C-DOT

PM-WANI Central Registry User Manual

Table of Contents

Chapter 1.

Introduction

Proliferation of broadband across the length and breadth of the country is an essential ingredient of Digital India. Towards this objective, it is envisaged to leverage public Wi-Fi network for delivery of broadband services. This is sought to be facilitated by rolling out WANI infrastructure with the broadband services being provided under distributed architecture and unbundling of infrastructure to improve performance by different players under the WANI eco system.

What is WANI framework?

While delivery of broadband is possible through different media and technologies, under the WANI framework, it is envisaged that last mile broadband connectivity, where the consumer accesses broadband services, will be through a network of public Wi-Fi access points. The backhaul requirement for these Wi-Fi access points will be met by procuring internet bandwidth from the telecom service providers/internet service providers. Under the distributed architecture and unbundling of functions, the WANI eco-system will be operated by different players who are described herein under:

- **Public Data Office (PDO):** It will establish, maintain, and operate only WANI compliant Wi-Fi Access Points and deliver broadband services to subscribers.
- **Public Data Office Aggregator (PDOA):** It will be an aggregator of PDOs and perform the functions relating to Authorization and Accounting.
- **App Provider:** It will develop an App to register users and discover WANI compliant Wi-Fi hotspots in the nearby area and display the same within the App for accessing the internet service.

- **Central Registry:** It will maintain, in accordance with the WANI architecture and specifications, the details of App Providers, PDOAs, and PDOs. To begin with, the Central Registry will be maintained by C-DOT.

Wi-Fi Access Network Interface (WANI) ensures the interworking among systems and software applications used by these distributed entities i.e., PDOA, PDO, App Provider, and Central Registry.

1.1. DEFINITIONS, ACRONYMS AND TERMINOLOGY

1.1.1. Definitions

The definitions for the terms used in this document are listed in the Table 1-1.

Table 1-1: Definitions Used in this Document

Definition	Explanation
802.11	IEEE Standards for Information Technology -- Telecommunications and Information Exchange between Systems -- Local and Metropolitan Area Network Specific Requirements (ISO/IEC 8802-11: 1999)

1.1.2. Acronyms

Table 1-2: Acronyms Used in this Document

Acronyms	Explanation
MAC	Medium Access Control
SSID	Service Set Identification
Wi-Fi	Wireless Fidelity

Chapter 2.

Central Registry

The Central Registry can be accessed by opening the URL "**https://pmwani.cdot.in**" in any Web browser.

Figure 1- Landing Page of Central Registry

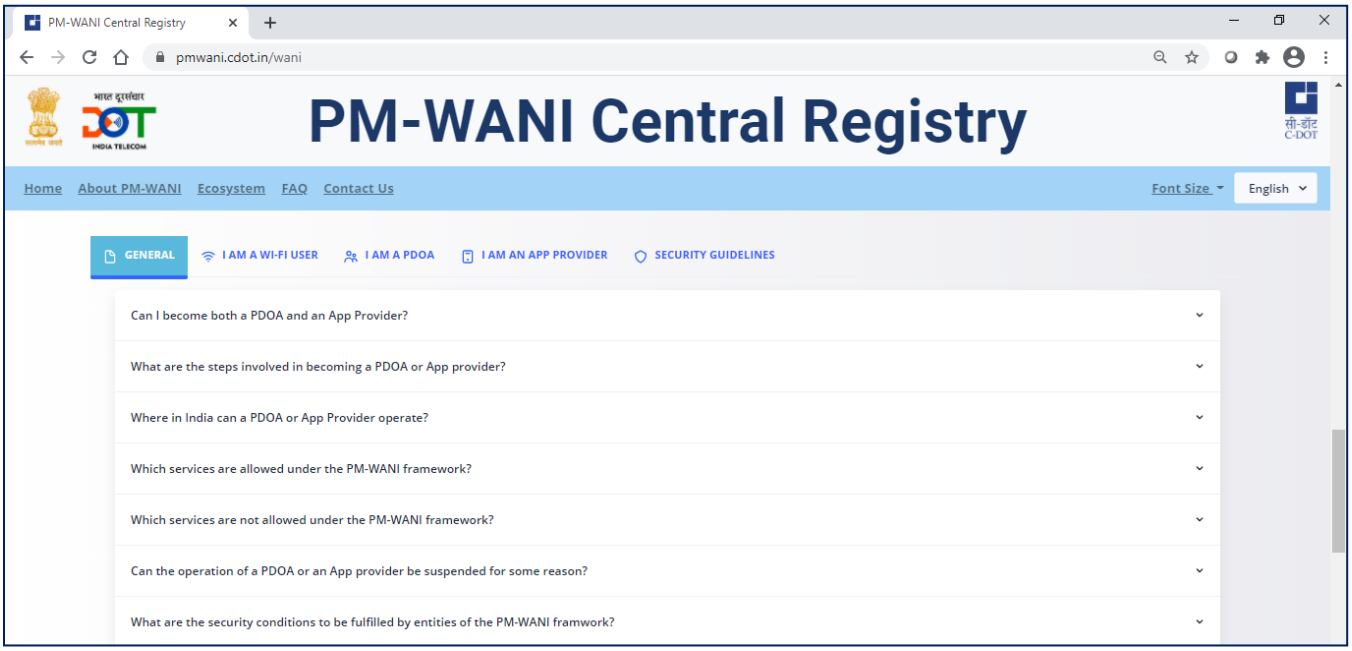


Figure 2-"FAQ" Section

Scroll down to read about PM-WANI and read the Frequently Asked Questions to resolve any queries. Please contact us for any feedback or any further queries & doubts.

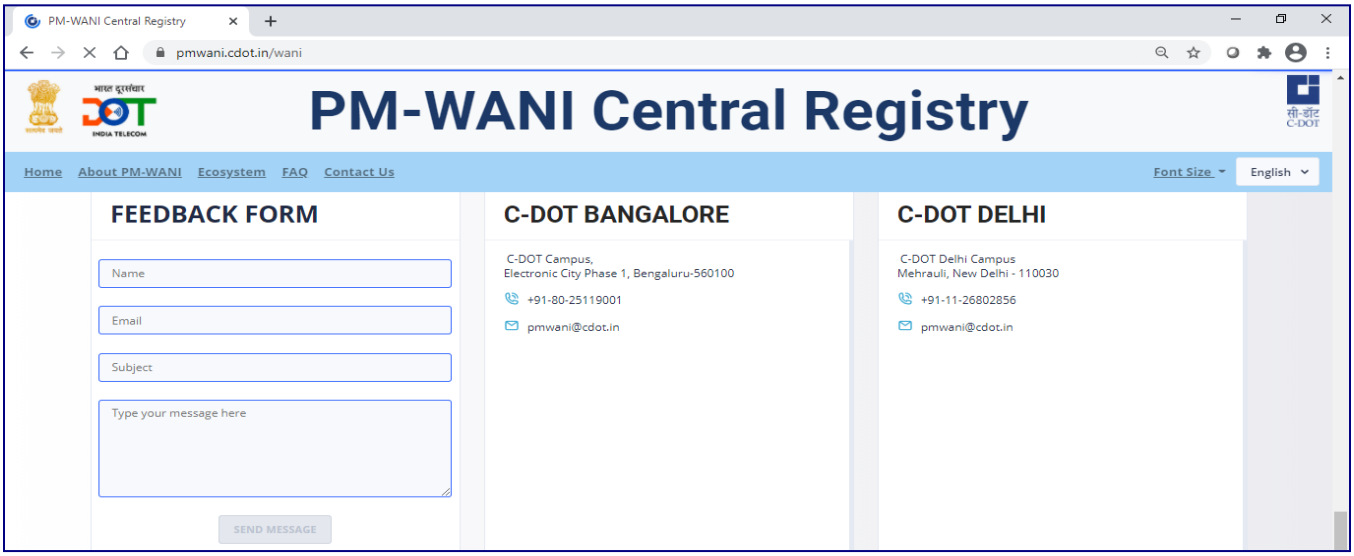


Figure 3- "Contact Us" Section to resolve queries

Chapter 3.

PDOA/App Provider Sign-Up

To register with the Central Registry as a PDOA or an App Provider, the user has to click on the "PDOA Portal" tab or the "App Provider Portal" tab as pointed out below:

Figure 4 – Click "PDOA Portal" tab is you are a PDOA

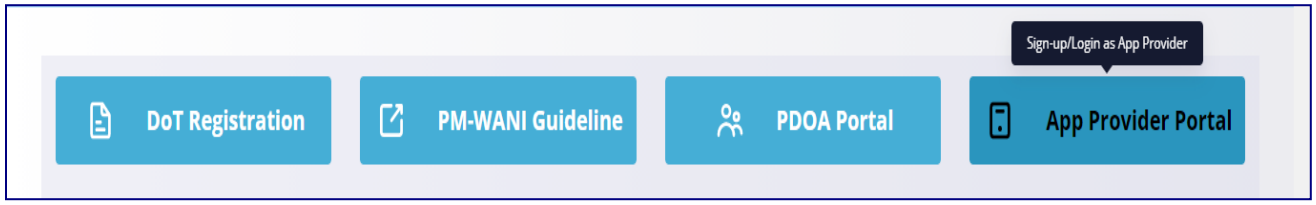


Figure 5- Click "App Provider Portal" tab if you are an App Provider

3.1. PDOA/APP PROVIDER PORTAL PAGE

The PDOA/App Provider Portal page allows the user to complete the PDOA/App Provider registration process. It has two sections- the "Sign-up" and the "Login".

3.2. OTP BASED SIGN-UP

After completing the registration process at the Saral Sanchar Portal, click the Sign-up button to initiate the registration process at the Central Registry.

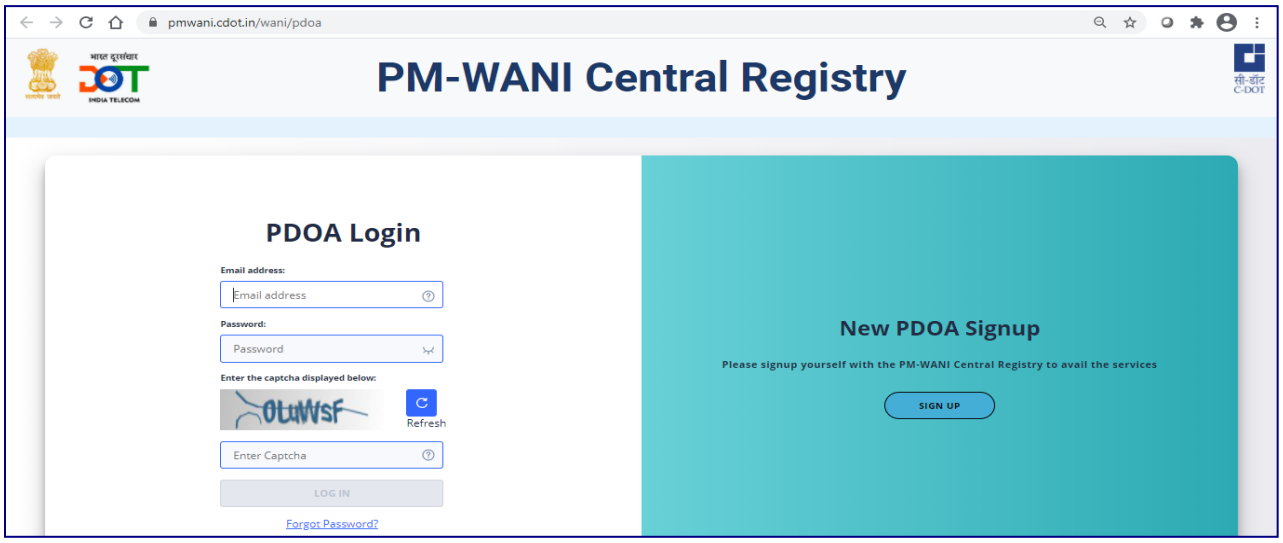


Figure 6- PDOA Portal Page

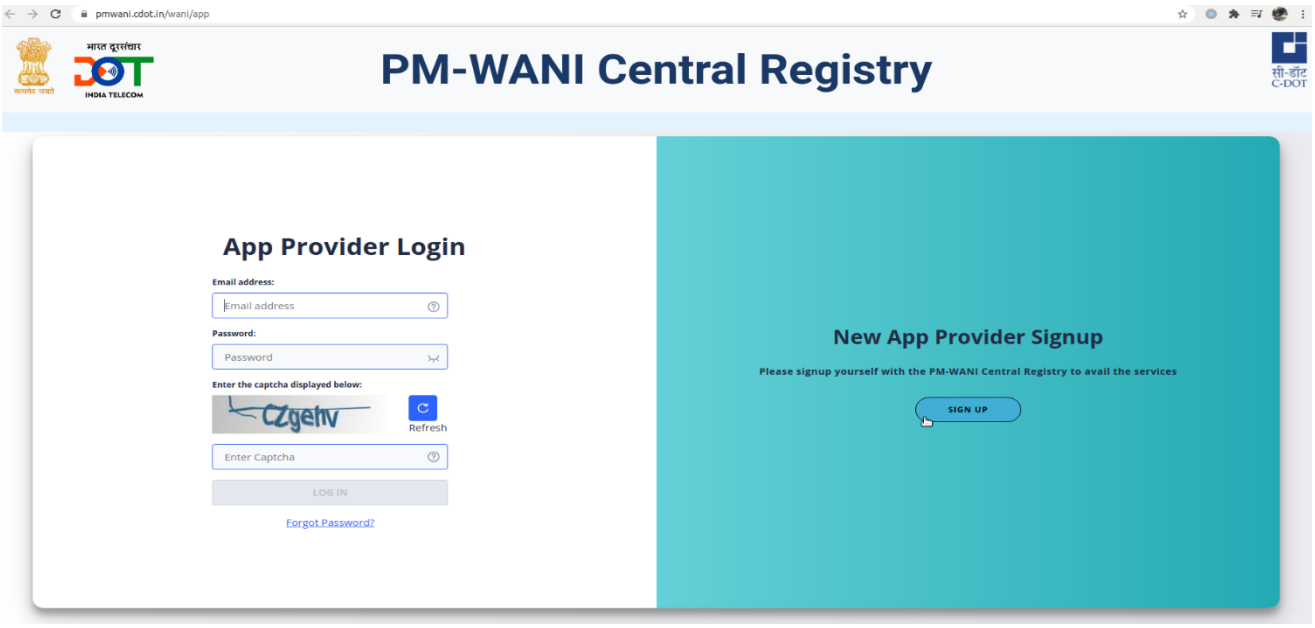


Figure-7-App Provider Portal page

In the Sign-up tab, provide the Saral Sanchar registration number, the email-id and the mobile number of the Authorized person of contact for your company, as registered with Saral Sanchar. Click the "SIGN UP" button.

