WASSUP

Wireless Assessment Security Standards Utility Program

End User Step-by-Step Usage Guide

Defensive Cyber LLC
Field Wireless Security Analyzer

FOR AUTHORIZED USE ONLY — This guide accompanies a passive wireless reconnaissance tool intended for ISSM/ISSO wireless security assessments conducted under current, documented authorization only.

Document version: 1.1 — adds battery indicator, tap-to-open power detail & automatic low-battery shutdown
Date: September 4, 2026
Covers: splash/AUP screen with device time zone confirmation, live dashboard, sortable Access Points & Bluetooth tables, Watchlist high-priority alerting, Focused Scan, Bluetooth discovery with manufacturer-data vendor detection, passive device/OS fingerprinting, Saved Assessments, Internet Uplink (network details, guest network sign-in, saved network management) & email, the dynamic on-screen keyboard, safe shutdown/reboot, and reading this guide directly on the device, plus the battery indicator with tap-to-open power detail and automatic low-battery shutdown

Contents

1. Introduction

WASSUP (Wireless Assessment Security Standards Utility Program) is a handheld passive wireless reconnaissance device built for ISSM/ISSO wireless security assessments. It discovers WiFi access points and clients across 2.4GHz, 5GHz, and 6GHz, discovers nearby Bluetooth devices with vendor identification from two independent signals, can park on a specific network's channel to catch clients that don't transmit often, and can raise an immediate high-priority alert if a specific system on an imported watchlist is detected. Its onboard internet uplink can also sign in to guest networks with their own web-based portal pages. Findings can be exported as CSV/JSON data or as a branded assessment report with RMF/eMASS-aligned control fields, and specific access points can be flagged to include their attached hosts directly in that report.

This is Version 1 of the tool — the first release where every feature described in this guide is fully functional end to end. This guide walks through every screen in the order you'll actually encounter them: from power-on and the Acceptable Use Policy, through the live dashboard and each of its sections, to generating a report and shutting the device down safely.

This tool must only be used under current, documented authorization for the specific wireless environment being assessed. See the full Acceptable Use Policy text in Appendix A.

What the device looks like

WASSUP is built into a rugged, sealed field case with four antennas across the top feeding its multi-band radios. It is operated entirely from the touchscreen mounted in the lid, so there is nothing to plug in to use it in the field. The photos below show the actual unit.

Photo 1 — The WASSUP unit powered on. On boot it comes straight up to the splash screen with the Acceptable Use Policy, ready for the assessor to fill in and acknowledge before the live dashboard opens (see Section 2).

Photo 2 — The top of the unit, where the four antennas mount. They feed the two onboard WiFi adapters, which run in monitor mode so WASSUP can passively capture across the 2.4, 5, and 6 GHz bands at the same time.

The left side of the unit carries its ports and the main power switch:

Photo 3 — The left side of the unit. On the right, from top to bottom: the USB-A port, the HDMI port, and the power switch. The USB-C charging port is at the lower middle.

USB-A port (upper right). Use this port to copy reports and the user guide out to a USB drive, or to import an asset watchlist for the tool to scan against.

HDMI port (middle right). Connect an external monitor or a projector here to mirror the touchscreen onto a larger display.

Power switch (lower right). This switch must be ON for the device to boot. It is the master power cutoff, not the everyday off control — see the caution below and Section 13.

USB-C port (lower middle). This is the fast-charging port for the internal battery.

> **Do not turn the device off with the side power switch. Always shut down from the on-screen power icon first (see Section 13); only after it has fully powered down should you flip the side switch off. If you leave the switch on after an on-screen shutdown, the Raspberry Pi's cooling fan keeps running and will slowly drain the battery.**

2. Starting the Tool

Splash Screen, Acceptable Use Policy & Time Zone

Every time the tool starts — including after every reboot — it opens to this screen. You cannot reach the live dashboard without completing this screen first; it resets on every restart rather than being remembered.

Figure 1 — Initial splash screen: tool identity, purpose, and the start of the Acceptable Use Policy.

Step-by-step

1. Read the purpose statement and control tags (AC-18, CA-7, CA-8, RA-5, SC-40, SI-4).
2. Scroll the Acceptable Use Policy box all the way to the bottom. The acknowledgment checkbox stays disabled until you do. The full policy text is reproduced in Appendix A.
3. Fill in the three required fields: **Conducted By**, **Organization**, and **eMASS System Name**. All three carry through into every report you generate this session.

