# 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.

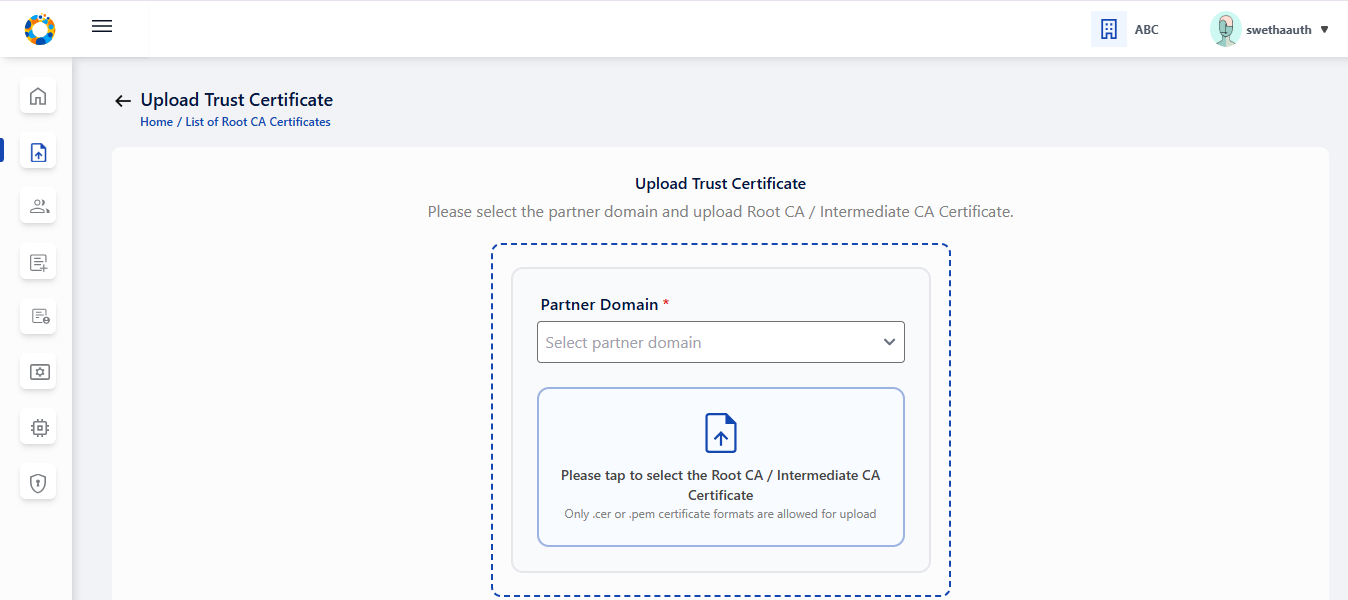
As a process of Partner onboarding onto PMP after successful registration, Partner is required to **Upload CA signed Partner Certificate** on behalf of their organisation which would be used to build a trust store in MOSIP to cryptographically validate that they are from a trusted organisation to perform 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

