Fleet 3 Network, Router, Wi-Fi, and MDC Config Guide

Rev: 30 Sep 2024

Axon Enterprise, Inc.
17800 N 85th St
Scottsdale AZ 85255
USA

Contents

Router and VPN configuration **1**
Router configuration 1
Cradlepoint configuration 1
Requirements 1
Recommendations 1
VPN configuration 2
Local traffic 2
Video upload 2

MDC configuration **3**
MDC system requirements 3
Multicast DNS 3
Firewall settings 3
Proxy settings 4
Dashboard notifications 4

Cradlepoint router configuration **5**
Configuration for Wi-Fi-connected dashboard 5

Router and VPN configuration

This guide describes requirements, recommendations, and configuration information for the network, router, Wi-Fi, mobile data computer/terminal (MDC/T, hereafter referred to as just MDC) and mobile computing devices (Android and iOS) for Axon Fleet 3 common deployments.

For installation of the Fleet Dashboard application, see the first topic in the **Dashboard operation** section for your operating system on the Fleet 3 product page.

Router configuration

The Axon Fleet 3 Hub and MDC require ethernet connections to the in-vehicle router to communicate with the Axon Service (such as Axon Evidence) through cellular (3G/LTE/5G) and/or Wi-Fi connections. Axon does not provide cellular service or a SIM card. Customers using an APN or VPN may require special configurations, including firewall exemptions, to enable communication between Fleet Hub and Axon Service.

Axon Fleet 3 uses the Local Area Network (LAN) of the in-vehicle router to communicate with the MDC and the router's Wide Area network (WAN) to communicate with Axon Service.

Cradlepoint configuration

For a Cradlepoint router, follow the configuration requirements in Cradlepoint router configuration on page 5.

Requirements

- Hub must be connected directly to router's LAN ethernet port
- For best experience, MDC should also be connected to router's LAN ethernet port; if you prefer to connect your MDC to your router over Wi-Fi, contact your Axon representative
- MDC and hub must be on the same subnet
- Change the router local domain to "local"

Recommendations

- Ignition sensing capability with power off delay configured to match Axon Fleet 3's **Power Off Delay** setting

VPN configuration

Depending on your agency configurations, a VPN may force all IP-based traffic to travel through its tunnel to a remote network. To allow software residing on the MDC to communicate locally to the hub, the traffic must be exempt from the tunnel.

A VPN administrator must be available during Axon Fleet installation.

Local traffic

Use a split tunnel to ensure local network traffic and traffic destined for port 5353 (mDNS) do not flow through the VPN. Refer to your VPN provider documentation for instructions on configuring this exemption.

For example, if the local in-car network is 192.168.0.0/24, implement a rule to exempt traffic destined for this network and port 5353. For details, see https://netmotionsoftware.zendesk.com/hc/en-us/articles/4402637148051-Axon-Fleet-Dashboard-Policy.

Video upload

Video data files may be quite large. If a VPN is enabled on the in-vehicle router, add an exemption for the hub domain name axoncar.local or static IP to prevent offload traffic from being steered through a remote network.

MDC configuration

Axon Fleet 3 uses the vehicle's MDC to interface with the hub through Fleet Dashboard, which lets a user start/stop recordings, review and tag videos, view Automated License Plate Reader (ALPR) hits, and modify user preferences.

MDC system requirements

Axon Fleet Dashboard has the following minimum specifications for PC:

- **Operating system** – Windows 10 or later
- **Processor** – Intel Core i5-11th Gen or newer
- **Memory** – 8 GB RAM or more
- **Storage** – 10 GB of free space
- **Display** – 1024x768 or higher
- **Network** – 1 Gbps ethernet port or 1 Gbps USB3 ethernet adapter

While hardware with lower specs may still function, meeting these requirements will ensure the best possible experience with Axon Fleet Dashboard.

Multicast DNS

Fleet Dashboard uses Multicast DNS (mDNS) to discover the Fleet Hub.

If the MDC uses Windows 10, it supports Multicast DNS by default and no action is needed.

Firewall settings

Firewall considerations:

- Only Dashboard's inbound sign-in flow requires momentarily inboard traffic.
- Fleet Hub and Dashboard originate all traffic (except noted above) for outbound communication; whenever a port is referenced below, it is always initiated by outbound traffic.

