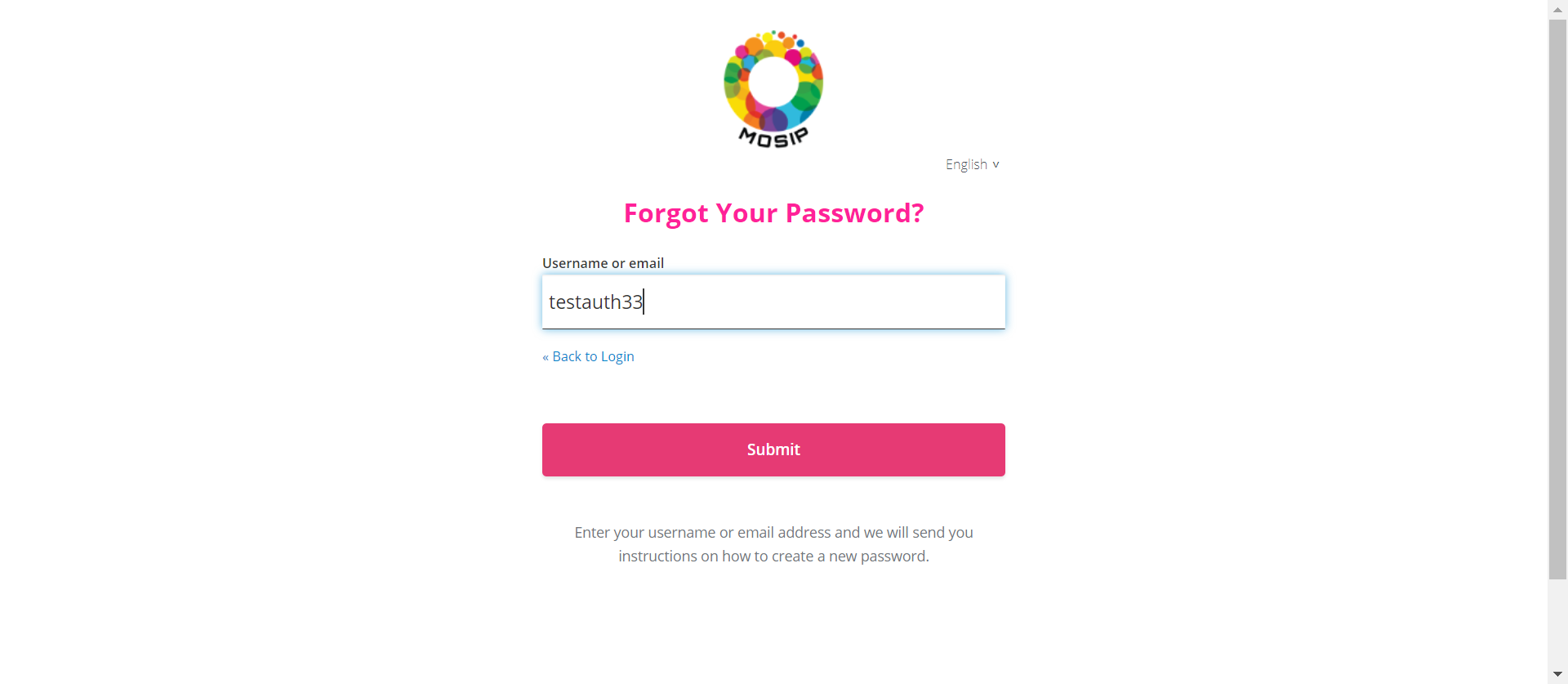
### Forgot Password

You can retrieve password in case you are unable to recall.

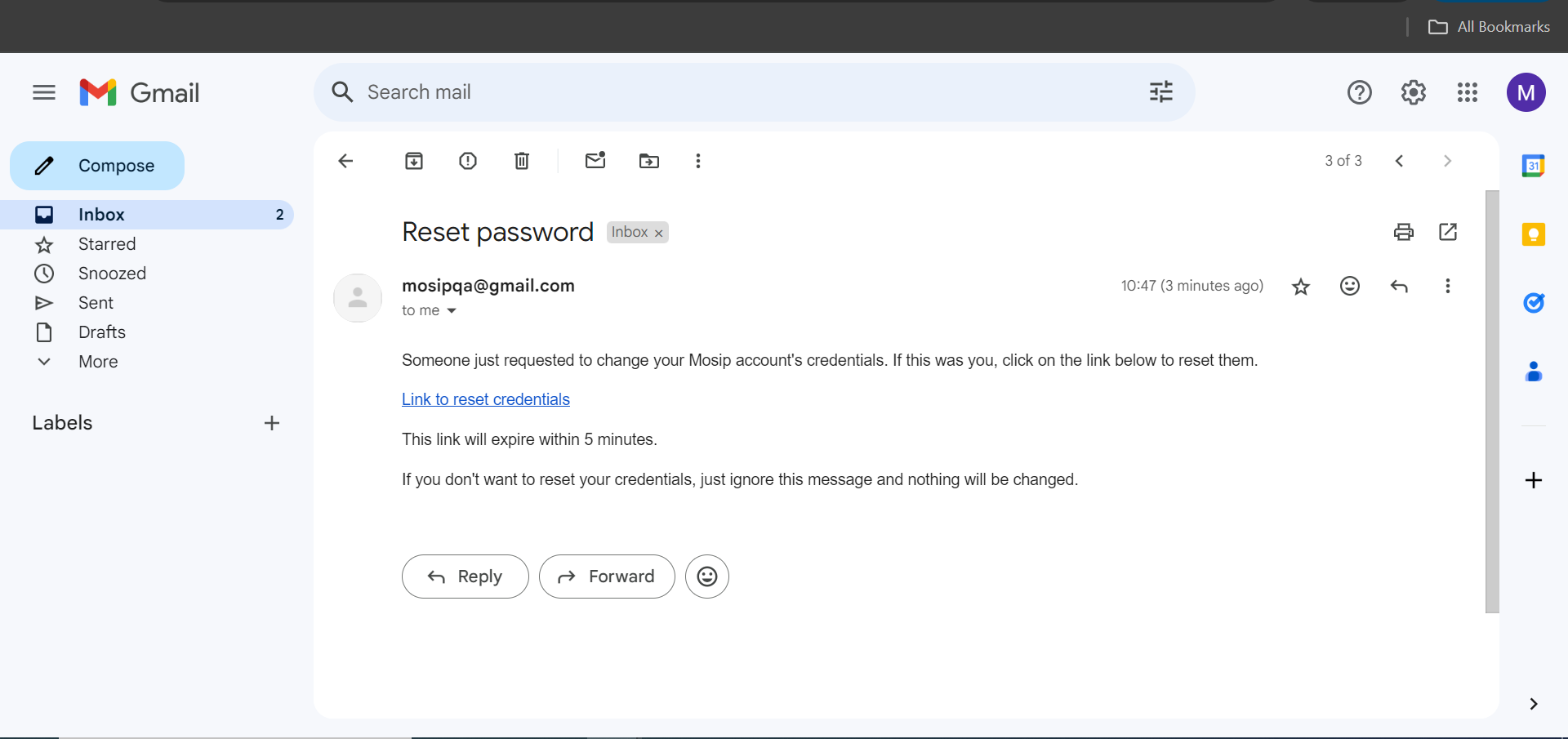
1. Click on **Forgot Password** link displayed on login page to reset password.