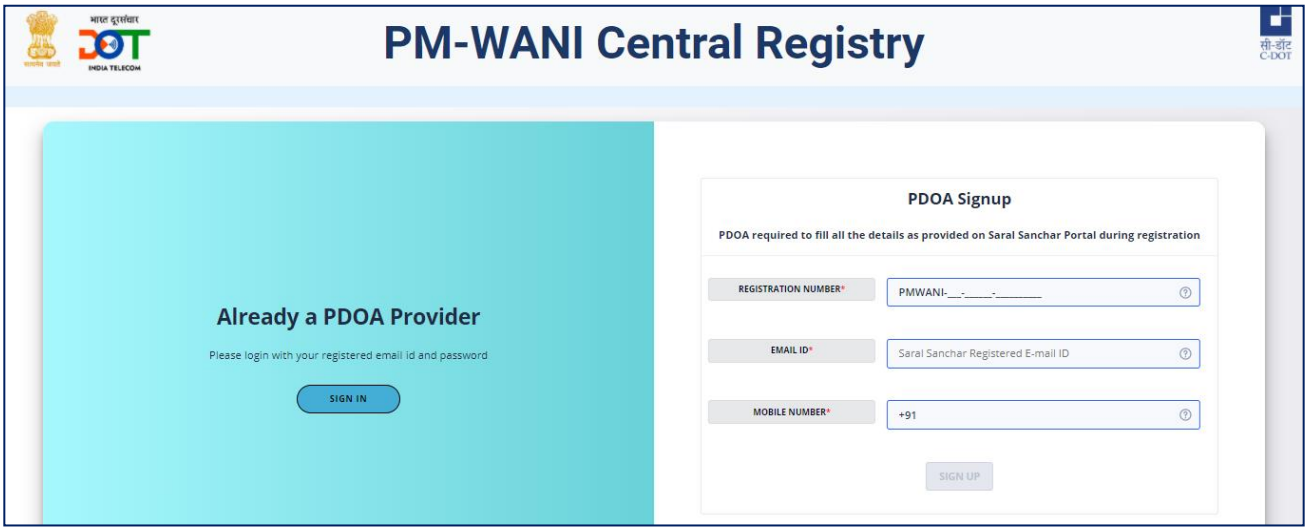


Figure 7- PDOA Sign-up Page

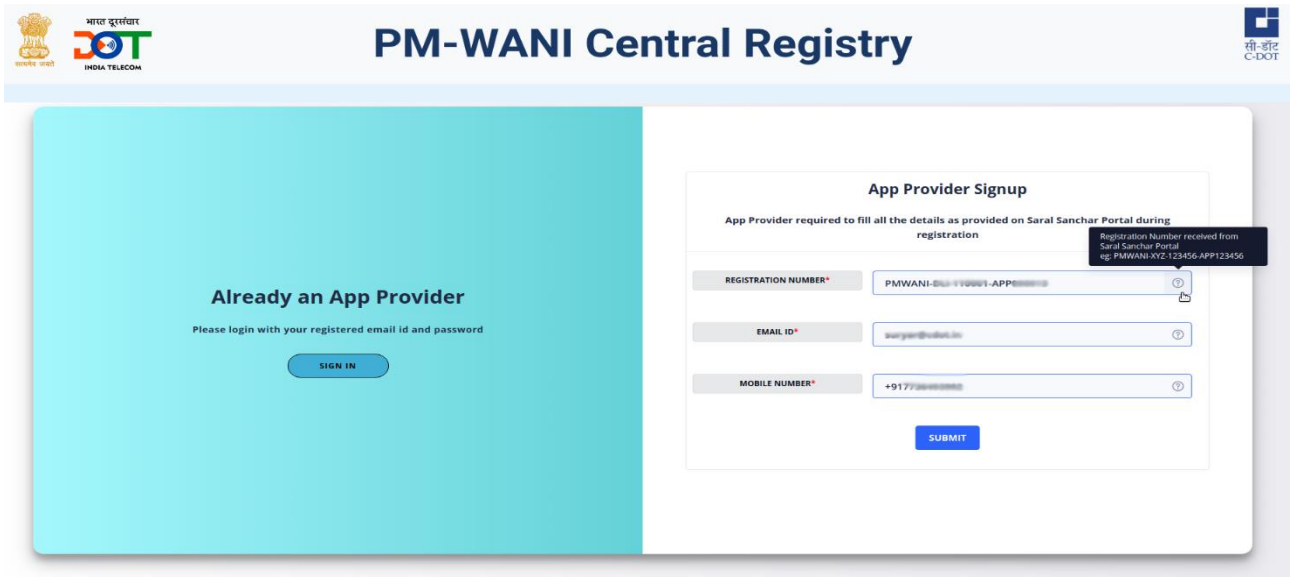


Figure 8- Provide the registration number, email ID and mobile number. Click Submit to Proceed

An OTP will be sent on the email-id and the mobile number. You can click the Resend button if the OTP isn't received within 60 seconds.

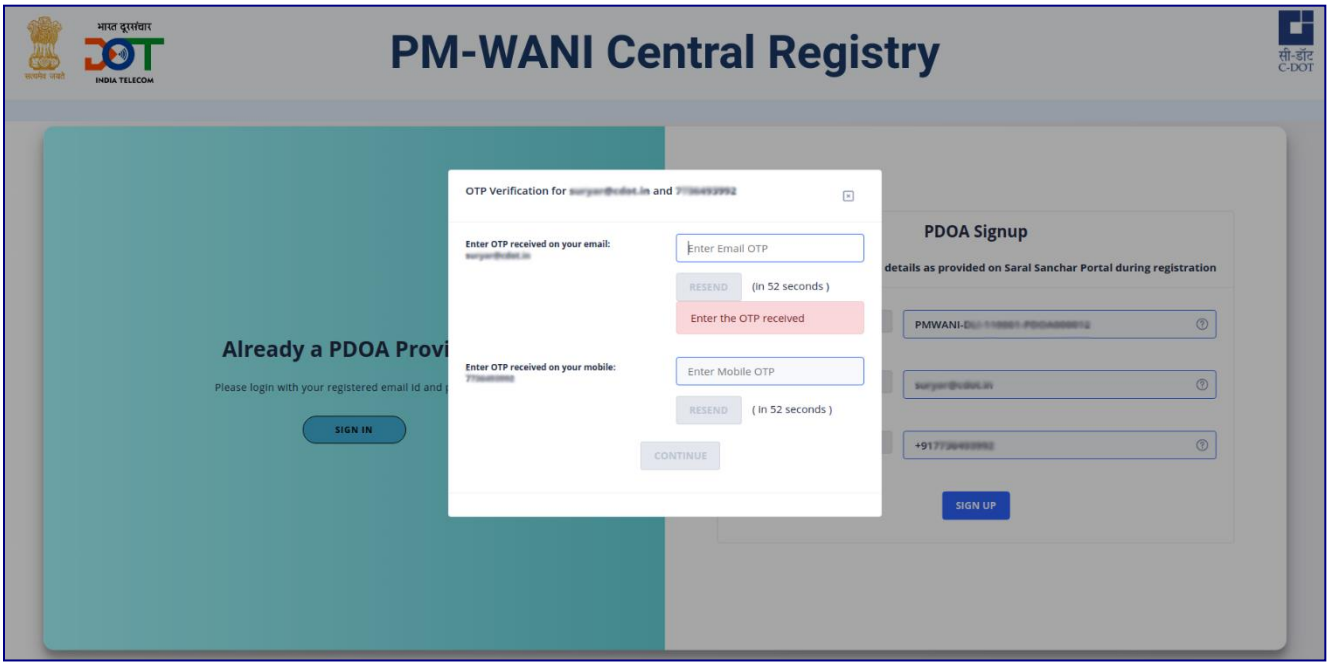


Figure 9 - Enter OTP for registering at Central Registry

Figure 10-OTP received on mobile and email-id

After the OTP is successfully verified, a password has to be created. Please ensure the password is sufficiently complicated as per the instructions.

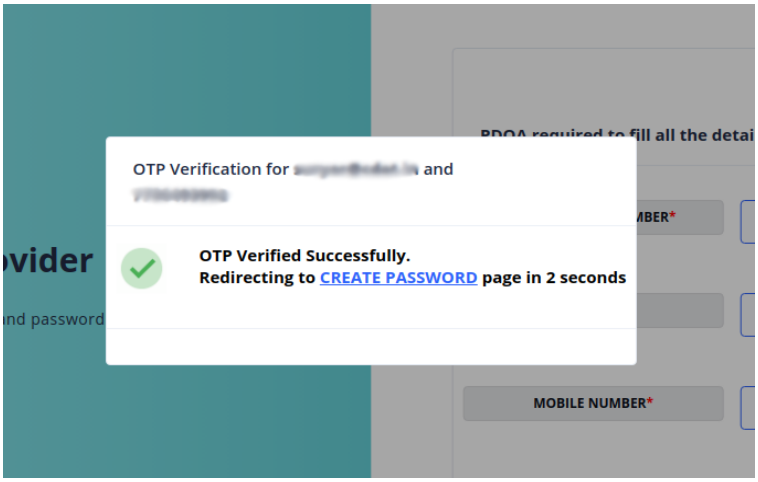


Figure 11- OTP successfully verified

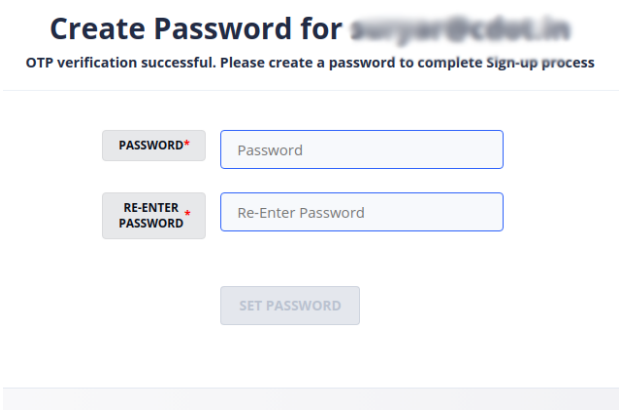


Figure 12- Create Password Page

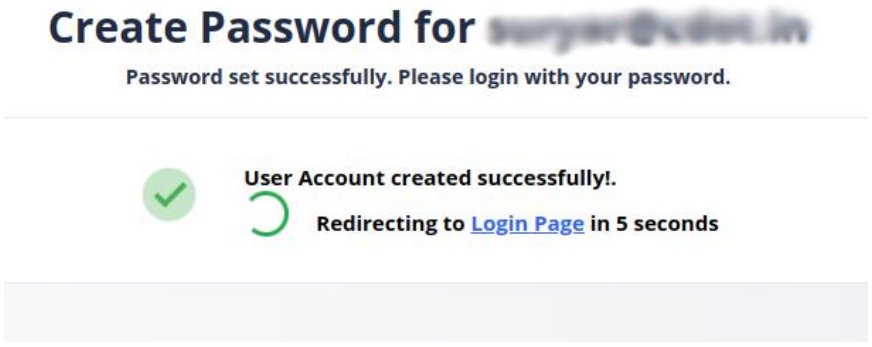


Figure 13- Password successfully created

After the password is created, you will be redirected to the Login Page. Read the next chapter for more details.

The same procedure needs to be followed in case of App Provider Sign up

Chapter 4.

PDOA/App Provider Login

Log-in to your account by providing the authorized person's email-id and the password that was set during the Sign-Up process.

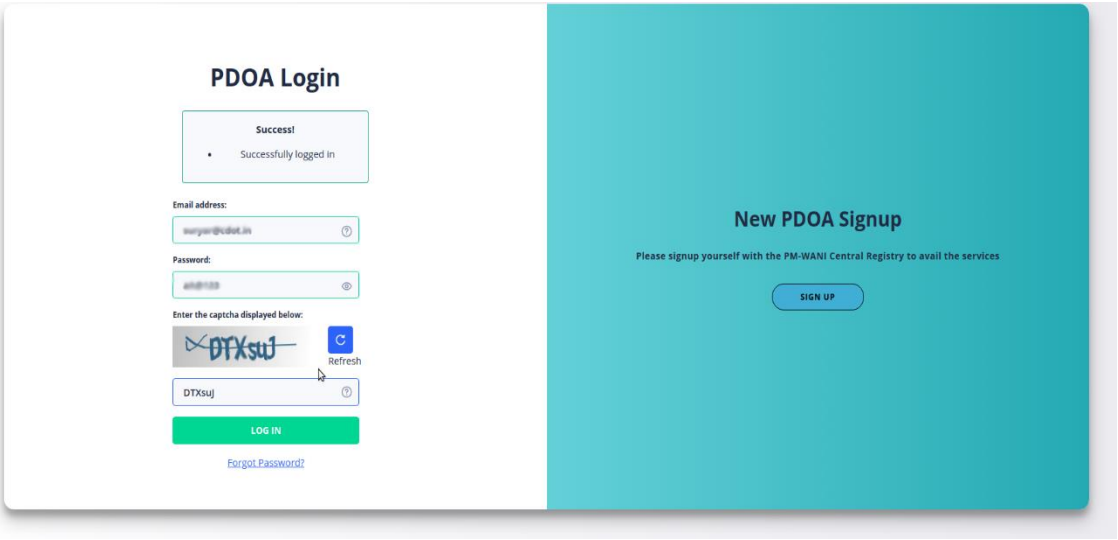


Figure 14- Successfully logged in to PDOA Account

4.1. SESSION

Only one session can be opened with the user credentials. Please logout from the first session to open a new session (Refer Section 3.2). Session idle timeout time is 10

minutes. Depending on the browser, the session will be closed when the browser or tab is closed.