Fleet Dashboard must be able to reach the Fleet Hub via **axoncar.local** on the following ports:

- 8000 (TCP): Used by Dashboard to authenticate against Axon Service; inbound traffic only, temporary port usage
- 8090 (TCP): Used for displaying the Axon Dashboard content, LiveView (using wss:// over 8090), and downloading Dashboard application updates
- 8100 (TCP): Used for playing videos
- 5353 (UDP): Used by Dashboard to discover the hub via Multicast DNS

- 53 (UDP): Used by DNS for fallback, Dashboard to Hub discovery, and router local domain configuration

Additionally, Fleet Dashboard must be able to access the following internet addresses:

- *.evidence.com (TCP 443) for signing into Axon Service
- Port 80 (outbound) for reachability checks to Axon Service
- fleetevidenceping.com (TCP 443) for Wi-Fi Direct Offload
- Any SSO provider domains you use
- If you have implemented network-based controls to manage internet access, you might find that your user, client, or device access won't connect with Axon Cloud Services unless specific network configurations are made; for help with this, see Managing Network Allowed Lists with Axon Cloud Services on my.Axon.

Proxy settings

Create a local proxy bypass rule to ensure **axoncar.local** traffic is not directed to the proxy and allow the MDC to communicate directly with the Fleet Hub on the in-vehicle LAN.

If using a traditional proxy, it should allow traffic to all internet addresses listed in Firewall settings. LINK

Adding **axoncar.local** to an allowed list should not be necessary.

Dashboard notifications

Dashboard displays notifications for ALPR hits. The default Windows setting for how long notifications are displayed is five seconds. Axon recommends making the display time longer so officers have more time to respond. This setting is found in the **Ease of Access** section. For more details on this setting, see Dashboard ALPR settings at My.Axon or the Axon Dashboard User Guide on the Fleet 3 product page.

Cradlepoint router configuration

Register and configure each Cradlepoint router from NetCloud Manager (NCM). Make changes in the NCM interface, not the local device UI. Use Groups to configure routers with a common configuration.

See Cradlepoint configuration on my.Axon for additional information on configuring a Cradlepoint router for Axon Fleet 3.

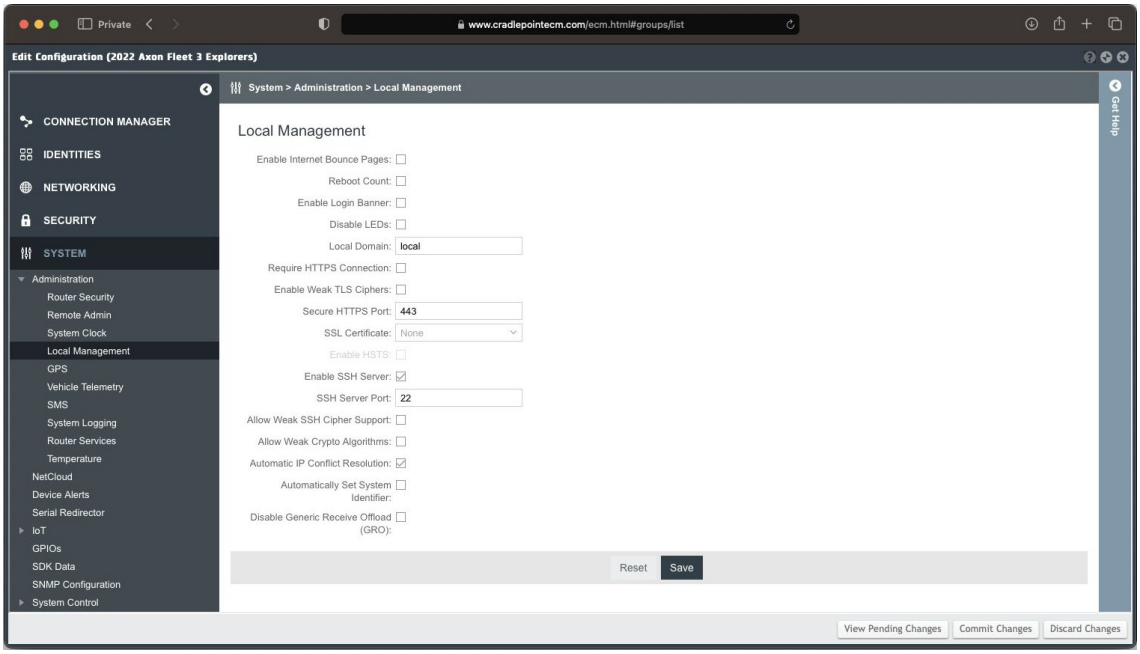
For more information about Cradlepoint devices or NetCloud Manager, see https://customer.cradlepoint.com/s/article/Getting-Started-with-NetCloud-Manager and https://docs.cradlepoint.com/r/IBR900-Getting-Started.

