HC0100 (V4M) SENSOR · TECHNICAL COMPATIBILITY BRIEF

Multi-Band WiFi Compatibility

Key takeaway

The HC0100 discovers devices at the IP layer, so the WiFi band a device uses is immaterial to detection. Split-SSID homes therefore work in the vast majority of cases. Detection only breaks where the network introduces true isolation — VLAN segmentation, guest networks, or client/AP isolation — not from band separation itself.

WHAT'S INSIDE

01 Introduction

The Halo Connect HC0100 (V4M) sensor is a 2.4 GHz-only WiFi device. Ubiety recommends using it with residential WiFi setups consisting of a single SSID spanning both the 2.4 GHz and 5 GHz bands, where the router handles band steering. This is the configuration the HC0100 is designed, tested, and validated on.

While uncommon, some homeowners configure their routers to broadcast separate SSIDs for the 2.4 GHz and 5 GHz bands. This is not a configuration Ubiety advertises, validates, or actively maintains software support for — yet it does not always cause operational disruption. This brief explains why, and identifies the specific configurations that can cause unexpected behaviour.

02 How the HC0100 detects on-network devices

The HC0100's discovery engine operates at the IP / networking layer (Layer 3), rather than the physical layer (Layer 1) or data-link layer (Layer 2). The WiFi band the sensor is connected to is therefore immaterial to device discovery. Its discovery mechanisms include:

- ARP broadcast sweep
- Passive packet sniffing
- mDNS service discovery
- DHCP snooping
- Reverse DNS / NetBIOS queries

The on-network presence scan functions correctly as long as the phone and the sensor meet the following conditions:

1. They share the same subnet.
2. If on separate subnets, routing between them is permitted with no blocking ACL or firewall rules.
3. Client and AP isolation is disabled.
4. The phone is not on an isolated guest network.
5. The phone and sensor are not on separate VLANs (VLAN separation is the most common mechanism that violates conditions 1 and 2).

In practice, for a typical consumer residential deployment, these conditions are met by default. The sensor and phone end up on the same broadcast domain whether the router uses a single combined SSID or separate SSIDs per band.

03 Network configuration requirements

The critical factor is not which SSID or band a device connects to, but whether both devices share the same Layer 2 broadcast domain and Layer 3 subnet.

On virtually all consumer routers — including ISP-provided equipment, Eero, Orbi, TP-Link Deco, Netgear, and ASUS — splitting the SSID by band is a wireless-layer-only change (Layers 1–2). Both SSIDs bridge to the same LAN, the same DHCP server issues addresses from the same pool, and all devices land on the same subnet. A phone on `homewifi_5g` and an HC0100 on `homewifi_24g` remain fully visible to each other.

Scenario	Same subnet?	HC0100 detects phone?	Why
Single combined SSID (band steering)	**Yes**	**Yes**	The designed, tested and validated configuration.

Scenario	Same subnet?	HC0100 detects phone?	Why
Split SSIDs, same router, no VLANs	**Yes**	**Yes**	Both SSIDs bridge to the same LAN, DHCP pool and subnet.
Split SSIDs, VLAN-tagged per band	**No**	**No**	Layer 2 isolation at the VLAN boundary; ARP and mDNS do not cross.
Guest network with client isolation	**No**	**No**	Separate subnet with client isolation enforced by the router.
Enterprise managed APs (UniFi, Meraki), VLAN-per-SSID	**No**	**No**	Explicit VLAN-per-SSID config creates isolated broadcast domains.

While split-SSID deployments function correctly in the supported scenarios above, the HC0100 is designed and validated exclusively on single-SSID networks with band steering. Split-SSID compatibility is incidental to the Layer 3 discovery architecture and is not a tested or supported configuration.

04 Configurations that break detection

The following will prevent the HC0100 from discovering devices across bands:

1. VLAN-segmented SSIDs. If the router or access point tags each SSID to a different VLAN, each band becomes its own isolated broadcast domain. ARP sweeps and mDNS discovery will not cross VLAN boundaries.
2. Guest network isolation. Most routers implement guest SSIDs with client isolation and a separate subnet. If a resident’s phone is on the guest network, the sensor cannot see it unless the router allows client isolation to be disabled — not universally available.
3. AP / client isolation. A setting on some routers that prevents wireless clients from communicating even on the same SSID and subnet, blocking the ARP and passive-sniffing mechanisms the HC0100 relies on. Common on routers offering a dedicated `IoT network`.
4. Separate DHCP scopes without VLAN tagging. If an administrator manually configures different subnets per SSID (e.g. `192.168.1.x` for 2.4 GHz and `192.168.2.x` for 5 GHz) without VLAN tagging, the bands sit on different broadcast domains and the sensor will not discover devices across them.
5. Firewall / ACL rules blocking inter-subnet traffic. If the phone and sensor are on separate but routable subnets, rules blocking traffic between them prevent IP-based discovery even where routing would otherwise permit it.

05 What to verify in split-SSID deployments

For on-network detection to work correctly in a split-SSID household:

1. Confirm both SSIDs share the same subnet. In the router admin interface, verify the 2.4 GHz and 5 GHz SSIDs are assigned to the same LAN/bridge interface with the same DHCP pool.
   a. If this option isn't exposed in the router interface, they are most likely already on the same subnet.
2. Ensure no per-SSID VLAN tagging. Typically only a concern on enterprise or managed network hardware.
3. Ensure client / AP isolation is disabled. Sometimes enabled by default on certain routers, and will silently break local device discovery.
4. Confirm resident phones are not on the guest network. Guest SSIDs are almost always isolated and will break presence detection.

While split SSIDs on consumer hardware work in most cases, the HC0100 is validated on single-SSID networks. If issues persist, consolidating to a single SSID with band steering is the recommended resolution and provides the most predictable behaviour.

06 Exception: visitor QR-code assignment

The visitor onboarding flow has different network requirements for the primary user and the visitor.

Primary user

The primary user's phone must be on the same SSID as the HC0100 sensor when generating the QR code. The app enforces this check and displays an error rather than the QR code if the phone is on a different SSID.

Visitor

The visitor's phone does not need to be on the same SSID — it only needs to reach the primary user's phone IP over the network. The QR code encodes the primary user's phone local IP and port (e.g. `ws://192.168.0.102:1028`), and the visitor's browser opens a WebSocket directly to that address. As long as routing exists and no firewall blocks the connection, the flow succeeds — confirmed working across different subnets where no ACL or firewall blocks exist.

The visitor's IP is then captured from the incoming connection and matched against device records populated by the HC0100's on-network scan; on a match, the visitor is registered to the profile. Once registered, both the visitor and primary user can connect to any band or SSID on the same network, and ongoing presence detection reverts to the standard IP-based mechanisms.

07 Conclusion

The HC0100 is designed and validated on single-SSID networks where the router manages band steering. Its 2.4 GHz-only limitation does not restrict its ability to detect devices on a 5 GHz band in split-SSID deployments, because on-network discovery operates at the IP layer and is indifferent to wireless frequency as long as devices share a common broadcast

domain and subnet. Split-SSID compatibility is a consequence of this architecture, not a guaranteed configuration.

For the overwhelming majority of residential deployments, split-SSID configurations are safe and require no special accommodation. The configurations that cause failures are those introducing actual network isolation — VLAN segmentation, guest-network isolation, or client/AP isolation — rather than simple band separation.

Diagnostic focus

When issues are reported in split-SSID environments, focus on network isolation mechanisms rather than band separation. In enterprise or managed deployments, VLAN-per-SSID is the most likely culprit; in consumer deployments, guest-network enrollment and client isolation are the most common causes.