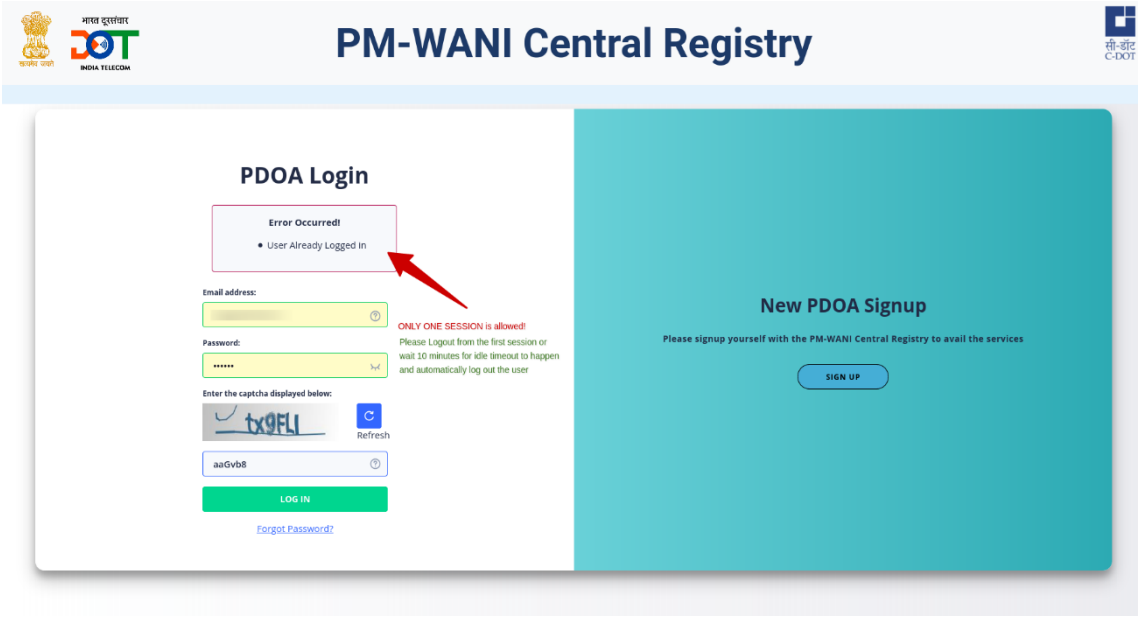


Figure 15- Only one Login session permitted at a time

4.2. LOGOUT

Logging out from an active session can be done by clicking on the top right corner. Clicking the "Log out" option will terminate the session and logout the user.

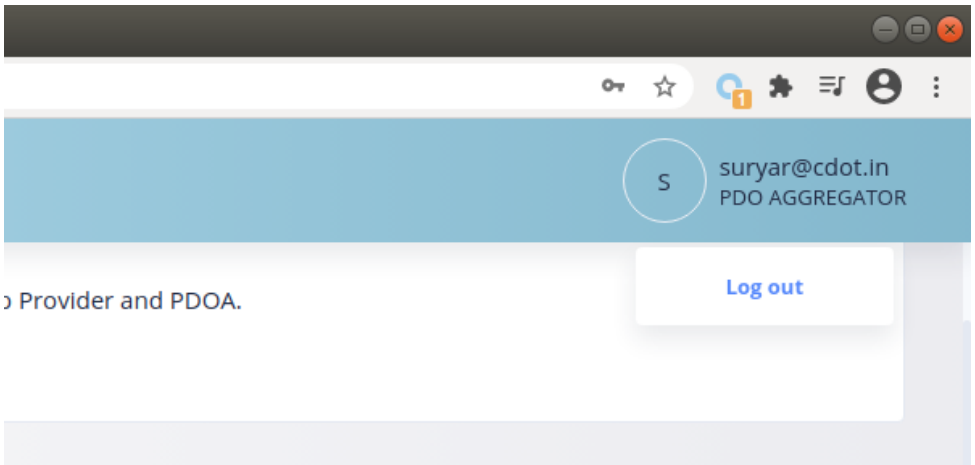
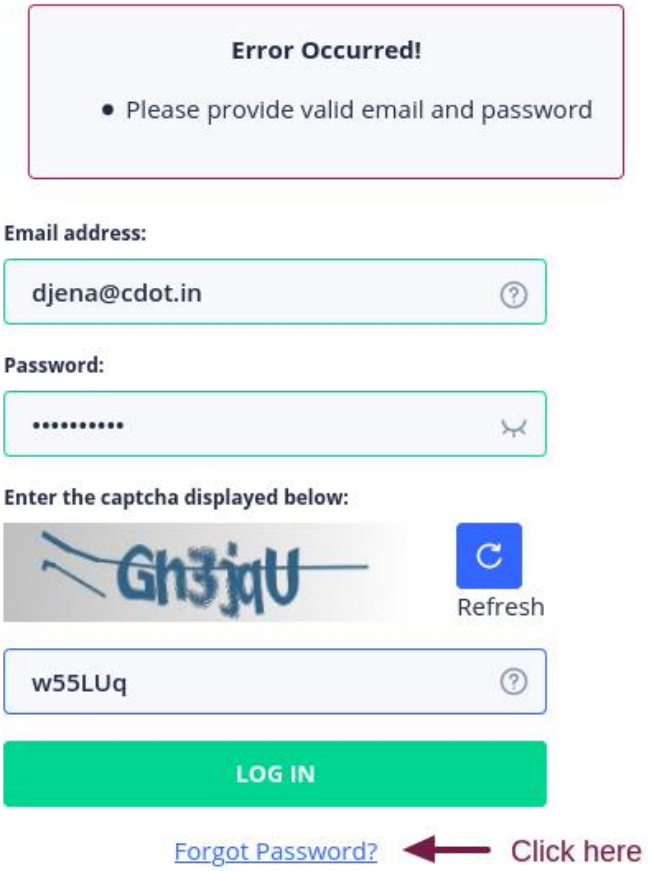


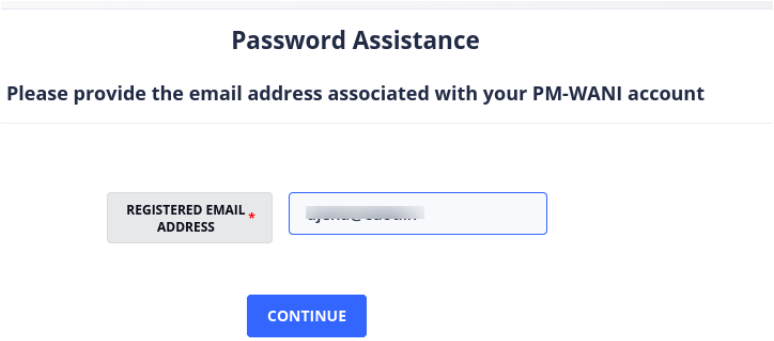
Figure.17. logout

4.3. FORGOT PASSWORD

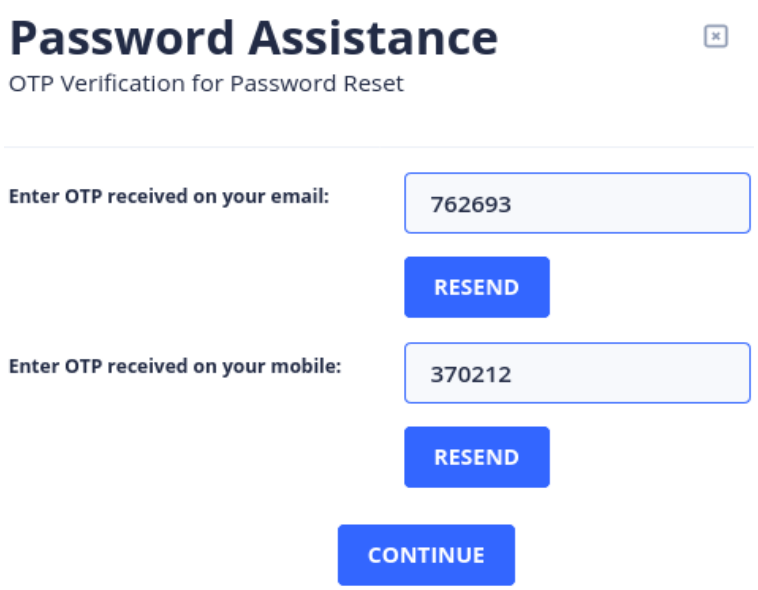
Step 1: If password is wrong/forgotten, click "Forgot Password"



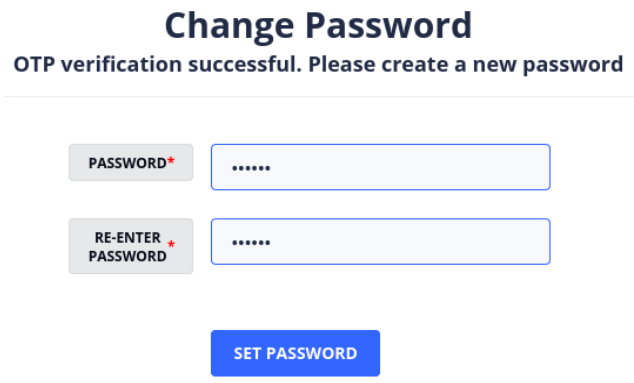
Step 2: Enter the authorized person's registered e-mail ID.



Step 3: Enter the OTP sent to the Authorized person's registered E-mail ID and mobile phone



Step 4: Set the new password



Step 5: Login with new password

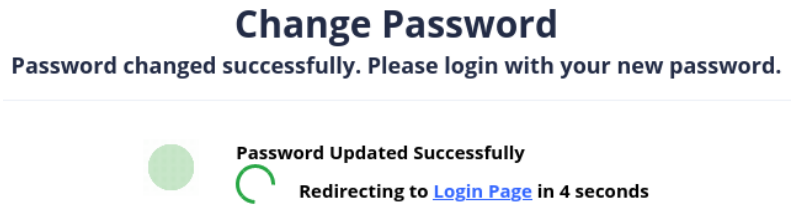
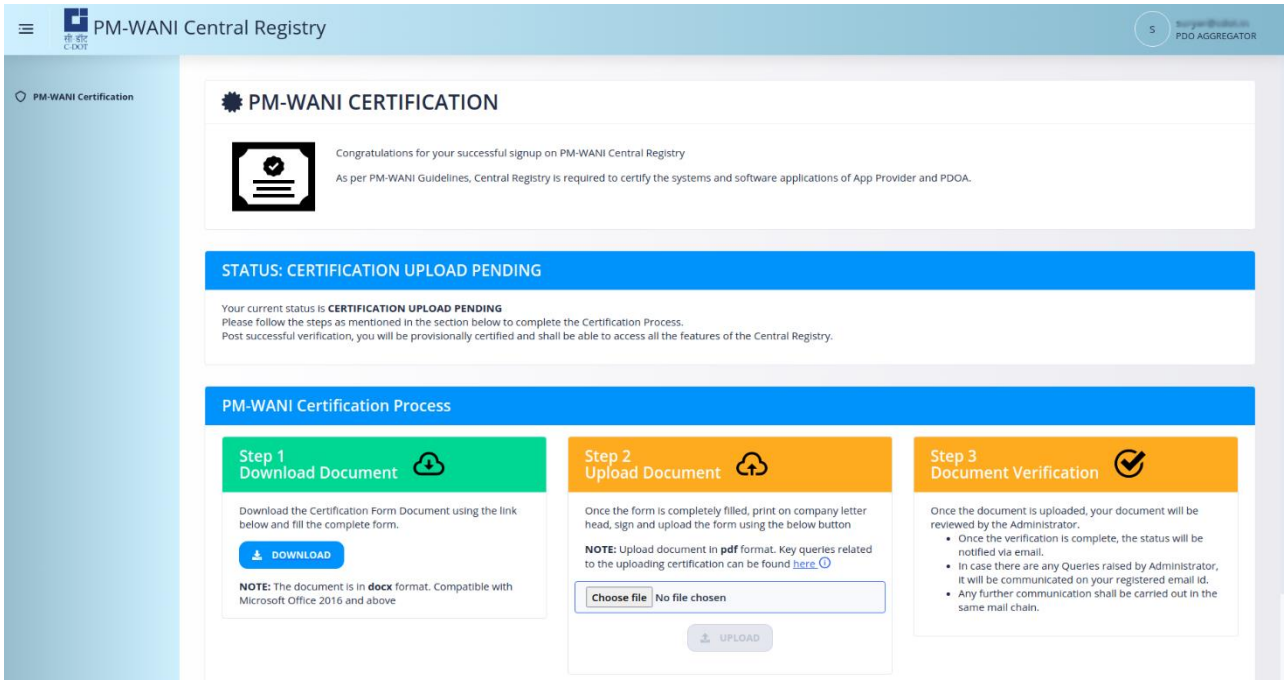


Figure 16- Forget Password

Chapter 5.

PDOA/App Provider Certification

After OTP verification is complete and password is set, the user has to login to the PDOA/App Provider account. This opens up the Certification Page as shown below.



STATUS BAR:

This is a color-coded indicator of the status of Certification of PDOA. On logging in for the first time, the Certification Page shows the STATUS as "CERTIFICATION UPLOAD PENDING" in blue color to indicate that the Certification Form upload is pending. The color changes to yellow when the Verification of uploaded Certification Form is pending as shown in Figure.

5.1. PM-WANI CERTIFICATION PROCESS

Step 1: Download Document

Download the Certification Form by clicking the "DOWNLOAD" Button. This opens a Certification form. The questions specific to PDOA or App Provider are to be

answered accurately to ensure a smooth approval of certification process. Any queries regarding the questions or other queries can be communicated to the Central Registry via e-mail.