Configuration for Wi-Fi-connected dashboard

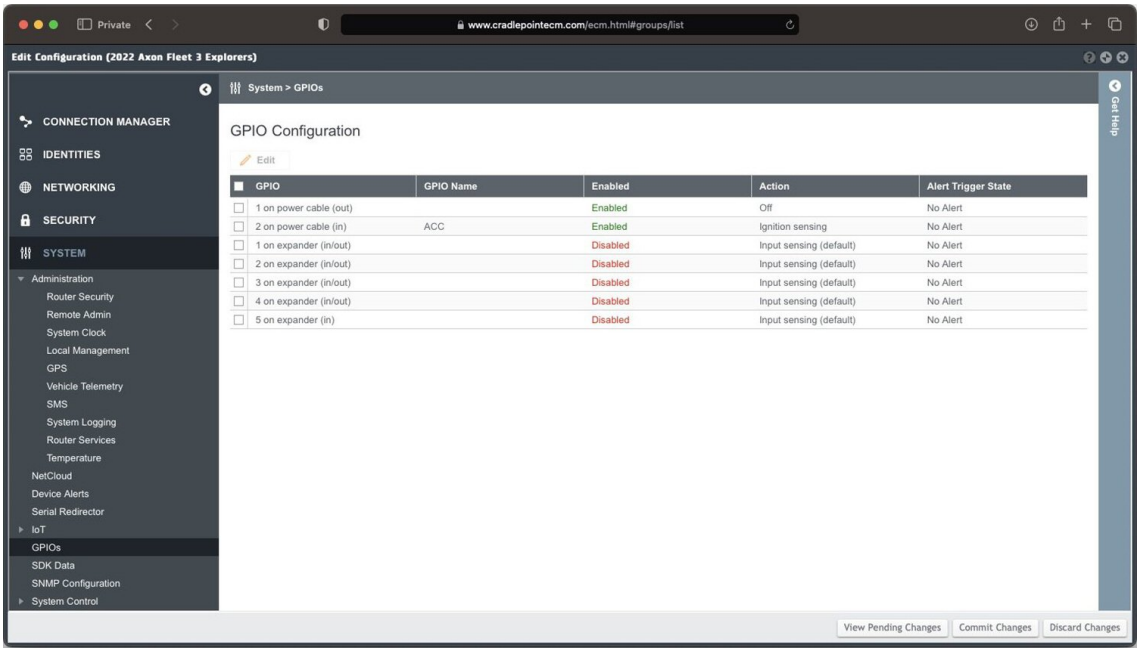
This instruction is for using the Cradlepoint user interface. This UI is not controlled by Axon and may have changed since this process was documented here. If you have questions about this process, contact Cradlepoint directly.

1. Sign in at https://www.cradlepointecm.com.
2. Select the first blue-colored **Connect** button under Netcloud (not the 2nd one under Cascade).
3. If **Switch to Classic UI** displays at top of page, select it. If **Try the New UI** displays, proceed to next step.
4. Prior to making config changes select **Groups** in the left-nav.
    a. Select **Add** and create a new group named **<Agency Name> - Fleet 3 Wireless Dashboard**.
    b. Locate the group the router(s) is/are currently in.
    c. Select the check box next to the group.
    d. In the **Configuration** dropdown, select **Export** and save the config file with a descriptive filename for use later, such as: *IBR900-<agency-name>-default-config-<date/time>.json*.
    e. In the **Configuration** dropdown, select **Copy To** and copy the config to the new group created above.

