



IMMUNITY NETWORKS · eBOOK

The PM-WANI Playbook

Everything you need to launch and run a compliant, profitable public Wi-Fi business in India under PM-WANI.

A Make-in-India OEM guide

immunitynetworks.com · +91 91367 90819

Contents

1. What is PM-WANI
2. How to become a PM-WANI PDO

Compiled from the Immunity Networks knowledge base. For tailored design help, contact our engineers.

1. What is PM-WANI

PM-WANI (Prime Minister Wi-Fi Access Network Interface) is the Government of India framework that lets anyone — from a tea shop to a telecom operator — offer public Wi-Fi without a licence. For entrepreneurs and operators it is one of the most accessible connectivity businesses in the country. This guide breaks down how it works and what you need to run it well.

The four PM-WANI roles

The framework defines four participants. A Public Data Office (PDO) owns the hotspot — the local shop or venue that sells Wi-Fi. A Public Data Office Aggregator (PDOA) provides the platform, authorisation and accounting for many PDOs. An App Provider runs the consumer app that discovers hotspots and signs users in, and the Central Registry maintained by C-DoT ties it together.

The commercial point is simple: a PDOA can sign up hundreds or thousands of PDOs, each a revenue-sharing hotspot, with no telecom licence required. The technology has to handle onboarding, billing and compliance at that scale.

What you actually need to deploy

Three things make or break a PM-WANI rollout: certified hardware, a flexible captive portal, and compliant logging.

Certified access points. Your hotspots must be reliable in the field and meet Indian certification. Immunity offers India's first PM-WANI certified access point in the Lotus Alpha range, built and supported in India.

A captive portal that converts. Users meet your splash page first. It needs app-based onboarding, vouchers or prepaid plans, and a clean branded experience. Our captive portal and Gateway Controller handle authentication, bandwidth tiers and billing.

Central IPDR logging. Public Wi-Fi in India carries a legal duty to retain Internet Protocol Detail Records. Net Cloud centralises tamper-evident IPDR with configurable retention so audits are straightforward.

Turning Wi-Fi into recurring revenue

The economics work when you can meter and monetise. Define free and paid tiers, sell time or data passes, and settle revenue across PDOs automatically. Done well, each hotspot becomes a small recurring-revenue node, and the PDOA platform is the business.

Where Immunity fits

We provide the full stack — certified APs, gateway, captive portal, billing and central IPDR — managed from a single console, with local Indian support. See how this runs in production in our public Wi-Fi case study, then talk to our team about your deployment.

2. How to become a PM-WANI PDO

PM-WANI (Prime Minister Wi-Fi Access Network Interface) lets almost anyone in India offer paid public Wi-Fi — without a telecom licence and without heavy capital. If you run a shop, a café, a society or a small ISP, becoming a Public Data Office (PDO) is one of the most accessible connectivity businesses in the country. This guide walks through exactly how to do it.

What is a PDO, and where do you fit?

PM-WANI defines four roles. A PDO owns the physical hotspot and sells Wi-Fi to end users — this is you. A PDO Aggregator (PDOA) provides the cloud platform that authorises users and handles accounting for many PDOs. An App Provider runs the consumer app that discovers hotspots and signs people in. The Central Registry, maintained by C-DoT, ties everyone together. As a PDO you don't need a licence; you partner with a registered PDOA who handles the regulated parts.

Step 1 — Decide your location and demand

Public Wi-Fi earns where people dwell and need data: tea shops, markets, bus stands, residential societies, hostels, clinics and rural commercial streets. Estimate daily footfall and how long people stay. A spot with 100+ daily users who linger is a viable hotspot; a location people pass through in seconds is not. Start with one or two strong locations rather than spreading thin.

Step 2 — Choose a PDOA

Your PDOA is your platform partner. They provide the captive portal, user authentication, billing and the mandatory compliance logging. Evaluate them on: certified hardware support, a flexible and branded captive portal, transparent revenue-share, reliable billing and settlement, and proper IPDR logging. A weak PDOA means a weak business, so choose carefully.

Step 3 — Get PM-WANI compliant hardware

Your hotspot needs a reliable, certified access point. Cheap consumer routers fail in the field and may not meet certification. Immunity offers India's first PM-WANI certified access point, available in indoor and ruggedised outdoor models, built and supported in India. For multi-AP sites you'll also want a small managed switch and the Gateway Controller for the captive portal and billing.

Step 4 — Register and go live

Working with your PDOA, your hotspot is registered with the PM-WANI Central Registry. The PDOA configures the captive portal (your branding, the sign-in method — OTP, app or voucher), sets your tariffs, and connects billing. Once registered and configured, users discover your hotspot in a PM-WANI app, authenticate and buy access. You're live.

Step 5 — Stay compliant (IPDR & retention)

Public Wi-Fi in India carries a legal duty to retain Internet Protocol Detail Records (IPDR) and related logs for the period mandated by the Department of Telecommunications. A good PDOA and platform — for example Immunity Net Cloud — centralises tamper-evident IPDR with configurable retention, so audits are straightforward and you stay on the right side of the rules.

How the money works

PDOs typically sell access in time or data bundles — for instance a small charge for an hour, a day or a weekly pass — with revenue shared between PDO, PDOA and app provider. Margins come from volume:

each hotspot is a small recurring-revenue node, and the business grows as you add locations. Premium tiers (faster speed, higher quota) and local advertising can add to the base. Run the numbers for your footfall before scaling.

Common mistakes to avoid

The usual failures are: buying uncertified consumer hardware that dies outdoors; picking a PDOA on price alone; ignoring the captive-portal experience (a clumsy login kills conversion); and treating compliance as optional. Get those four right and a PDO is a genuinely viable micro-business.

Getting started with Immunity

Immunity provides the full PDO stack — certified access points, gateway, captive portal, billing and central IPDR — with local Indian support. Read our PM-WANI solution, see a public Wi-Fi case study, or talk to our team about your first hotspot.