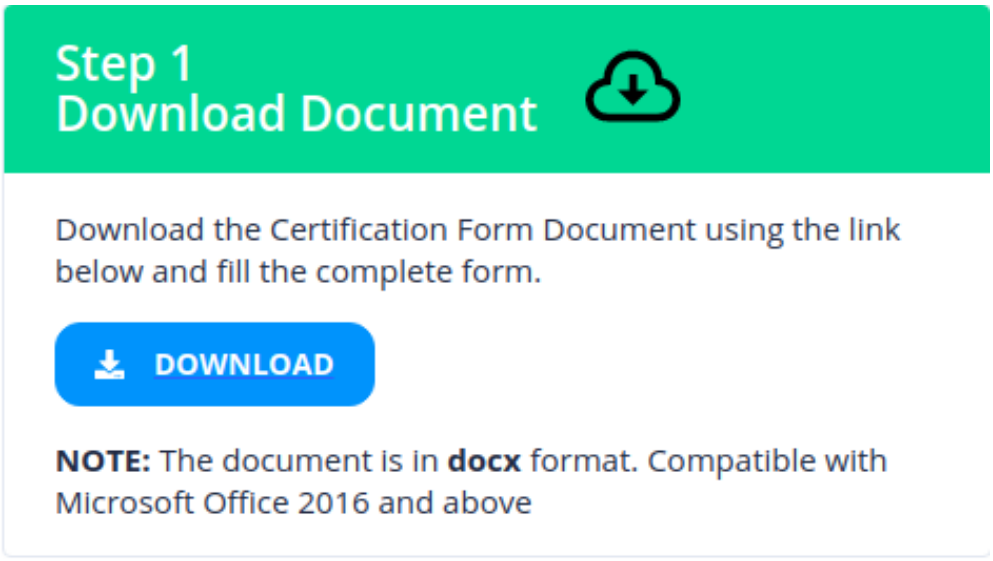
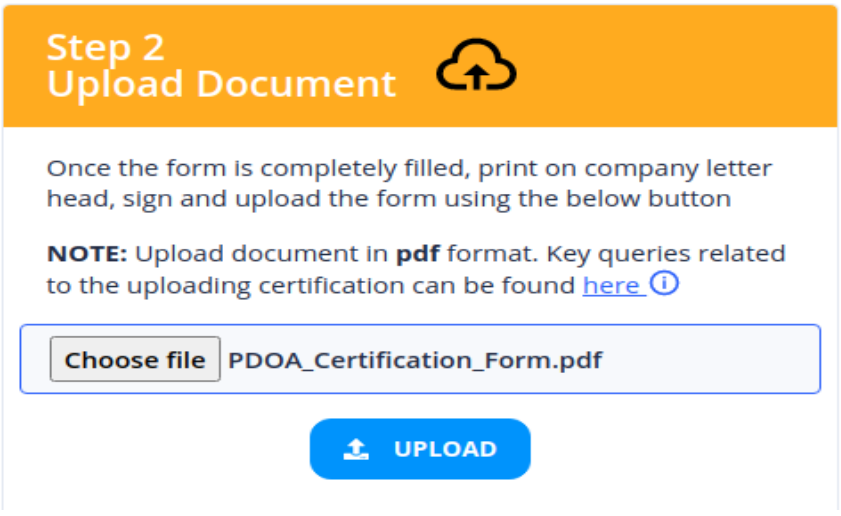


Figure 17- Certification Page

Step 2: Upload Document

Print the filled Certification Form on your company's letterhead and get it signed by the authorized point of contact. Scan this Certification Form in pdf format and upload it. If there are any queries related to the upload process, click the information icon.

(NOTE: Certification Form for App Provider and PDOA are different. Please ensure the correct form is uploaded.)



On uploading the Certification Form correctly, the Certification Page changes as follows:

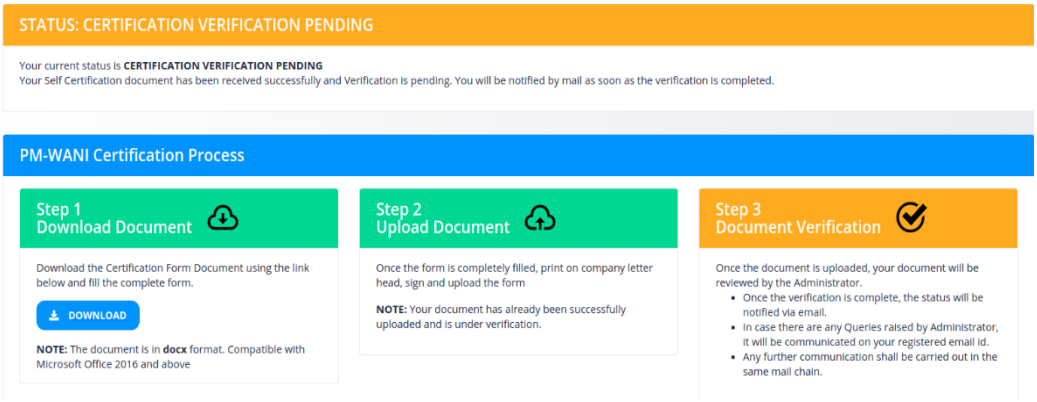
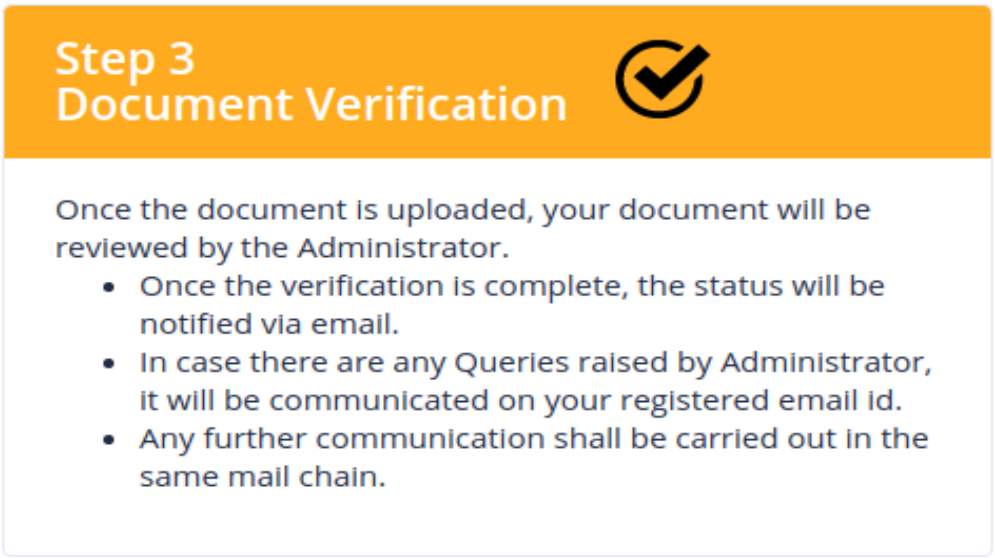


Figure 18-Certification Page status changed to "CERTIFICATION VERIFICATION PENDING"

Step 3: Document Verification

Wait for the document verification to be done by the Central Registry. Any queries and clarity required for certifying the claims made will be communicated on the registered e-mail ID. This will take up to 7 working days. Once successfully verified and certification is granted, an email will also be sent as below:-



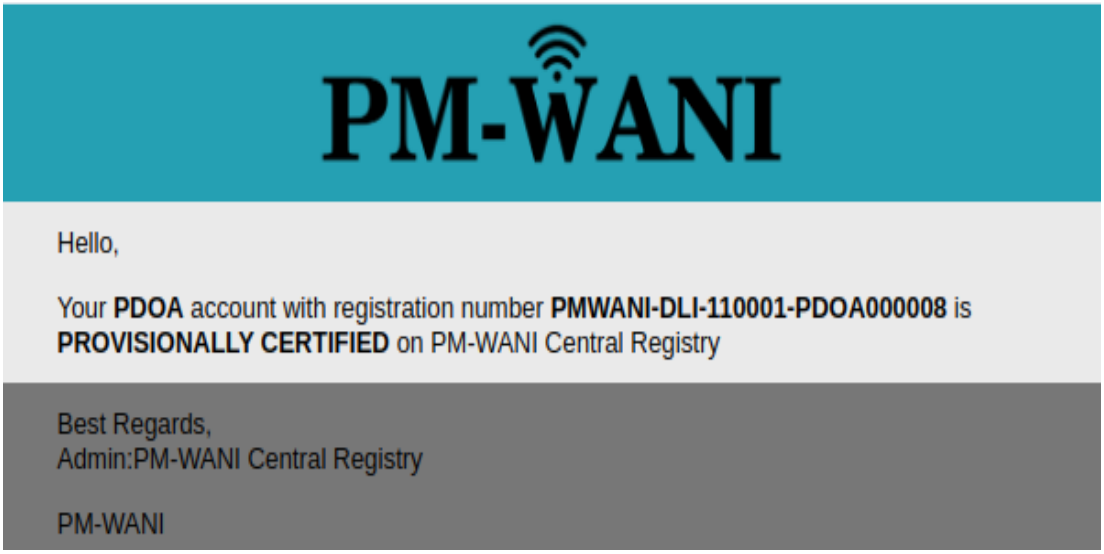


Figure 19- Certification granted e-mail intimation

Chapter 6.

Security Certificate

After being certified, the PDOA/App Provider has to login again. The following page opens up. Please upload at least one Public Security Certificate obtained from any Certificate Authority. Please read the Help Guide and upload the security certificate as per the format specified.

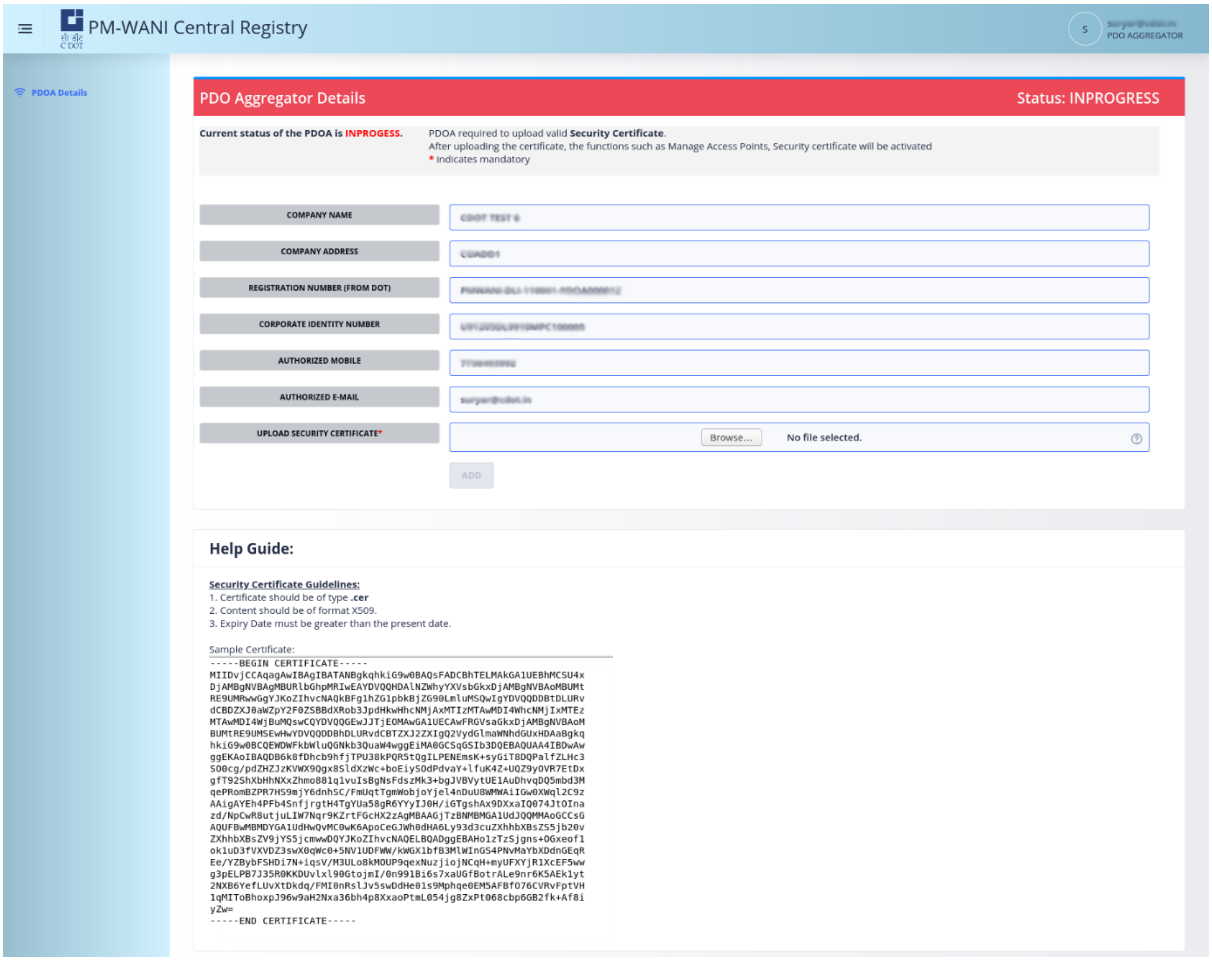


Figure 20- Security certificate has to be uploaded as per the Help Guide

(NOTE: The Status bar at the top indicates the status of the PDOA/App Provider registration. The red color indicates "INPROGRESS" state. It changes to green color to indicate "ACTIVE" state after uploading a correct Security Certificate.)

Figure 21-Add Security Certificate obtained

NOTE: The App Provider has to add its backend server's authentication URL along with the Security Certificate. Refer Section for more details

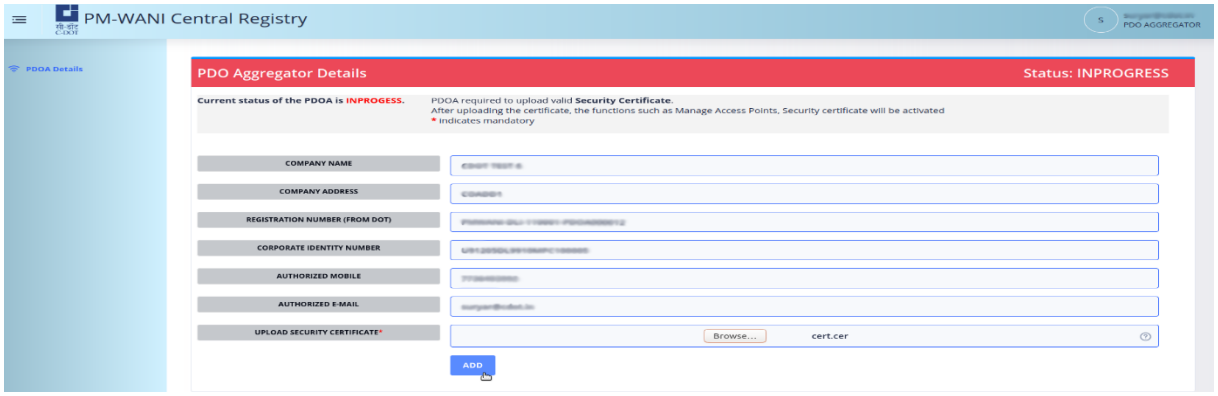


Figure 22- PDOA account becomes Active after adding a valid Security Certificate

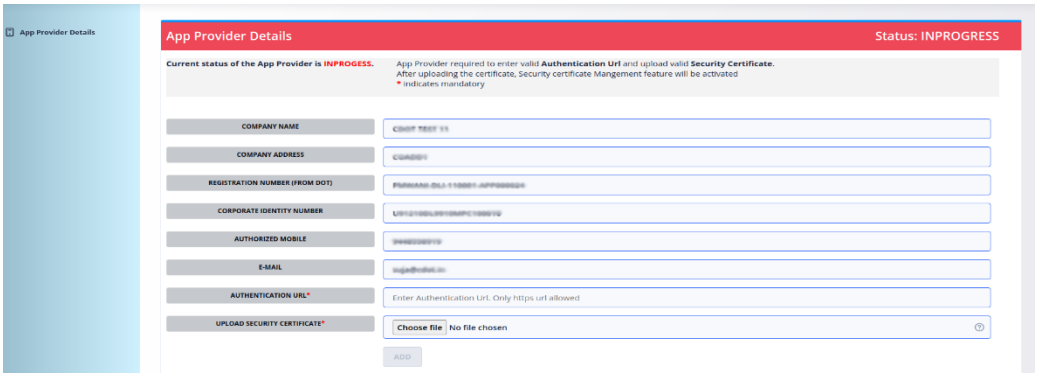


Figure 23- App Provider Security Certificate and Auth URL

6.1. MANAGE SECURITY CERTIFICATE

This section allows the PDOA user to view, edit and add multiple Security Certificates as per the PM-WANI Guidelines.