5. Match the following settings and then **Save**:

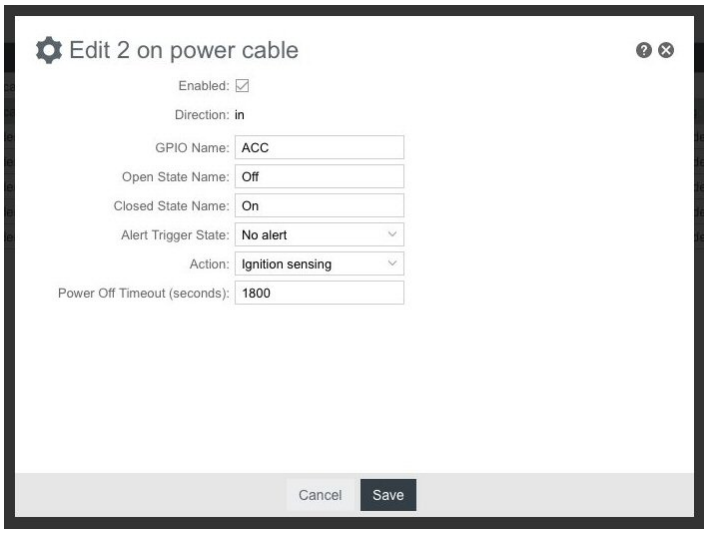


6. In the left-nav, select **System** > **GPIOs**.

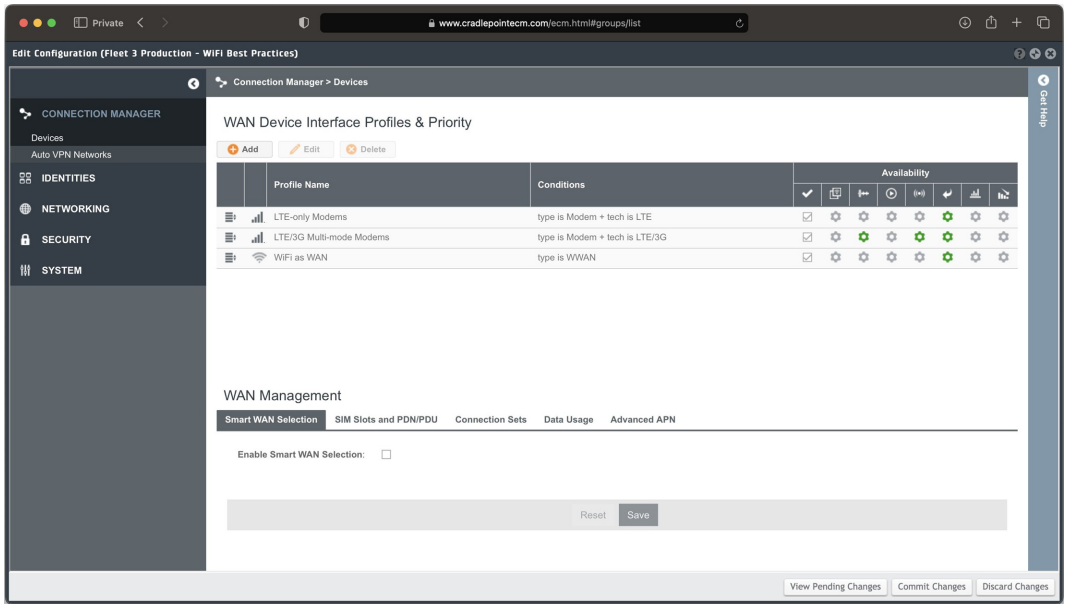


   a. Select the check box for GPIO #2.
   b. Select **Edit**.

c. Select the **Enabled** check box, set the various fields as shown below, and then **Save**.