 ” alt=““>

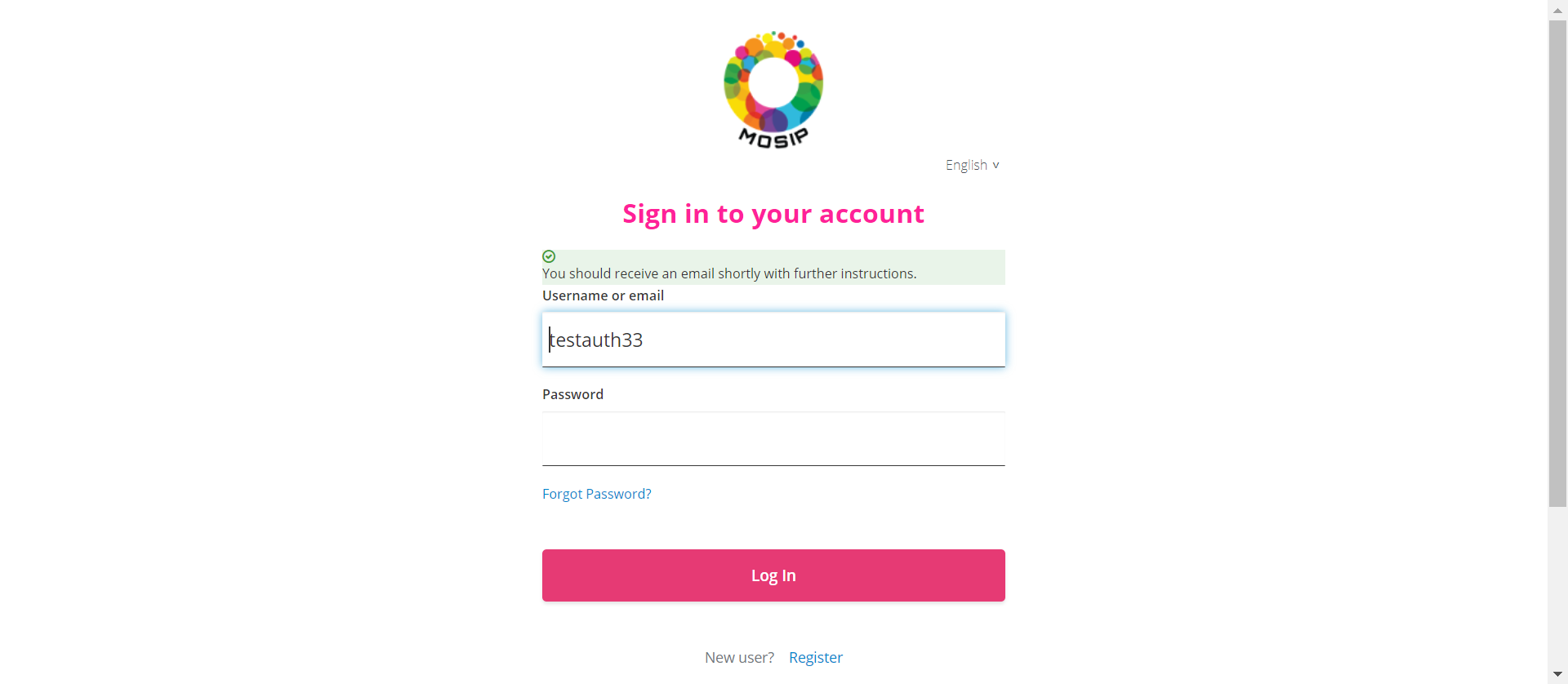
1. Enter registered email address and submit, a message is displayed informing user that further instructions to reset password has been sent on te email address entered.

 ” alt=““>

1. Click on the Reset password link received on his email address, you will be redirected to Change Password screen.

 ” alt=““>

1. Enter a new password that adheres to password policy and re enter to confirm before you save it.

 ” alt=““>

1. After clicking submit, This new password will be further used in subsequent logins