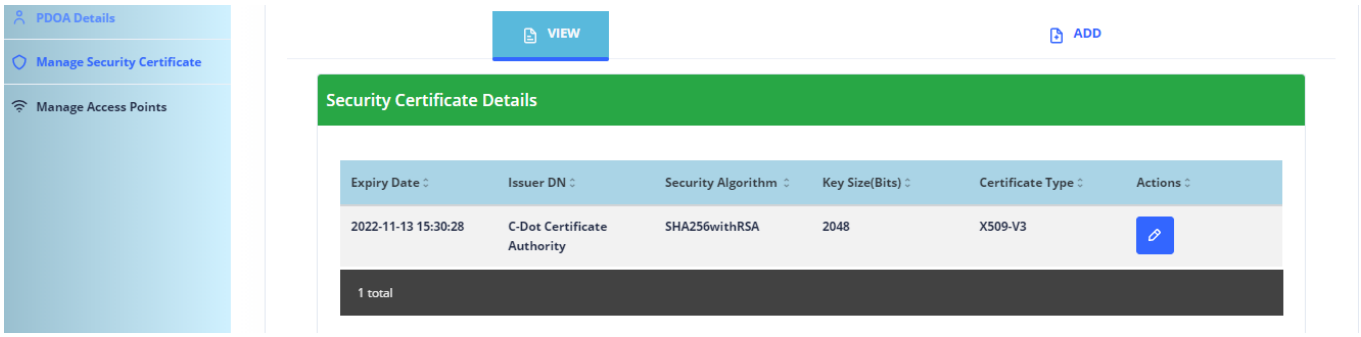


Figure 24- Manage Security Certificates Page

6.1.1. View Security Certificate

This section shows the list of the Security Certificates added by the user.

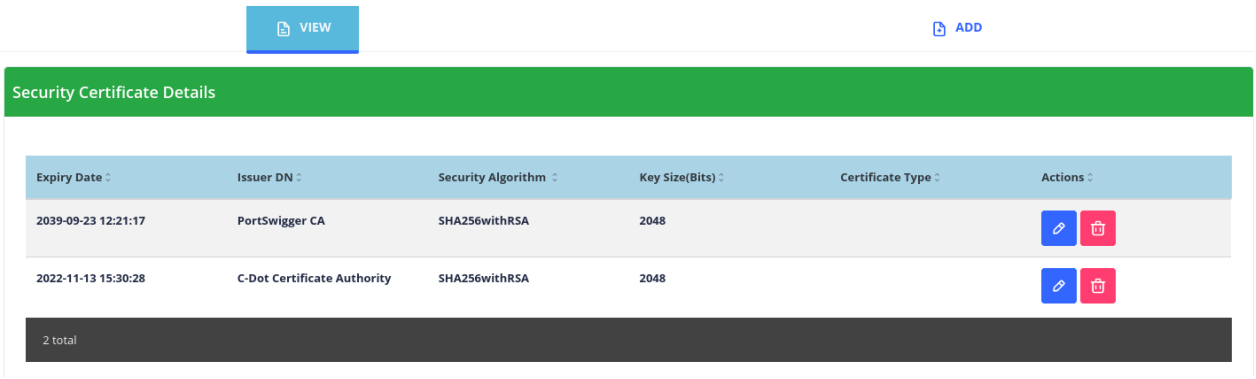


Figure 25- List of Security Certificates uploaded by user

6.1.2. Edit Security Certificate

The Edit button can be clicked to change the security certificate.

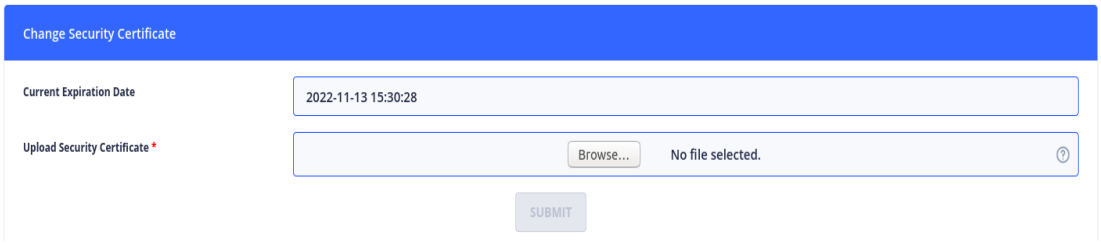


Figure 26- Edit Security Certificate

6.1.3. Add Security Certificate

New security certificates can be added by going to the ADD tab and uploading the new file.

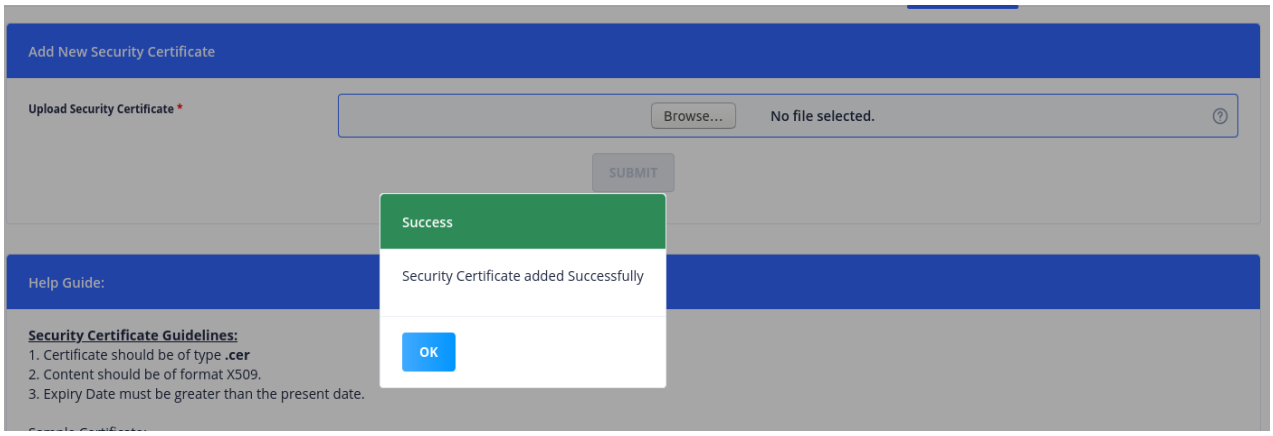


Figure 27- Successfully added Security Certificate

6.1.4. Delete Security Certificate

The Delete icon can be clicked to delete the security certificate if it is required.

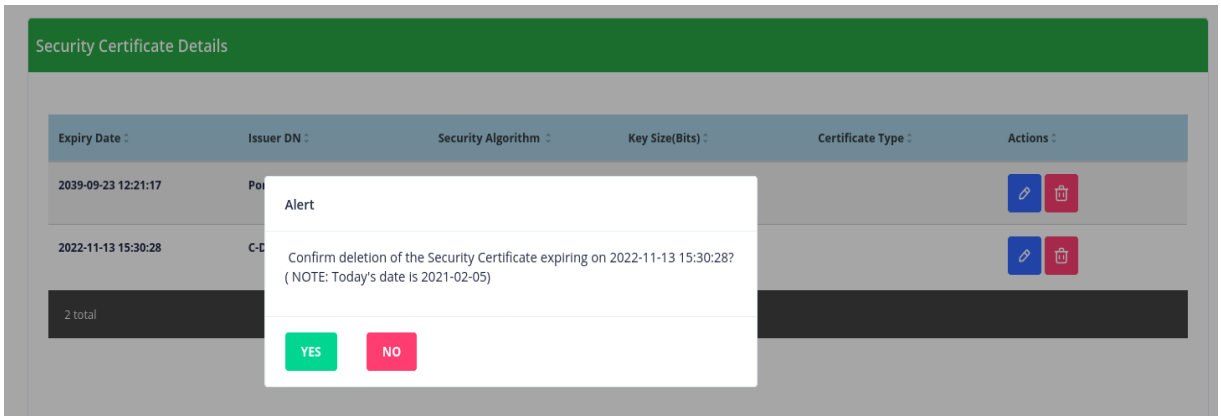


Figure 28- Confirm deletion of Security Certificate

Chapter 7.

PDOA's Access Point Management

The PDOA has to maintain the details of the Access Points deployed by the PDOs associated with it in the Central Registry. These details can be added one Access Point at a time by using the "Single Access Point" tab as described in Section. For the convenience of the PDOA, the "Bulk Upload" option is also provided as described in Section. After adding the access point details, the PDOA can view the information in the "AP Details" Section. If any Access Point detail is found to be incorrect, then that AP can be deleted as well.

The PDOA has to ensure that the Access Point details are maintained as per the following specifications:-

ATTRIBUTE	NEEDED	FORMAT
MAC ID	YES	6 Hexadecimal pairs (0 to 9, a to f, A to F) separated by: or -
SSID	YES	Alphanumeric String (min 5 to max 32 characters)
CAPTIVE PORTAL URL	YES	https URL of the Captive Portal Page
GEOLOCATION	Optional	Latitude and Longitude (in Decimal Degrees Format with max 6 decimal place accuracy) of AP's location
STATUS	YES	ACTIVE or INACTIVE
LOCATION NAME	YES	Character String
LOCATION TYPE	YES	DISTRICT
AVERAGE SPEED	Optional	Average speed offered to every user by AP. Value should in Mbps. It should be a positive integer.
FREE USAGE	Optional	Time for which access is free on the AP. If this AP offers any free band in minutes.

ATTRIBUTE	NEEDED	FORMAT
PAYMENT MODES	Optional	Payment modes supported by payment gateway of CP e.g. –Cash, Coupon, Credit card, Debit card, Net banking, UPI, Wallet.
OPERATING TIME	Optional	Operational time of AP. Value should be in the format hh-hh where hh represents time between 00 and 24

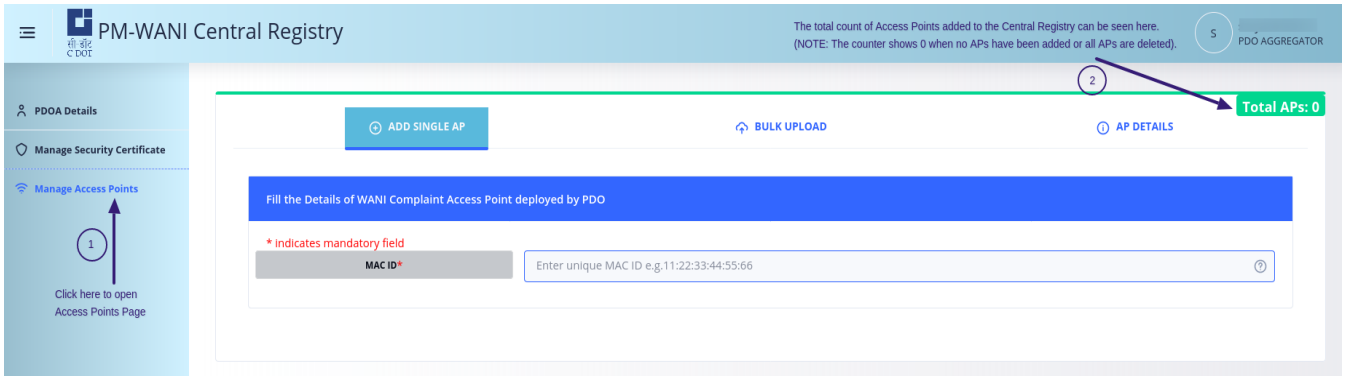


Figure 29- Manage Access Points Page

Initially the total number of Access Points present for a new PDOA is zero. When the PDOA adds the Access Point information, either using the "ADD SINGLE AP" or "BULK UPLOAD" tab, the total count of APs increases.

7.1. SINGLE ACCESS POINT

In this section, the following steps are to be taken to successfully add an access point:-

Step 1:

Ensure that the Access Point you are adding is not present previously in the Central Registry. The form will flag an error if MAC ID is already present as shown in Figure 25. If you have to update this access point information, then go to the "AP Details" tab and search for this AP by providing the MAC ID in the Search option. Delete the

AP and return to the "Add Single Access Point" tab to add the access point information.