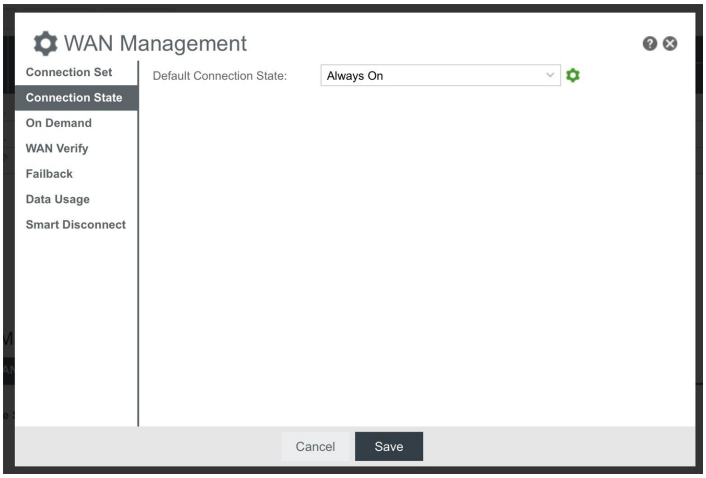


7. In the left-nav, select **Connection Manager** > **Devices**.
8. On the **WAN Device Interface Profiles & Priority** page, keep the entries shown in the image below, but delete other entries if the following conditions do not apply, then **Save**:
   a. 5G/LTE Multi-mode Modems – Keep if you use a 5G-capable Cradlepoint router+modem+SIM combo
   b. Ethernet – Keep if you connect Cradlepoints to WAN via ethernet (unlikely)
   c. 3G-only modems – Keep if you only uses 3G (unlikely)

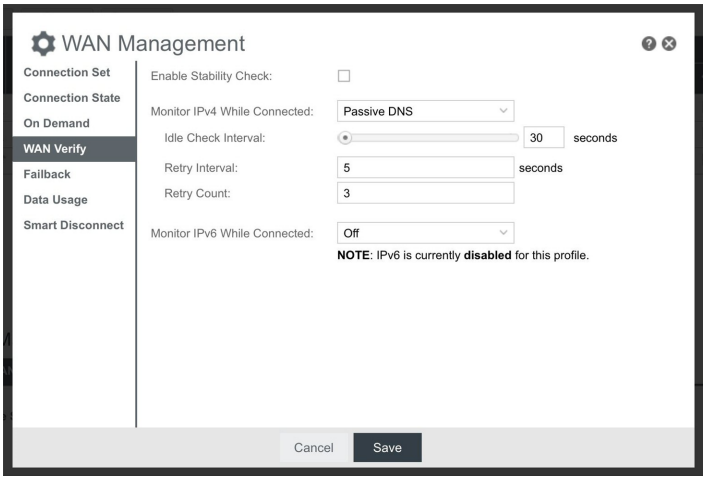


9. For **LTE/3G Multi-mode Modems**, select the second gear from left to open **WAN Management**.

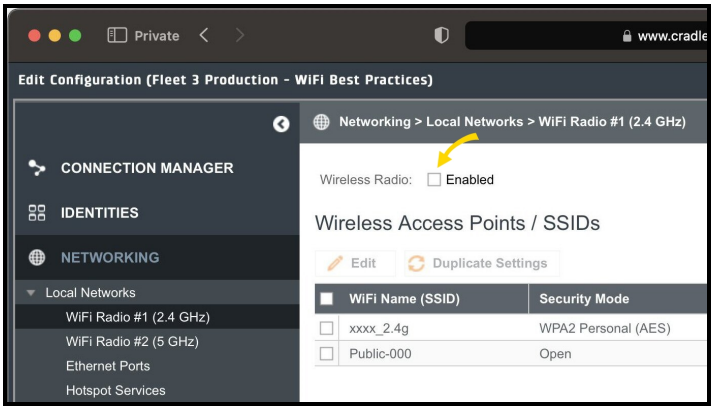
10. Set **Default Connection State** to **Always On** and then **Save**.