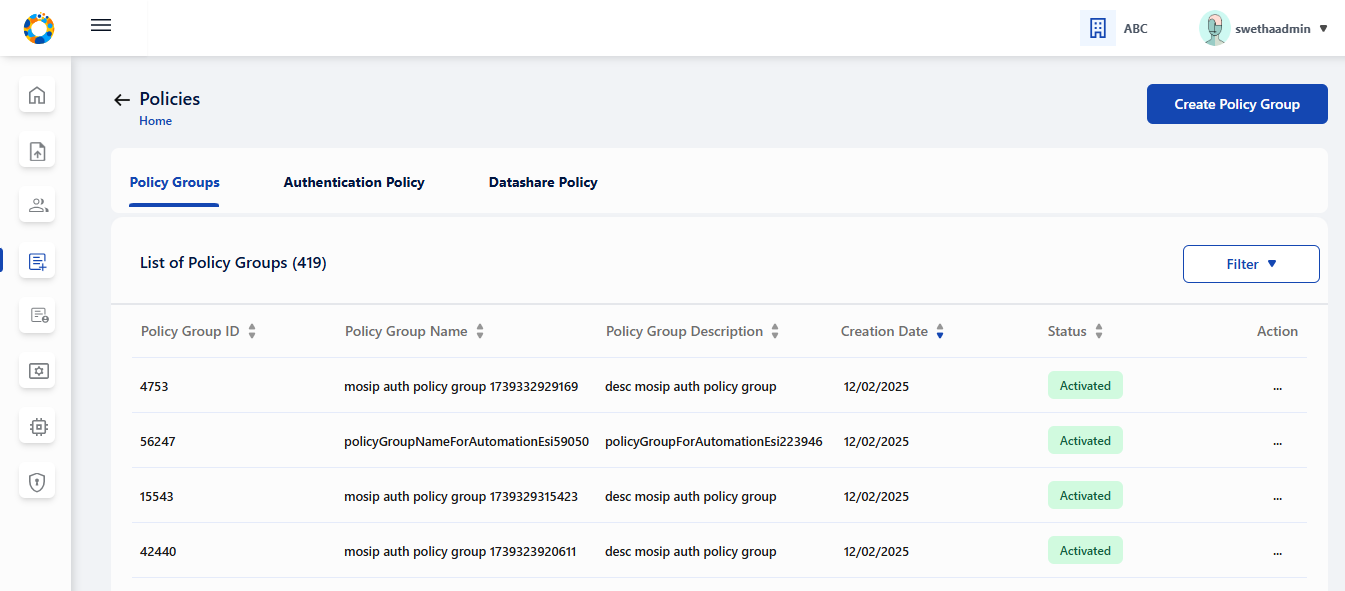
### Creating Policy Group and Policy

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.

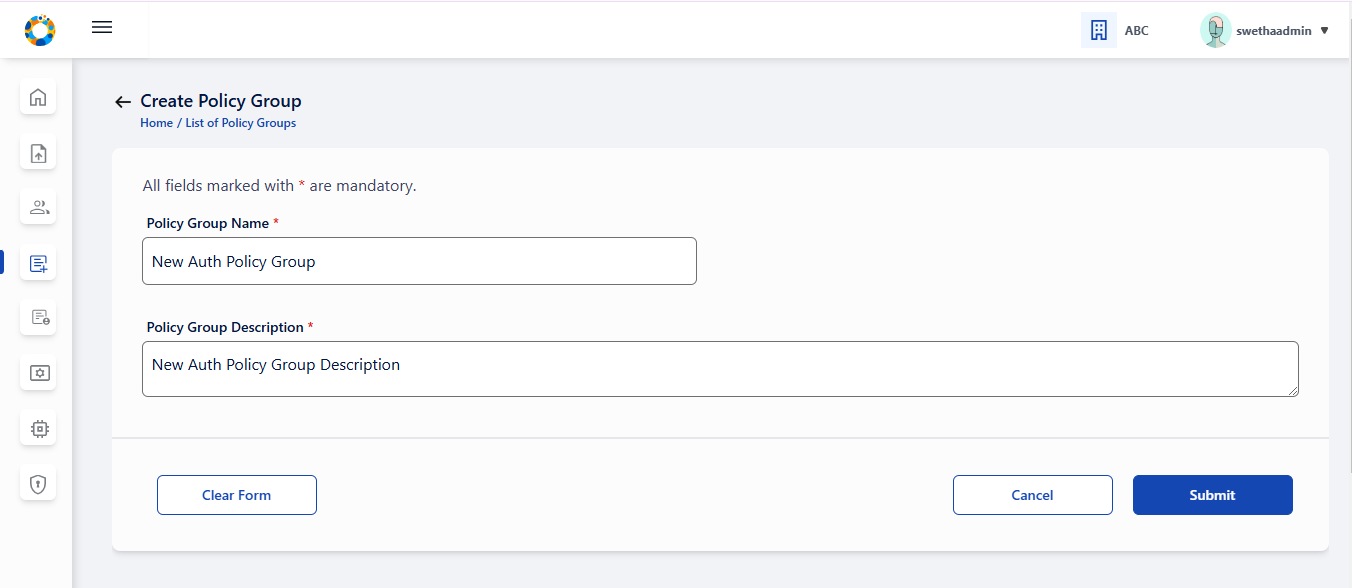
As an admin you will also have privilege to ‘**Approve Policy Request**’ when a Partner selects a Policy and it comes to you for approval, You can read more about this [**here**](end-user-guide.md#approve-policy-request).