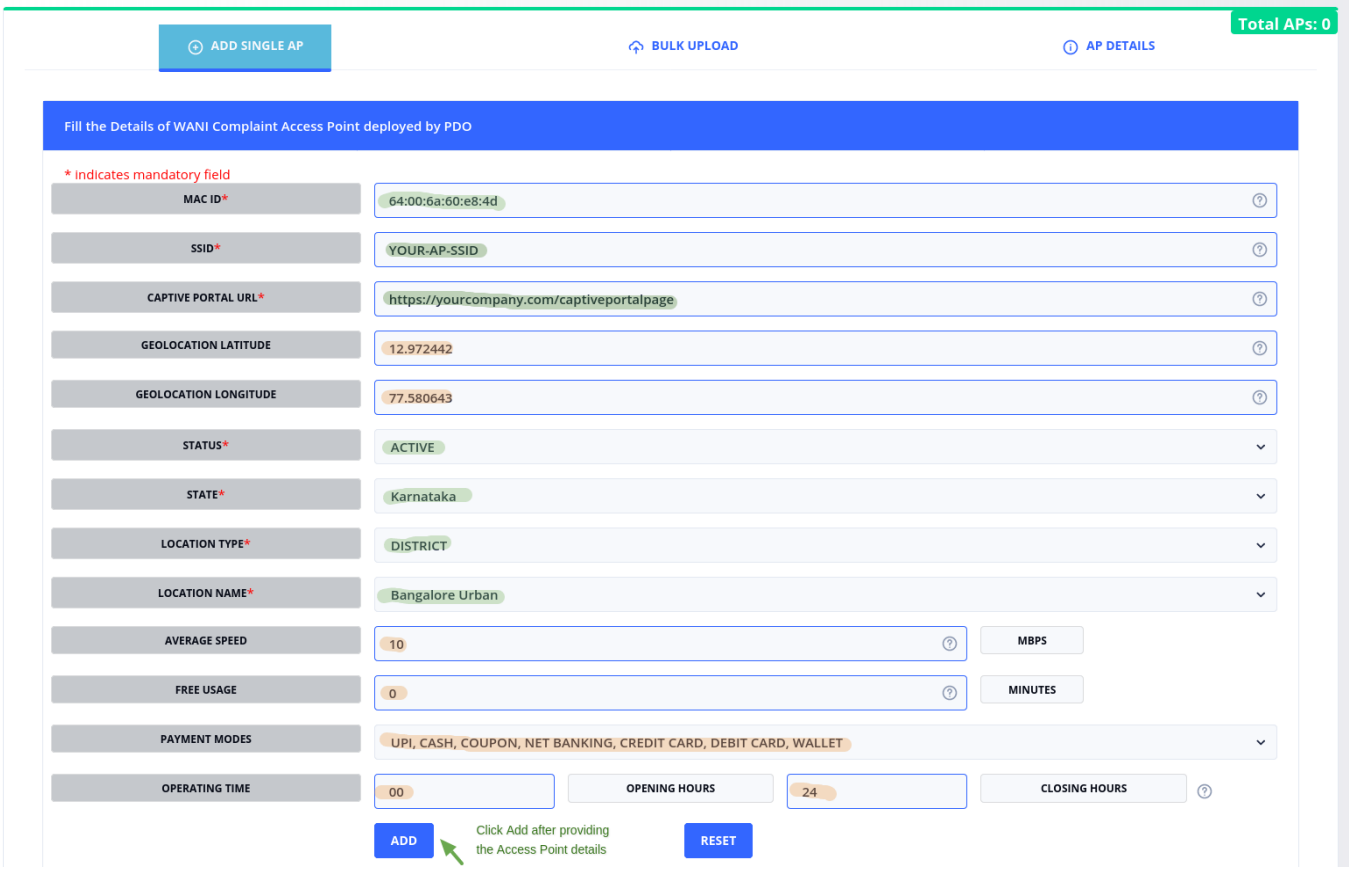


Figure 30- Giving a unique and valid MAC ID will open the Access Point form

Step 2: Start filling the form with the information of your Access Point. An example is shown below

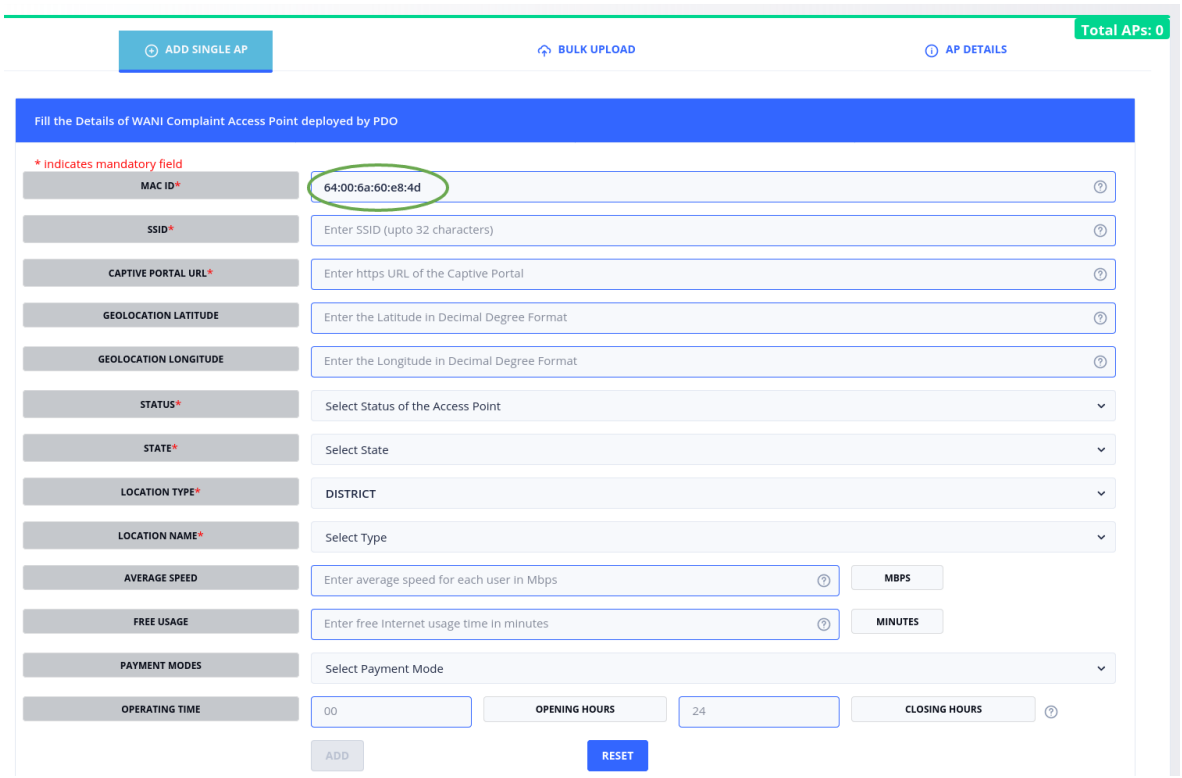


Figure 31- Completely filled Access Point Form

Please note that the fields highlighted in Green are mandatory fields and have to be filled to activate the "ADD" button. The fields highlighted in orange are optional fields and may be given. The "RESET" button can be used to reset the form to the state shown in Figure 22.

Step 3:

Click the "ADD" button. After clicking the "ADD" button, the Access Point details are successfully added. The counter will be increased by 1 as shown below.

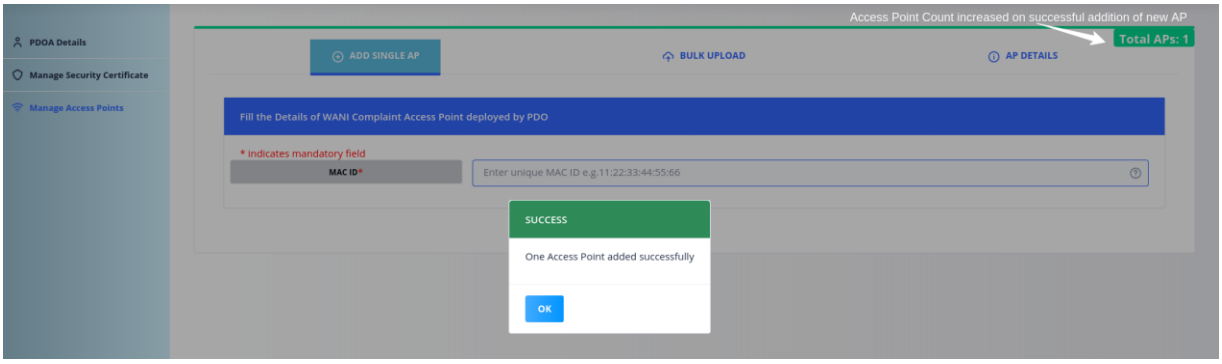


Figure 32- Single Access Point added successfully

Also, on trying to give the same MAC ID again, the following error will be flagged.

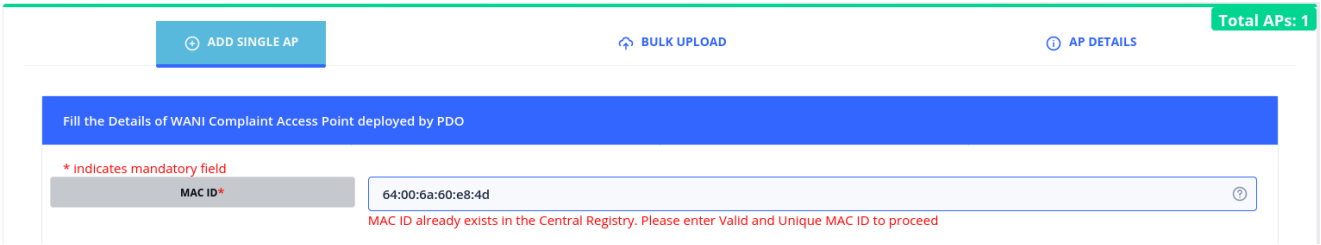


Figure 33- Existing MAC ID in the Central Registry will not be accepted again. Delete the entry and try again.

Please refer to Section 6.3 to view the details of the Access Point added.

7.2. BULK UPLOAD OF ACCESS POINTS

In this tab, multiple access points can be added to the Central Registry at a time. To do so, a **CSV (comma-separated values) file** has to be uploaded. The following steps have to be taken: -

Step 1: Download the sample.csv file.

Step 2: Download the Guidelines document. Read the instructions.

Step 3: Create your csv file & upload it. Please ensure that the guidelines and format is followed.

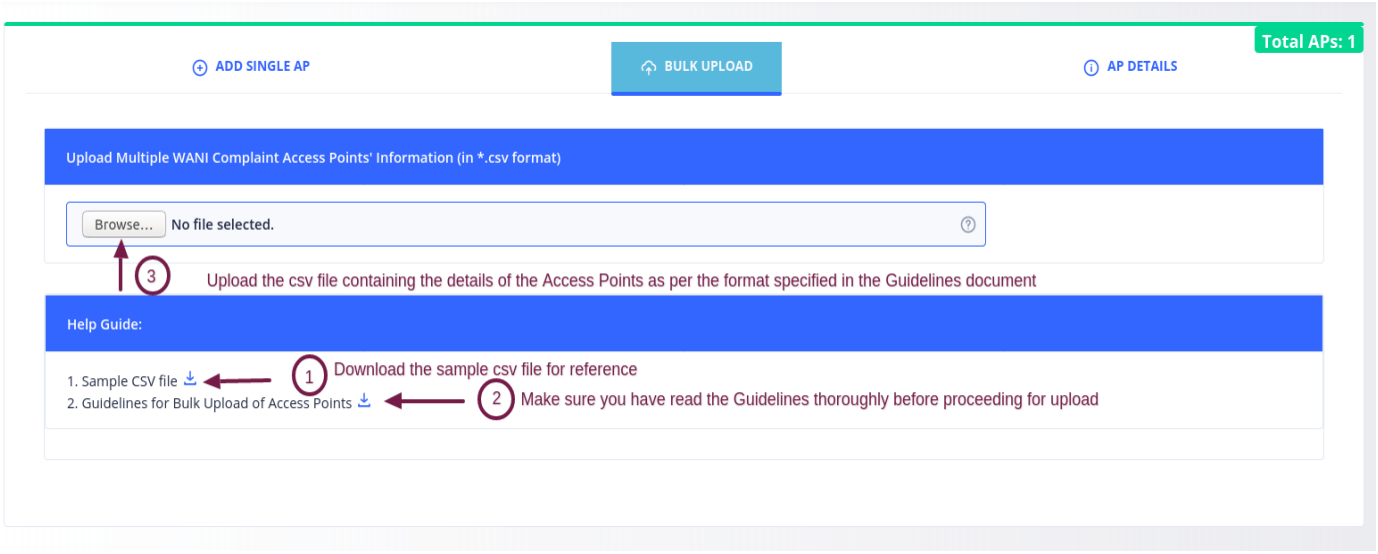


Figure 34- Bulk upload of Access Points Page

After the CSV file is uploaded by the PDOA, the file is parsed and all the incorrect entries are added to a separate CSV file. The error details and the line numbers are shown in a text file also. If any such invalid entries are seen as shown in the Figure below, please take the following steps:-

Step 1: Download the invalid entries zip file containing the aforesaid CSV file and text file.

Step 2: Close the pop-up to see the list of the correct AP details.

Step 3: Click the "ADD" button to add the correct entries to the Central Registry.

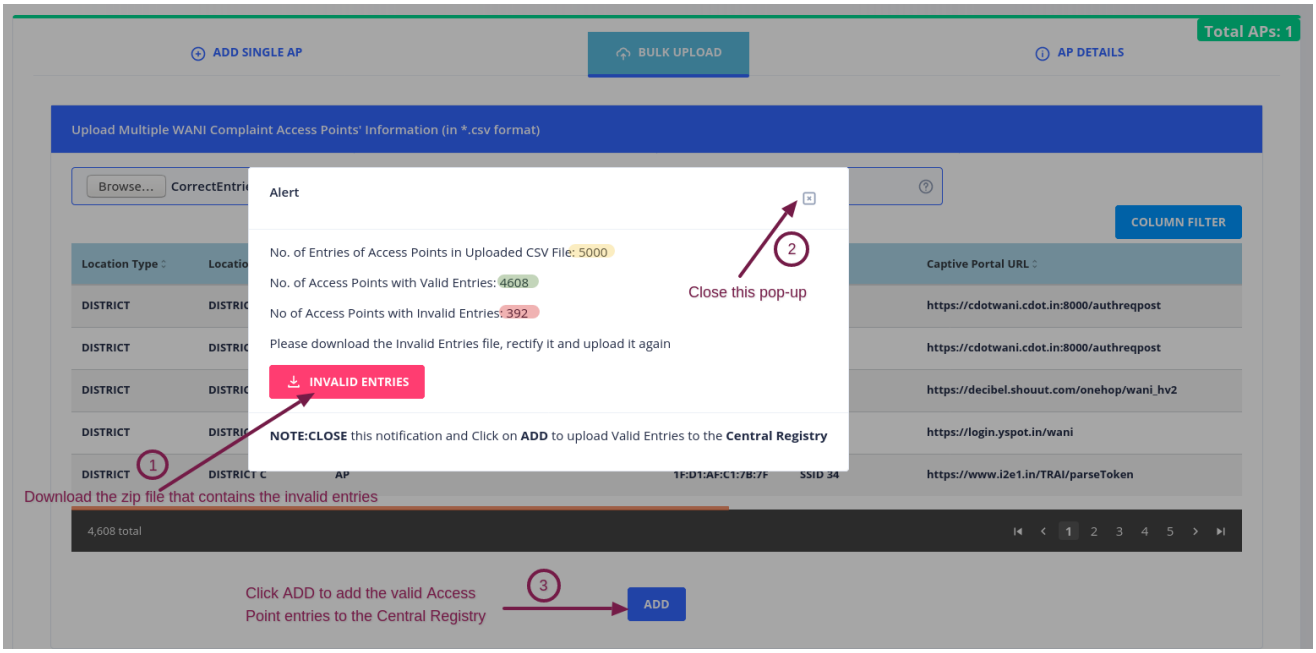


Figure 35- Parsing results with total entries (yellow), correct entries (green) and incorrect entries(red)