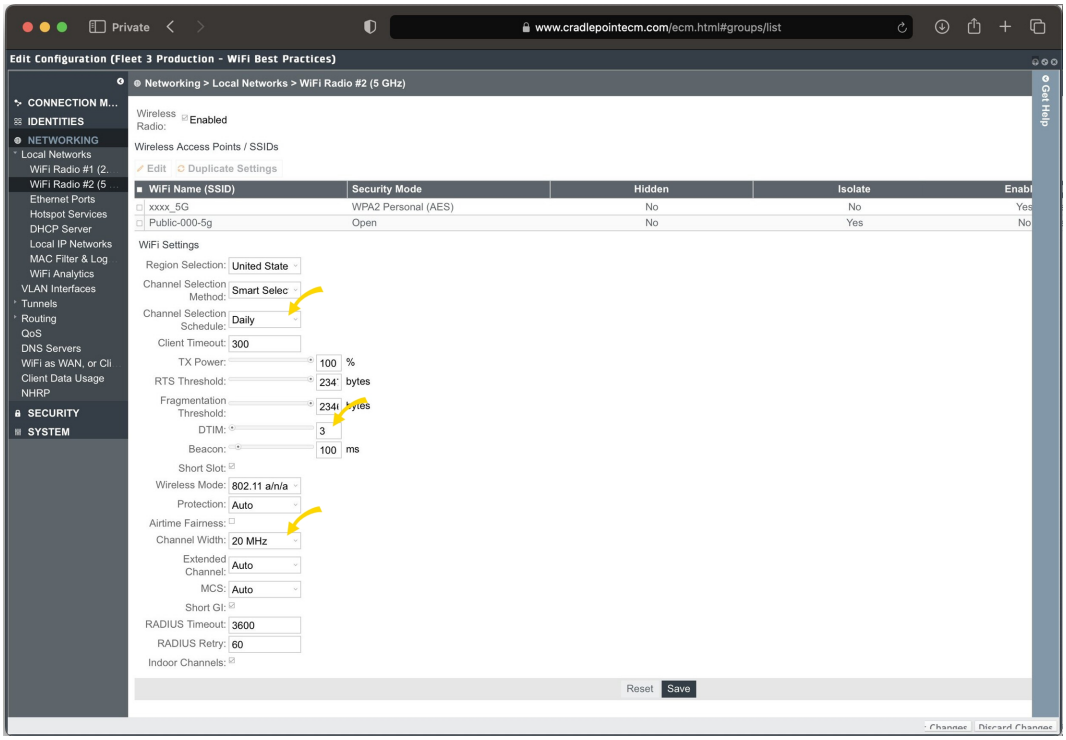
11. Select **WAN Verify** and set the various fields as shown below and then **Save**:



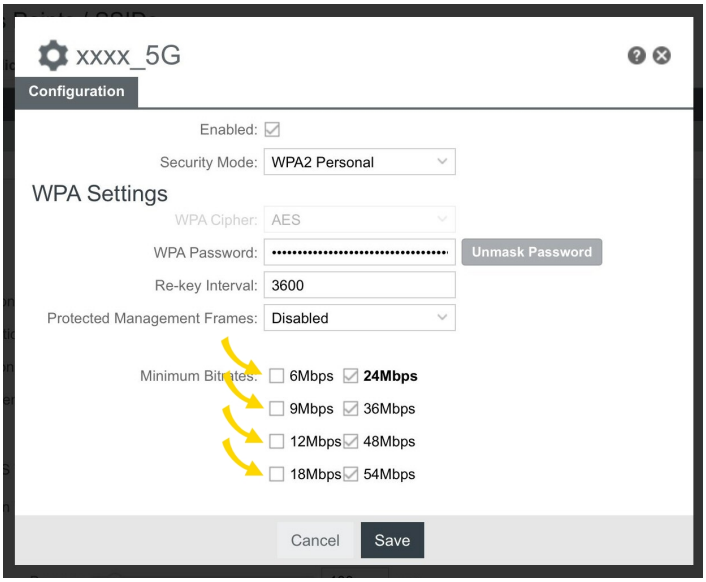
12. In the left-nav, select **Networking** > **Local Networks** > **Wi-Fi Radio #1 (2.4 GHz)** and clear the check box at the top. Select **Yes** to ignore the inaccurate warning about "disable all wireless wireless access to the router“ and then **Save**.



