

Guest WiFi diagnostic worksheet

Use one sheet per incident. Record the visible symptom first, then work through the checks in order. Page 1 is for venue staff. Page 2 is for the network owner or installer.

Venue or internal incident reference

Date, local time and timezone

Guest network name (SSID)

Device type and operating-system version

1 Which step fails?

- ☐ The guest network does not appear in WiFi settings
- ☐ The device cannot join the guest network
- ☐ The device joins, but the login page never appears
- ☐ The login page opens but is blank, incomplete or stuck
- ☐ The form submits, but the device still has no internet
- ☐ Internet works, then stops or asks for login again

2 Safe staff checks

- ☐ Confirm the guest is choosing the venue's genuine guest SSID, not a staff, payment or lookalike network
- ☐ Ask whether another guest device works on that same network. Record whether this affects one device, several devices, or everyone
- ☐ Open the device's WiFi settings and look for its sign-in prompt. On iPhone or iPad, the network details may offer **Join Network**
- ☐ For a device the owner agrees to use for testing, disconnect and reconnect. A remembered, already-authorized session may not show a fresh portal
- ☐ Test with a second device if available. Record its operating system and which step succeeds or fails
- ☐ Confirm the result using a harmless web page and the device's connection status; cellular fallback can make a WiFi test look successful

3 Record and escalate

Exact visible error and which devices are affected

What changed recently, if known, and the last time WiFi worked

Stop for security warnings. Do not bypass certificate or unsafe-site warnings, ask for account passwords, disable privacy features by default, or reset the router during service. Do not change the staff or payment network to fix guest access.

General troubleshooting aid, not a guarantee of compatibility. Public vendor guidance checked 2 October 2026. Hardware-specific changes belong to the authorized network owner.

Find the failed handoff

Change one thing at a time and keep a rollback plan. Controller menus and authorization methods vary by product and version. Verify the current vendor instructions for this installation.

Controller vendor and model	Controller and access-point firmware versions
Last known working configuration or change ticket	Authorized change window and owner

4 Check each handoff

- ☐ **Network association:** confirm the intended guest SSID is enabled and the test device is associated with the expected access point and network
- ☐ **Addressing and DNS:** check that the device has the expected guest-subnet address, gateway and working DNS. Keep guest-to-staff and guest-to-payment separation intact
- ☐ **Portal binding:** verify the portal is attached to the correct guest SSID or network, and that the intended authentication mode is selected
- ☐ **Portal reachability:** check the exact configured destination, a valid HTTPS certificate, and the minimum documented pre-authentication domains needed to render the page
- ☐ **Redirect context:** confirm required controller-generated parameters arrive intact. Do not invent, expose or log reusable credentials in the portal URL
- ☐ **Authorization:** after submission, inspect whether the controller reports this test client as authorized. A successful form alone is not proof of internet authorization
- ☐ **Post-authorization access:** if authorized but offline, check the relevant guest-network route, DNS, firewall and session limits rather than opening unrestricted access
- ☐ **Retest:** test the guest experience on a second operating system and confirm both internet access and the expected consent record. Do not label a previously authorized session as a fresh login test

5 Document the result

First handoff that failed, evidence, change made, and rollback reference

Retest date and outcome	Next action and responsible person

Share a redacted support handoff. Include symptom, timestamps/timezone, controller and device versions, failed stage, and a cropped error screenshot if useful. Remove guest emails, raw MAC addresses, tokens, passwords, cookies and sensitive internal network details before sharing externally.

Source guidance
Apple: Captive WiFi networks on iPhone and iPad
Ubiquiti: External Hotspot API and authorization workflow
TP-Link Omada: Portal authentication and pre-authentication access
VoqadoWiFi: Guided setup · Hardware compatibility checker