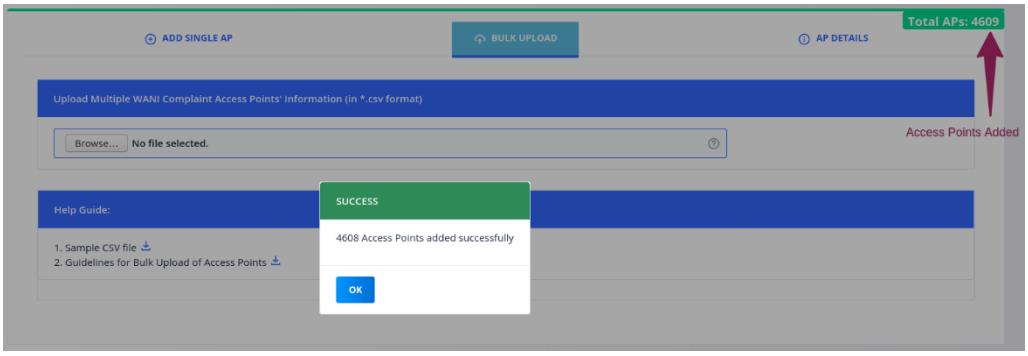


Figure 36- Please wait for the Access Points information to be added to the Central Registry

Step 4: Open the zip file to check the reason why the entries were flagged as incorrect. The following errors are possible: -

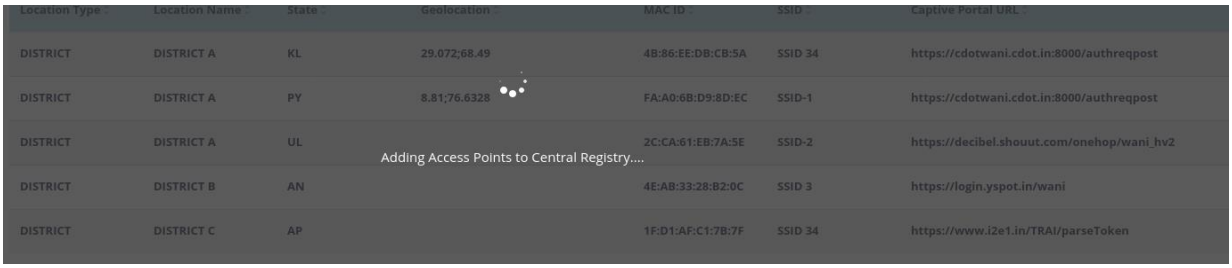


Figure 37- Successful addition of Access Points in Bulk Upload

1. Incomplete Mandatory Fields (When some mandatory field is missed)

   e.g. – East Sikkim,SK,DISTRICT,27.2166;88.3333,11:16:51:C2:0C:60,SSID-3,INACTIVE,OPENBETWEEN:09-17

   Above entry is missing the Captive Portal URL in the fourth field

2 Extra fields (When there are more fields than expected)

   e.g. - East Sikkim,SK,DISTRICT,,https://mycompany.in/cppage,,, 27.2166; 88.3333,EC-Cf:A8:e3:ae-Dd,SSID 21,ACTIVE

   There is an extra comma which increases the number of fields to more than expected.

3 Invalid Entries (When the format of the data provided is incorrect as per the Guidelines)

   e.g. - Sikkim,SK,DISTRICT,http://mycompany.in/cppage, 27.2166; 88.3333,EC-Cf:A8:e3:ae-Dd,SSID 21,ACTIVE

Above entry is have http URL instead of https URL

4 Repeated MAC IDs (When the MAC ID is duplicate in the CSV file uploaded)

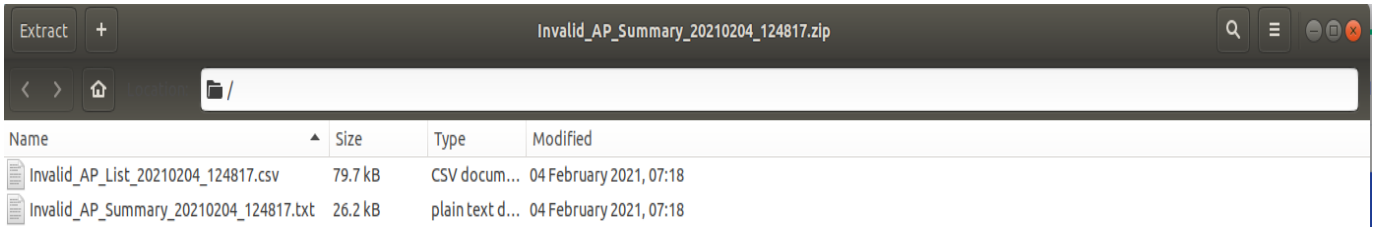


Figure 38- Contents of zip file

The zip file can be opened to see the enclosed text and CSV files as

Shown below:

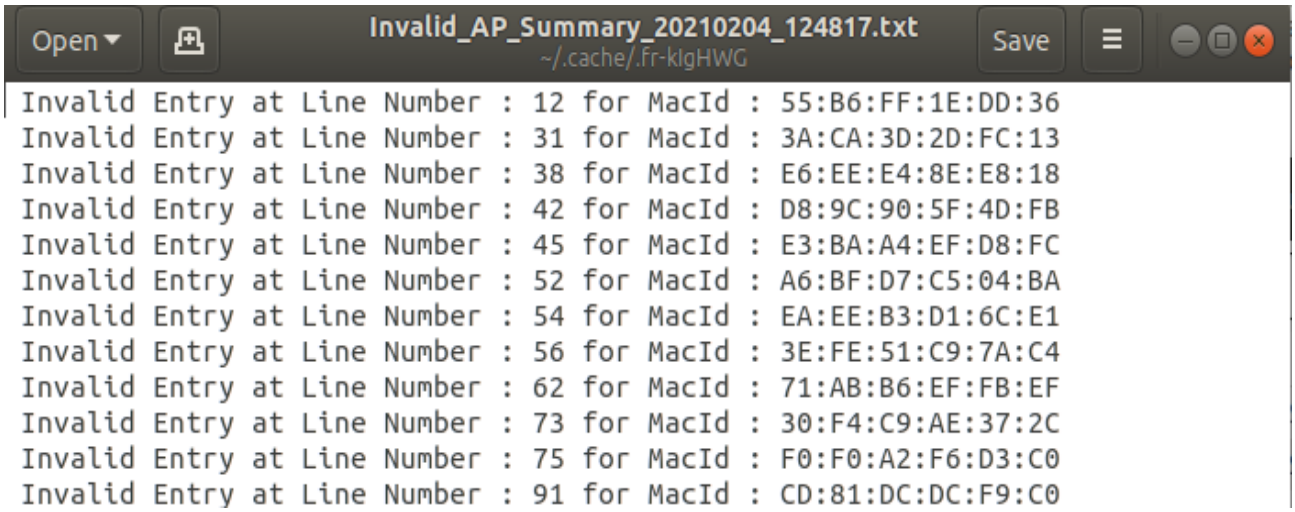


Figure 39- Incorrect Entries Description

The incorrect entries are highlighted with the MAC ID and line number. These entries can be seen in the original CSV file uploaded or can be directly rectified in the CSV file present in the zip file. After rectification, this new CSV file can be uploaded again.

7.3. VIEW ACCESS POINT INFORMATION

In this section, the PDOA can view all the information of the access points it has added to the Central Registry. The default page shows latest 5 AP entries made by the PDOA. Further entries can be viewed by clicking the page numbers.

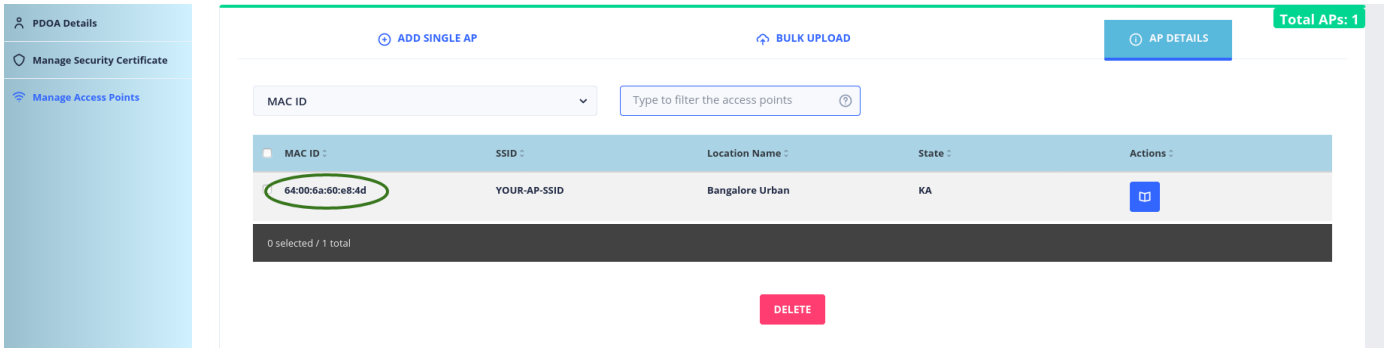


Figure 40- AP Details after adding single Access Point in Section 6.1

Each of these AP's details can be viewed in detail by clicking the View More icon present at the rightmost column as shown below:

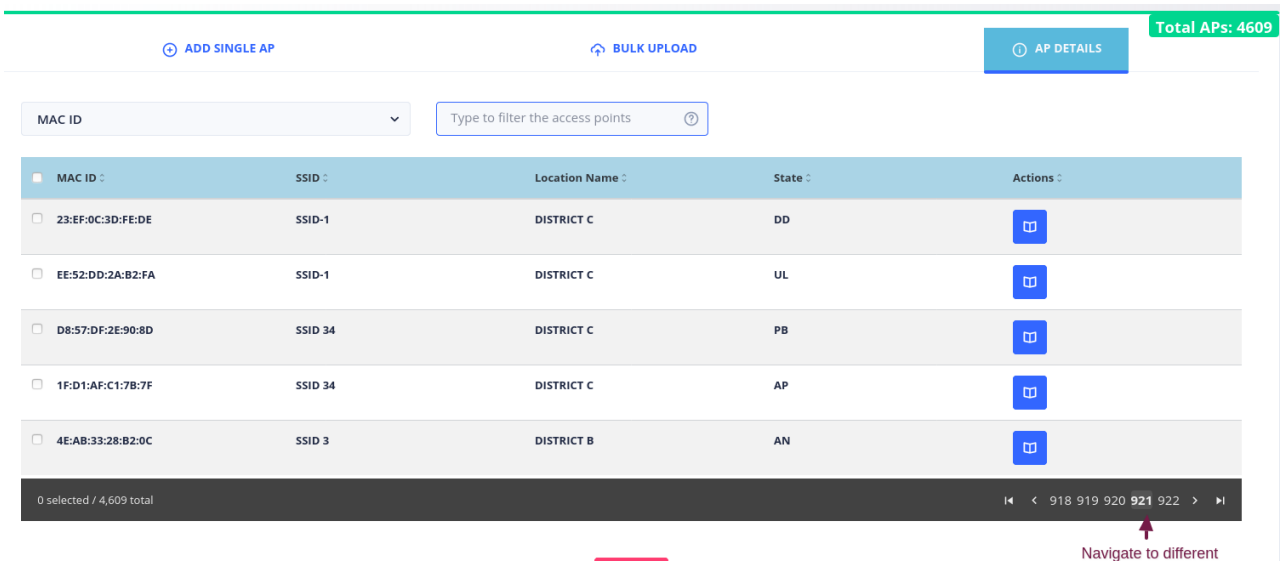


Figure 41- AP Details Page after Bulk Upload of 4608 Access Points in Section 6.2

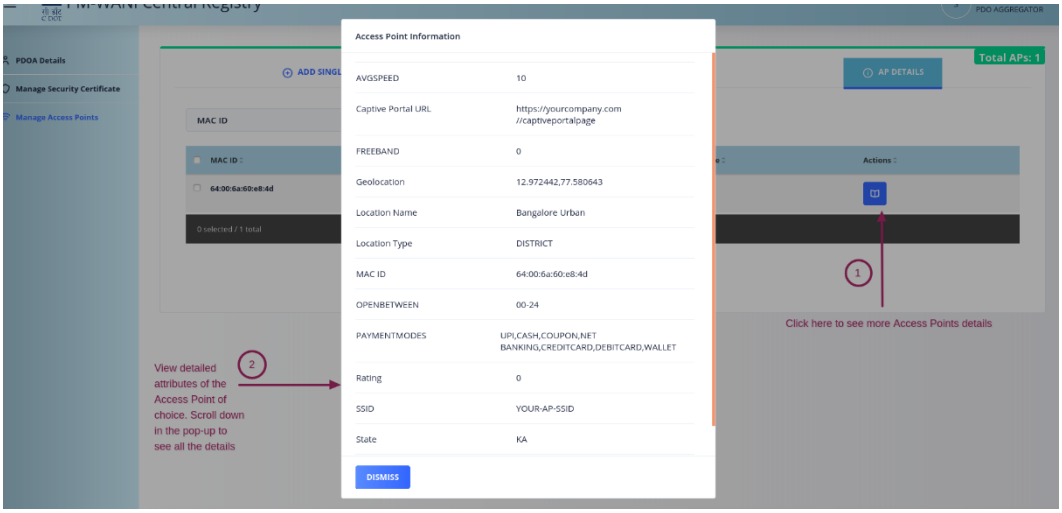


Figure 42- Access Point detailed view

7.3.1. View Filtered Access Points

The Access Points can be filtered on the basis of the MAC ID, SSID, Location Name or State

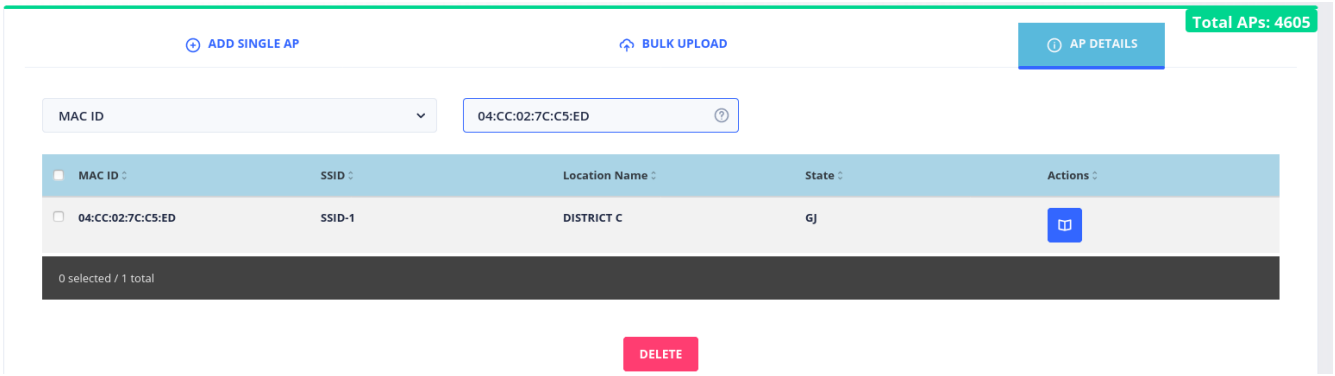


Figure 43- Searching by complete MAC ID of the AP will show exactly one AP since only unique MAC IDs are present in the CR