#### Create Policy group

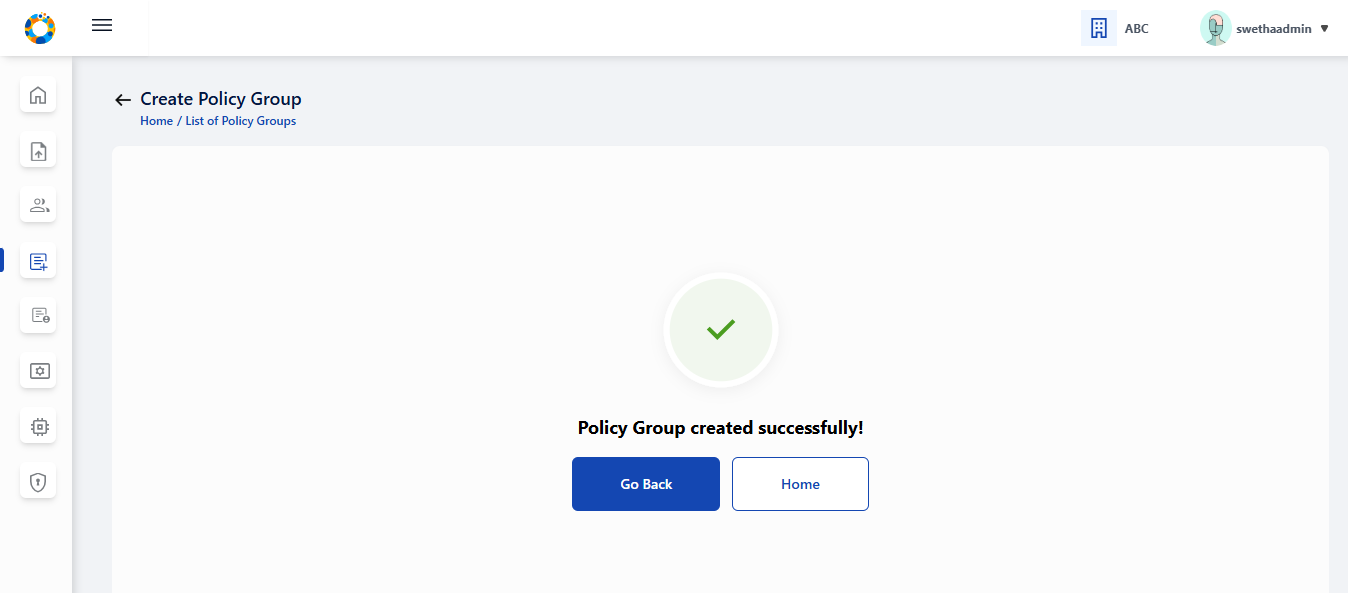
* Login as Partner Admin into the PMS portal (Older PMP Interface).
* All the policy groups created so far by Partner Admin/ Policy Manager are displayed on ‘List of Policy Groups’ page.



* 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.

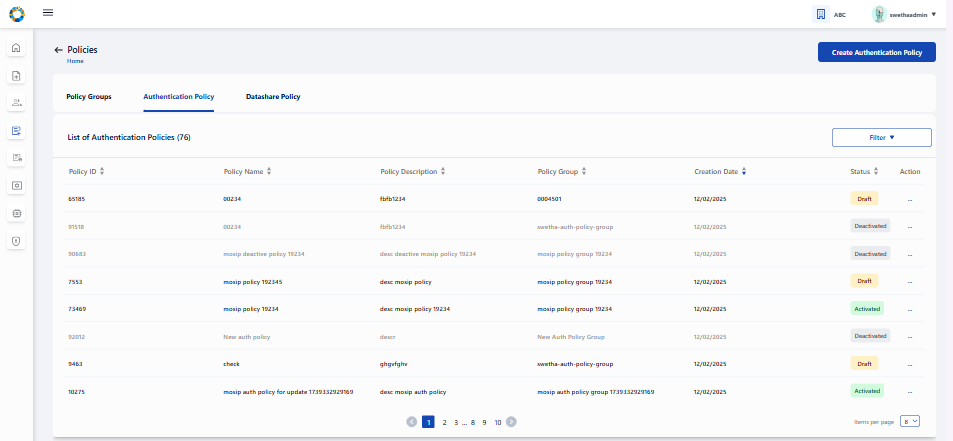


#### Create Auth policy

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.

