Raspberry Pi Quick-Start Guide for M5 Monitoring (PTAGIS)

1 Overview

This guide walks you through preparing a Raspberry Pi 4 or 5 for field-ready operation with PTAGIS M5 monitoring software. It covers hardware selection, OS imaging, secure networking, software installation, and maintenance best practices.

2 Hardware & Supplies

- Raspberry Pi 4 (2 GB +) or Raspberry Pi 5 — product page: https://www.raspberrypi.com/products/
- Official 5 V 3 A USB-C power supply
- 32 GB + Class 10/UHS-1 micro-SD card — consider industrial-grade for harsh environments
- Rugged case (IP-rated if outdoors) and passive heatsinks
- HDMI cable, USB keyboard + mouse, monitor (for first boot)
- Ethernet cable and reliable Internet connection
- Optional: UPS HAT or PoE HAT, surge-protected power strip, desiccant packs for enclosure

3 Prepare the micro-SD Card

1. Download and install **Raspberry Pi Imager** (https://www.raspberrypi.com/software/).
2. Insert the micro-SD card into your computer.
3. Launch Raspberry Pi Imager → **Choose OS** → *Raspberry Pi OS (32-bit, Bookworm)*.
4. Click the ⚙ Advanced Options button to pre-set:
   - Hostname (e.g., `rpi-m5-site1`)
   - Enable SSH and set a strong password or upload an SSH key
   - Configure Wi-Fi SSID/PSK and country code (if using Wi-Fi)
   - Locale and keyboard layout
5. Click **Write** and wait for completion, then safely eject the card.
6. Insert the card into the Pi, connect peripherals, and power up.

4 First Boot & System Update

On first boot, complete the graphical setup wizard if you didn't pre-seed settings. Open a terminal and run:

```
sudo apt update && sudo apt full-upgrade -y
```

Enable required interfaces via **raspi-config** → *Interface Options*: SSH, VNC, I2C as needed. Reduce GPU memory to 16 MB on headless deployments to free RAM.

5 Install Prerequisite Packages

Install general dependencies before M5 (adjust as required by future releases):

```
sudo apt install -y git curl libserialport-dev
sudo apt install -y watchdog unattended-upgrades mosquitto-clients  # optional
```

6 Install M5 Software

Download the latest ARM package from **PTAGIS M5 Downloads** (https://www.ptagis.org/software/m5). Choose armhf for Raspberry Pi 4 or arm64 for Raspberry Pi 5.

Install by double clicking on the *.deb file that was downloaded or

Copy the `.deb` file to the Pi (e.g., into `~/Downloads`).

Install:

```
sudo dpkg -i ~/Downloads/m5_*.deb
sudo apt -f install  # pulls any missing dependencies
```

Check service status:

```
sudo systemctl status m5
```

Open the local web interface at `http://<pi-ip>:5440` and create or import your site profile.

7 Configure Static Networking

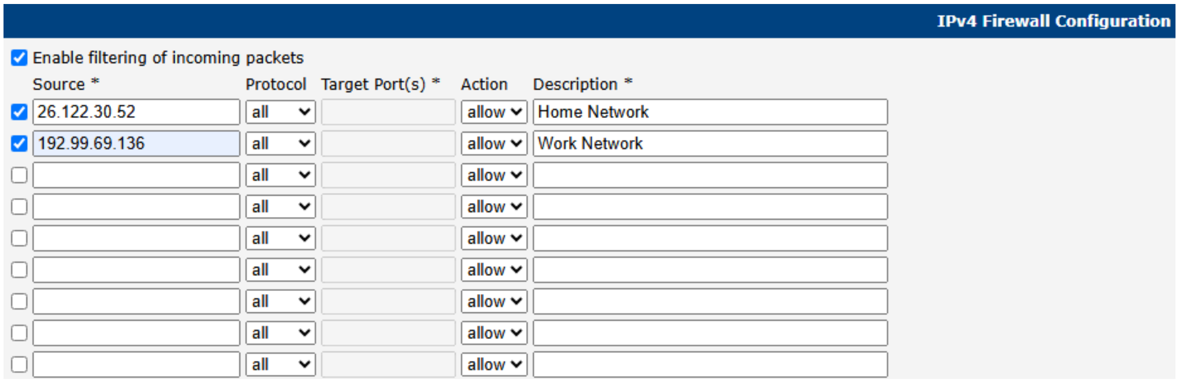
Edit `/etc/dhcpcd.conf` to assign the Pi a fixed LAN address so the router can forward external traffic reliably:

```
interface eth0
static ip_address=192.168.1.24/24
static routers=192.168.1.1
static domain_name_servers=8.8.8.8
```

Reboot with `sudo reboot` and verify using `ip a`.

8 Secure Remote Access

- **Port Forwarding** – map external TCP 5440 to the Pi's internal 192.168.1.24:5440.
- **Whitelist trusted IPs** in the router/firewall to limit who can reach the port (e.g., allow 203.0.113.5/32). Combine with a Dynamic DNS hostname if your client IP changes infrequently. See example below:



IPv4 Firewall Configuration

☑ Enable filtering of incoming packets

	Source *	Protocol	Target Port(s) *	Action	Description *
☑	26.122.30.52	all		allow	Home Network
☑	192.99.69.136	all		allow	Work Network
☐		all		allow	
☐		all		allow	
☐		all		allow	
☐		all		allow	
☐		all		allow	
☐		all		allow	
☐		all		allow	

- **SSH Hardening** – create key-based authentication (`ssh-keygen`), disable password login by setting `PasswordAuthentication no` in `/etc/ssh/sshd_config`.
- For highest security, deploy **WireGuard** or **OpenVPN** instead of exposing ports.
- Verify from off-site: `curl http://<public-ip>:5440` should return the M5 banner.

9 Monitoring & Maintenance

- Enable the hardware watchdog: `*sudo systemctl enable watchdog && sudo systemctl start watchdog*`.
- Turn on automatic security updates: `*sudo dpkg-reconfigure --priority=low unattended-upgrades*`.
- Check M5 logs live: `*journalctl -u m5 -f*`.
- Schedule a weekly reboot (optional) via `sudo crontab -e`: `0 3 * * 0 /sbin/reboot`.
- Keep an up-to-date cloned SD card in your field kit for rapid swap-outs.

10 Backups & Cloning

Use **Raspberry Pi Imager → Clone Drive** or tools like **rpi-clone** and **Clonezilla** to create full-disk images. Store at least one verified copy off-site.

11 Field Deployment Tips

- Use braided or conduit-protected cabling to reduce rodent damage.
- Label ports and power leads clearly; document the LAN layout in the site-profile.
- Place the Pi in a ventilated, shaded enclosure; keep temperatures below 70 °C.
- Add a small silica-gel pack to prevent internal condensation.
- Bring a USB-to-TTL serial debug cable for emergency headless access.

12 Troubleshooting Cheatsheet

```
`journalctl -u m5 -n 50`  # recent M5 logs

`ping 8.8.8.8`          # test WAN reachability

`vcgencmd measure_temp`   # check CPU temperature

`df -h`                 # verify free disk space

`sudo systemctl restart m5`  # restart service
```

13 Resources & Links

- Raspberry Pi Imager – https://www.raspberrypi.com/software/
- Raspberry Pi OS – https://www.raspberrypi.com/software/operating-systems/
- PTAGIS M5 Documentation – https://www.ptagis.org/software/m5
- Linux Command Handbook – https://www.freecodecamp.org/news/linux-command-cheat-sheet/
- Clonezilla – https://clonezilla.org/
- WireGuard – https://www.wireguard.com/