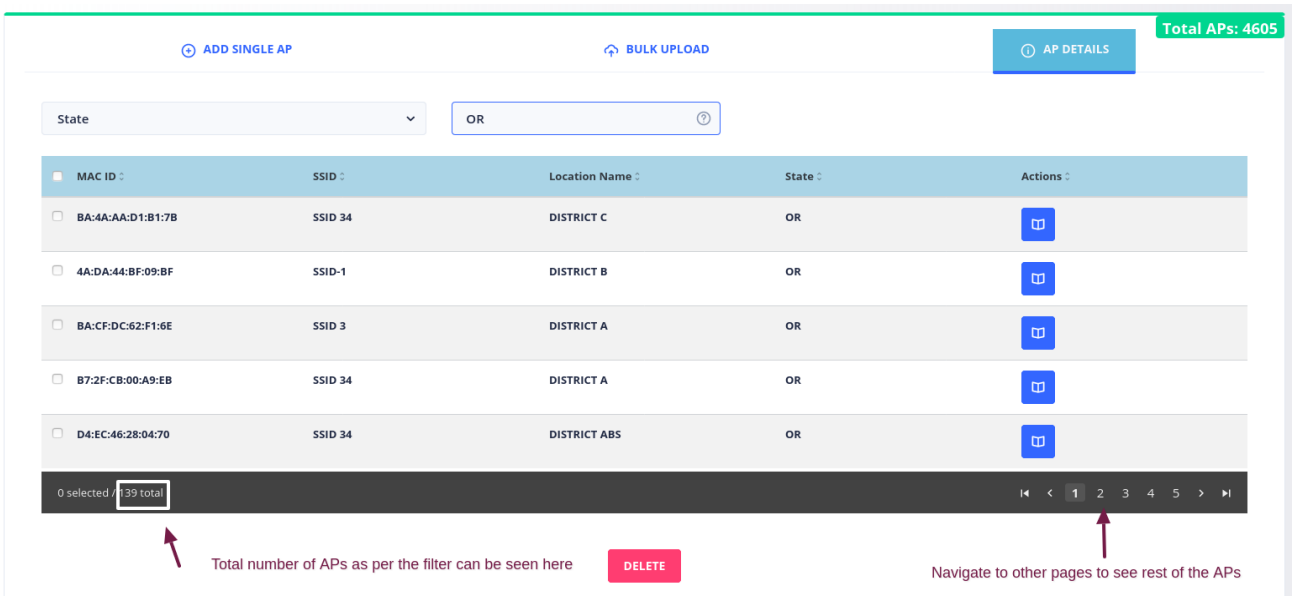


Figure 44- Filter for State by its abbreviation

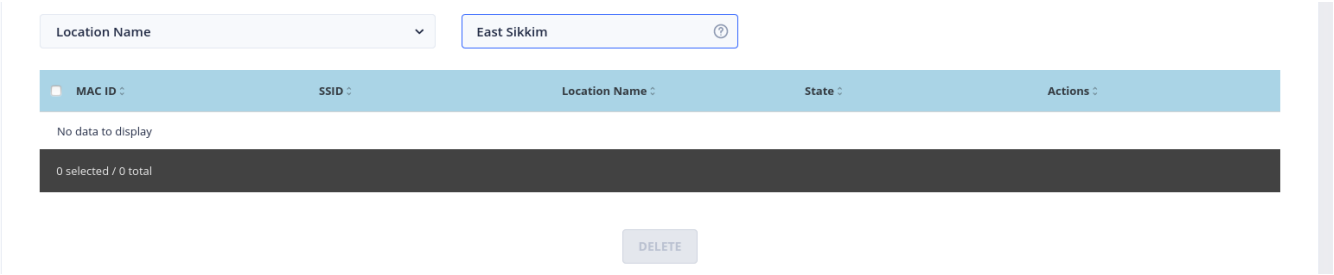


Figure 45- No Access Point are found by the search filter applied

7.4. DELETE ACCESS POINTS

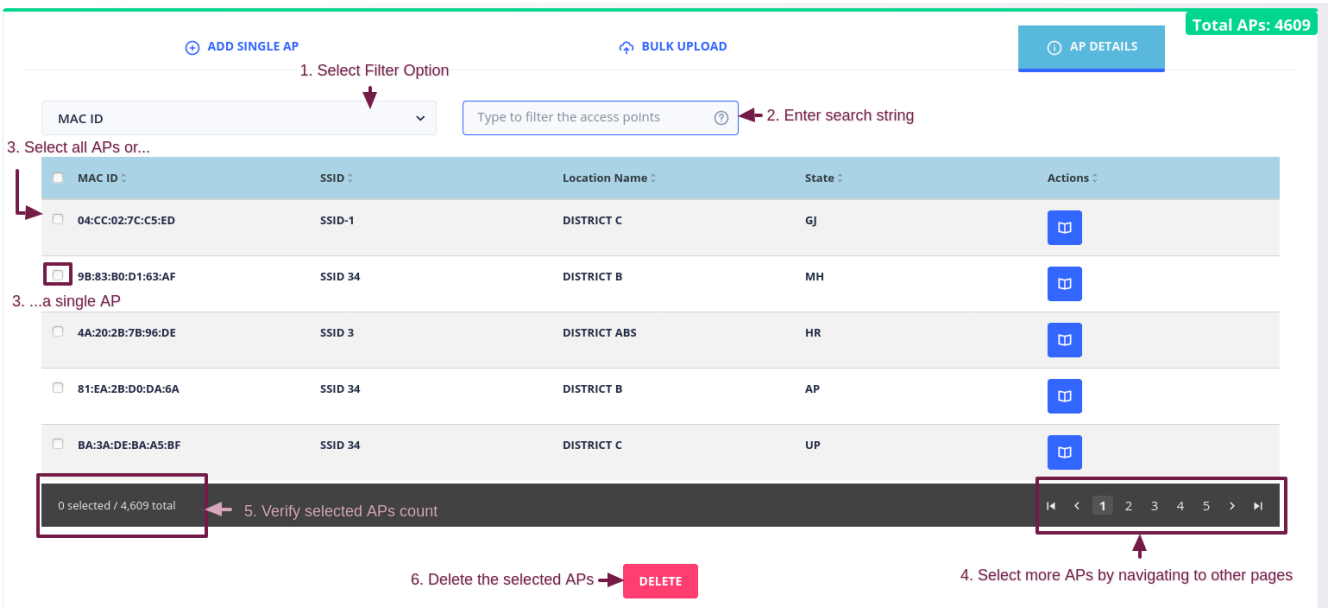


Figure 46- Steps to delete Access Point(s)

Deletion of the Access Points can be done by following the steps shown below:-

Step 1: Select the Filter Option i.e. MAC ID/ SSID/ Location Name/ State

Step 2: Enter the search string and search for the APs as per the required filter

Step 3: Select all the APs in list displayed or select individual APs to be deleted.

Step 4: Navigate to rest of the pages to select more APs for deletion

Step 5: Verify that the correct number of APs are selected

Step 6: Click the DELETE button

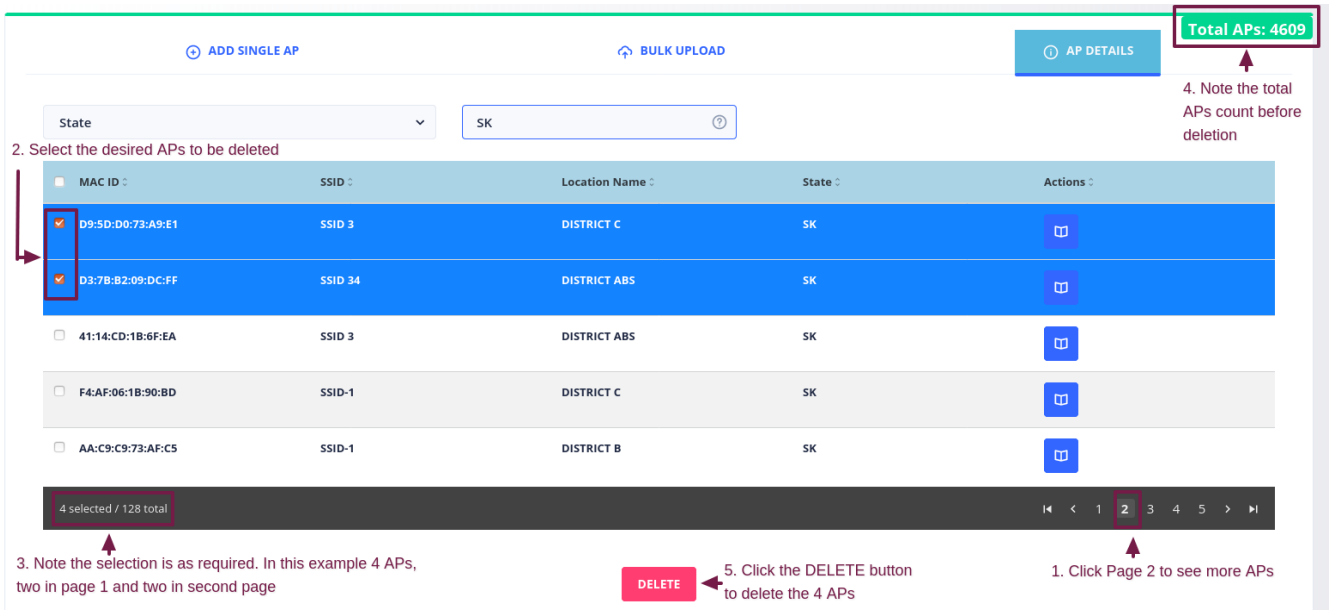
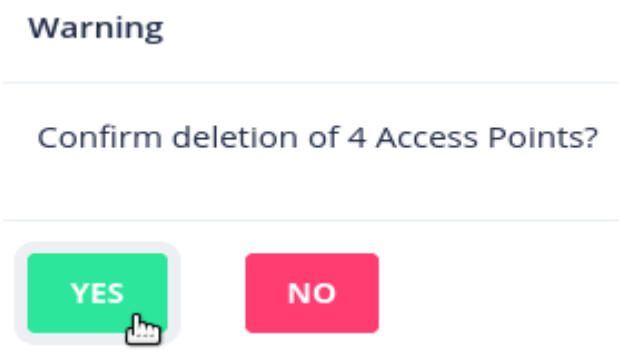


Figure 47- Example of deletion: 4 APs in the State of Sikkim

A pop-up will come to confirm the deletion of the APs. Click yes to confirm and proceed for deletion.



After deletion is confirmed, a pop-up notification will be shown at the top right corner and the AP(s) will be deleted.

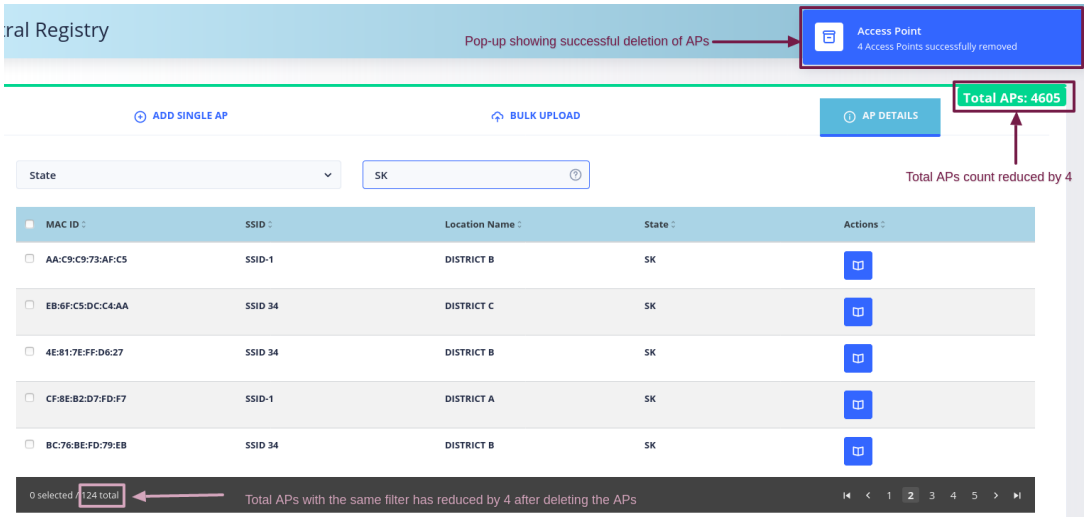


Figure 50- Steps to delete Access Point(s)

7.5. UPDATE ACCESS POINT INFORMATION

An Access Point's data can be updated by first deleting it from the Central Registry by following the steps mentioned in Section 6.4. After deleting it, it can be added in the "Add Single AP" tab as described in Section 6.1 with the updated values.

Chapter 8.

App Provider's Authentication URL

This information has to be provided by the App Provider after getting Provisionally Certified. It has to be given along with the Security Certificate. The auth URL can be edited if it is changed, by clicking the Edit button as shown below:-

Figure 48- Change the auth URL

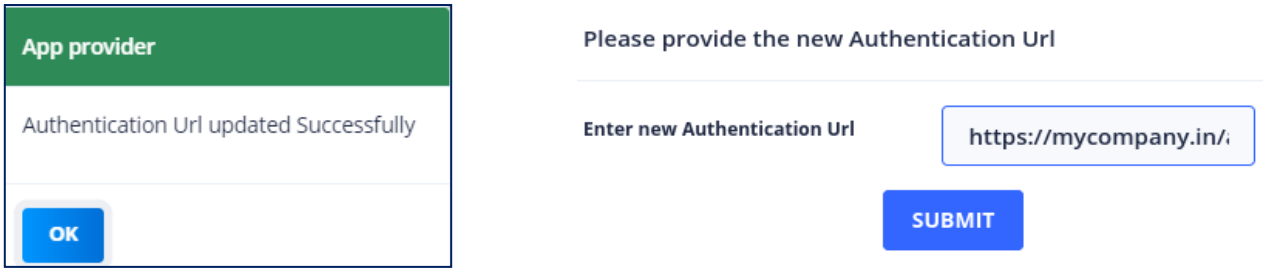


Figure 49- Authentication URL successfully updated

END