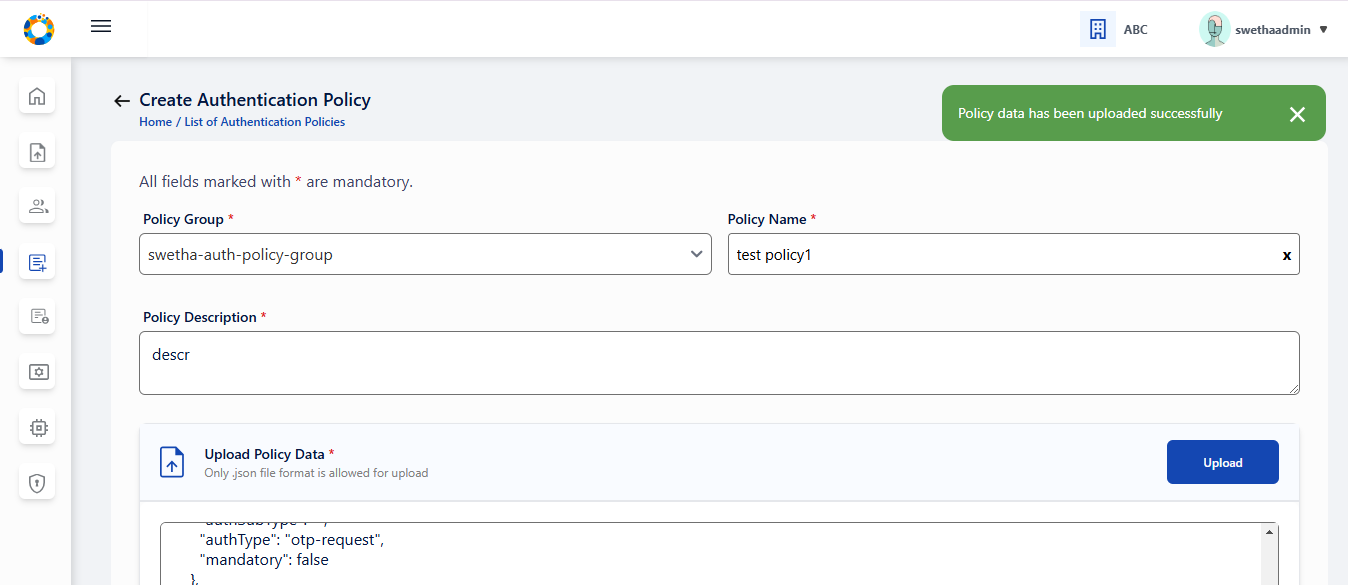
On clicking Authentication Policy tab, List of all previously created Authentication Policies are displayed.