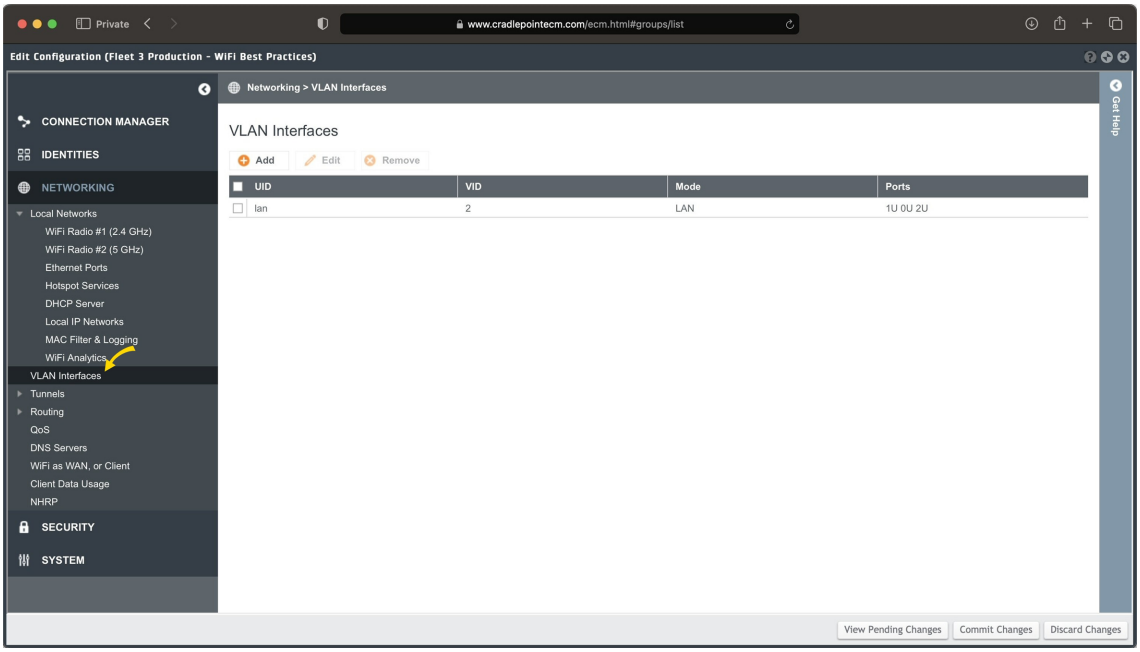
13. In the left-nav, select **Wi-Fi Radio #2 (5 GHz)**.
    a. Set **Channel Selection** to **Daily**.
    b. Set **DTIM** to **3**.
    c. Set **Channel width** to **20 MHz** and then **Save**.



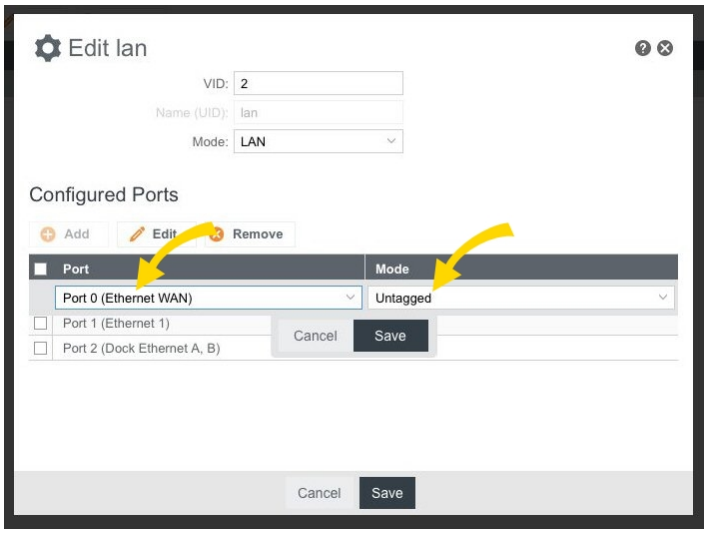
14. Select the check box next to the non-public 5G Wi-Fi SSID (such as **xxxx-5g**), then **Edit** immediately above it.
15. Disable bitrates less than 24 Mbps and then **Save**:



16. In the left-nav, select **Networking** > **VLAN Interfaces**.



17. To set both ethernet ports to LAN:
    a. Delete **wan**.
    b. Select the check box next to **lan** and select **Edit** immediately above it.
    c. Select **Add** and add **Port 0** as **Untagged** and then **Save**.



18. Select **Commit Changes** (see image in step 17).
19. Add each vehicle to the newly created group.

20. On each vehicle:
    a. In the left-nav, select **Networking** > **Local Networks** > **Wi-Fi Radio #2 (5 GHz)**.
    b. Select the check box next to the non-public 5G Wi-Fi SSID (such as **xxxx-5g**), then **Edit** immediately above it.
    c. Set **Wi-Fi Name (SSID)** to vehicle number or identifier, such as **8554-5g** or **Axon12-5g** and then **Save**.
21. Select **Commit Changes** to finish.