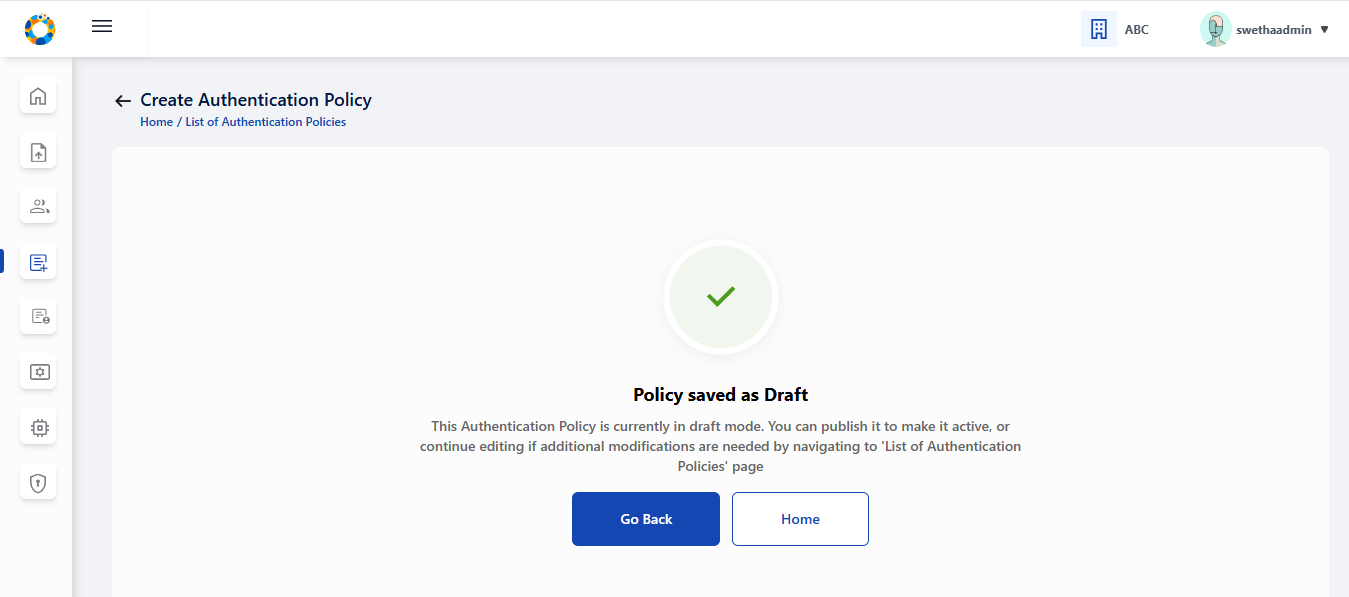
On clicking ‘Create Authentication Policy’ button, Partner Admin/ Policy manager is navigated to Create Authentication Policy page where details such as policy group, policy name, description etc will have to be entered

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.

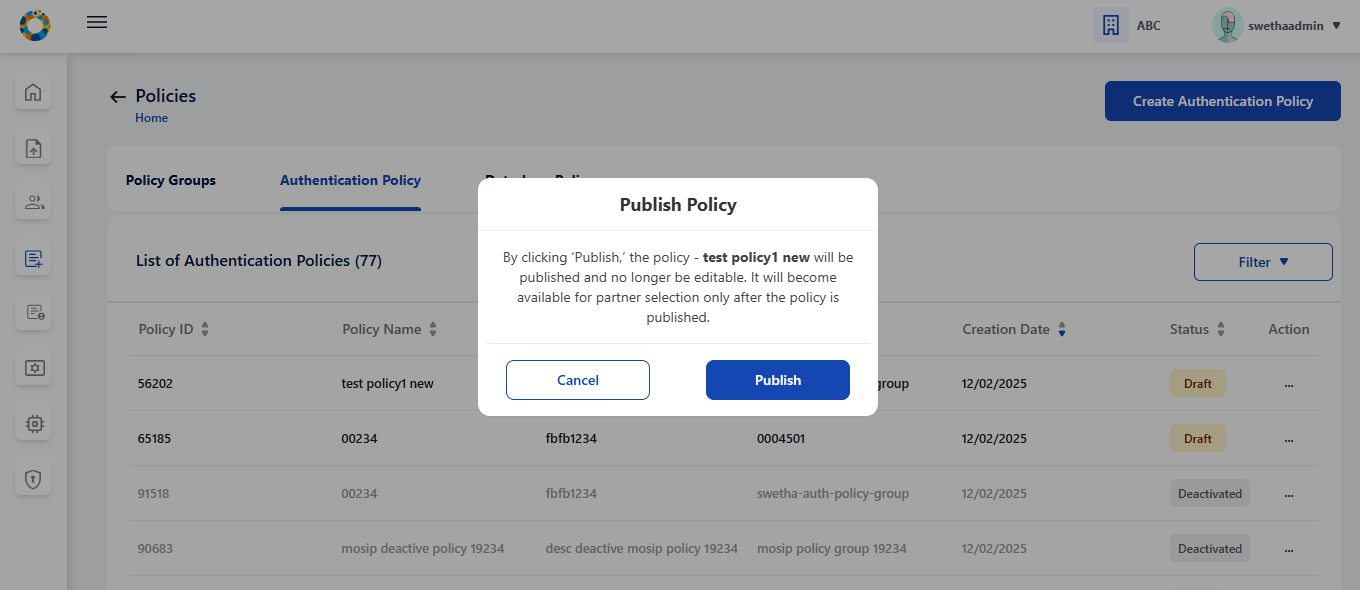


On clicking on Save as Draft, following success message appears .

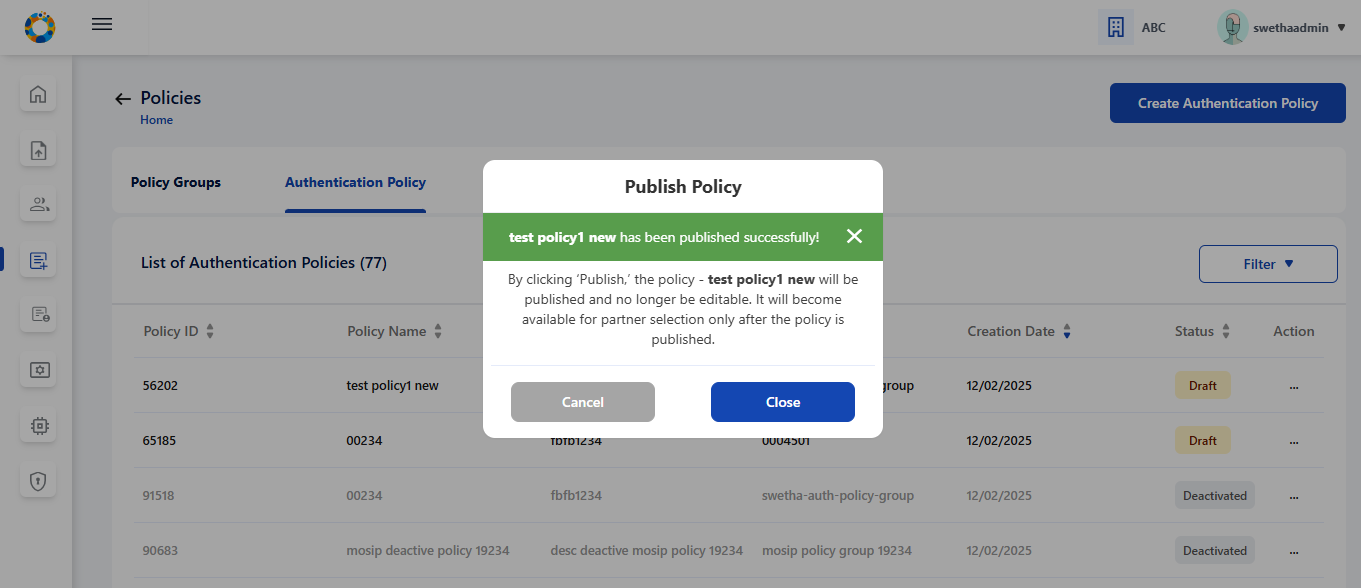


On clicking ‘Go Back’, admin is navigated back to tabular view where the policy is saved as ‘draft’ status.

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.



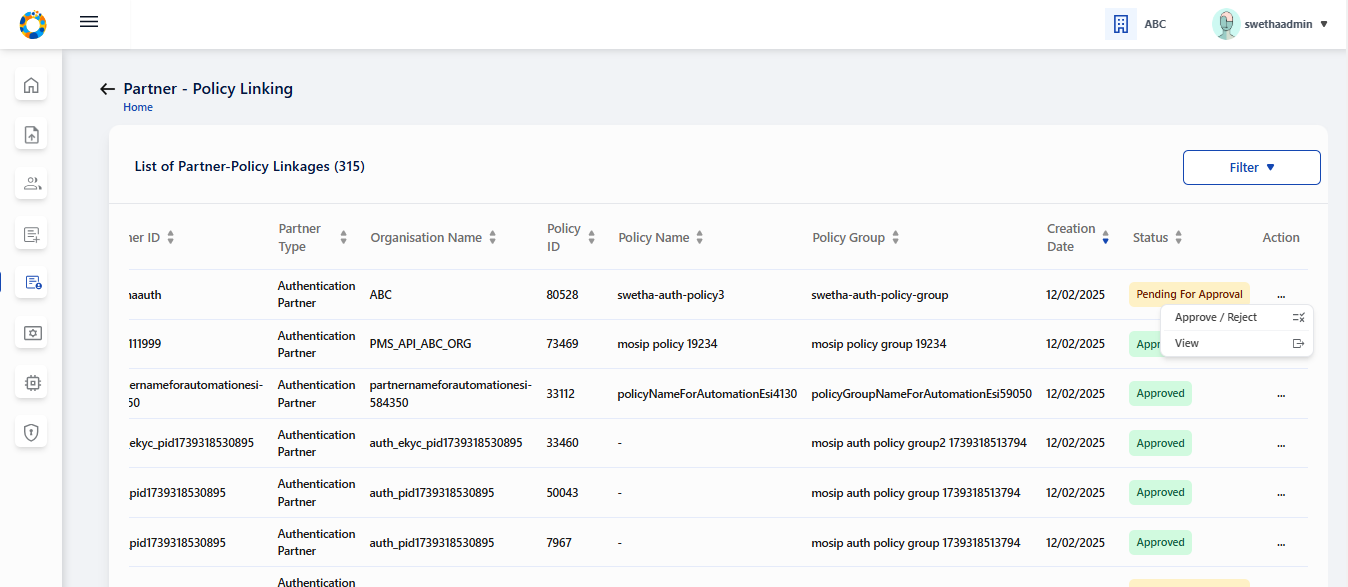
The given policy changes to ‘Activated’ status after being published. Once activated, the admin cannot edit the policy, hence the option is disabled.

Approve Policy Request

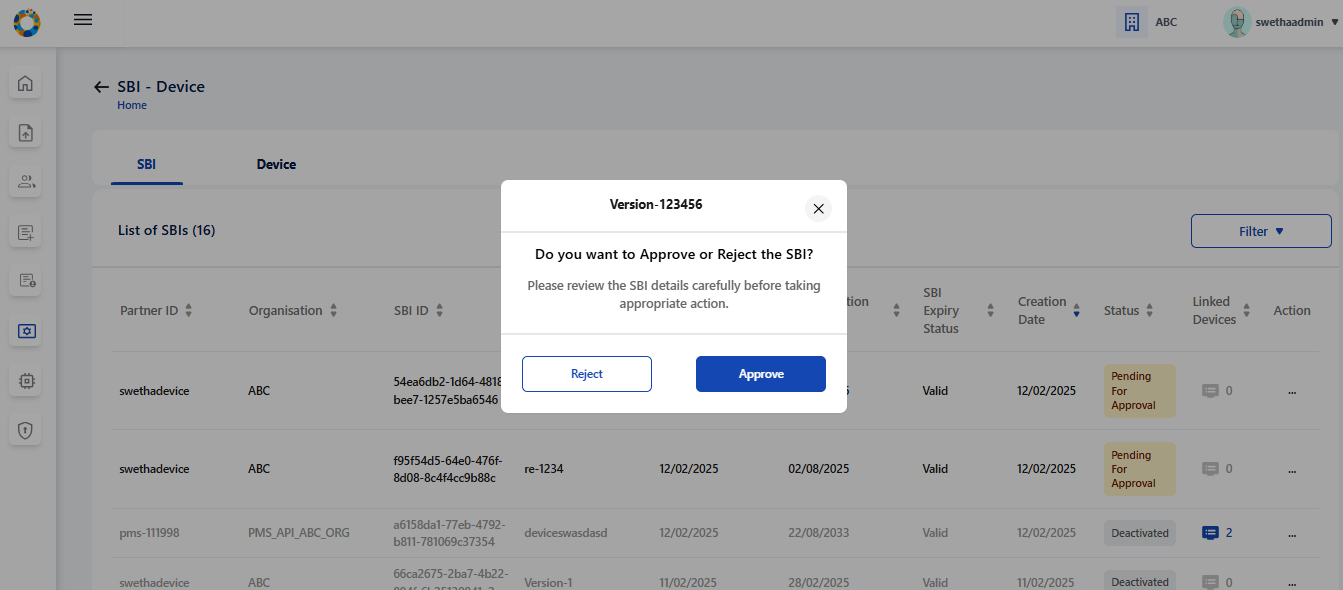
When a Partner have chosen a ‘Policy Group’ and the ‘Policy’, an approval request will come to you and you can approve or reject a ‘**Policy Request**’ using ‘**Request Policy**’ screen.

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.