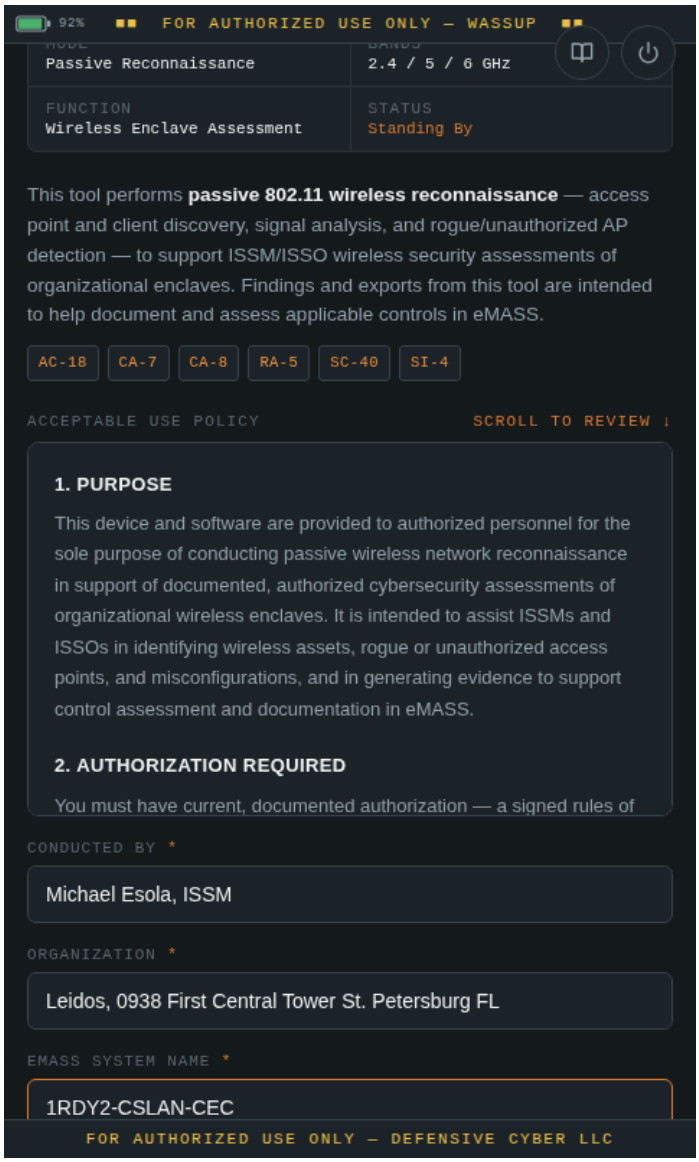


Figure 2 — All three required fields filled in.

4. Confirm the **Device Date, Time & Time Zone** shown is correct for wherever this assessment is actually taking place. This device travels between locations, so this isn't just a display — the dropdown genuinely reconfigures the Pi's own system clock if the current setting is wrong for where you are right now.

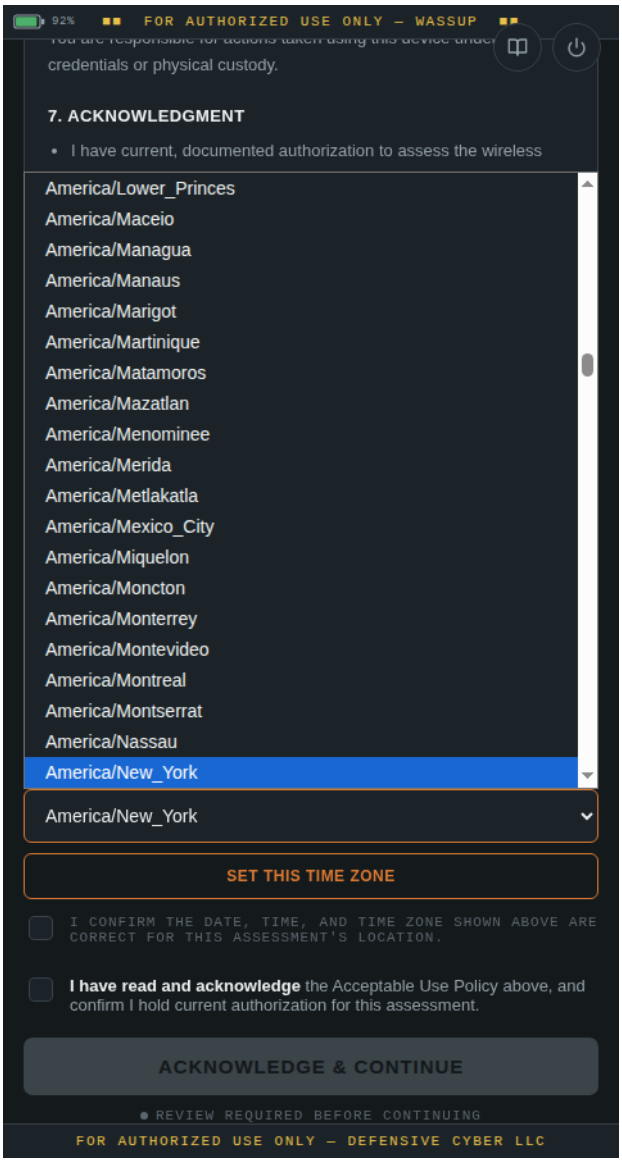


Figure 3 — The live date/time display, the time zone dropdown (pre-selected to whatever the system currently thinks it is), and the required confirmation checkbox.

If it's already correct, just check the confirmation box below it and move on — no need to touch the dropdown at all. If it's wrong for this assessment's actual location, pick the correct zone from the dropdown and tap **Set This Time Zone**.

> **Setting a new time zone restarts the kiosk display automatically after a few seconds, returning you to this same splash screen with the corrected time now showing. This is expected, not an error — a running display has to restart fresh to pick up a system-level time zone change; it can't be shown live without one. Every timestamp elsewhere in this tool, and the "Device Time Zone" field in every generated report, depends on this being set correctly.**

5. Check the acknowledgment box. The button turns solid orange and the status line confirms authorization once every required field above is complete, including the time zone confirmation.

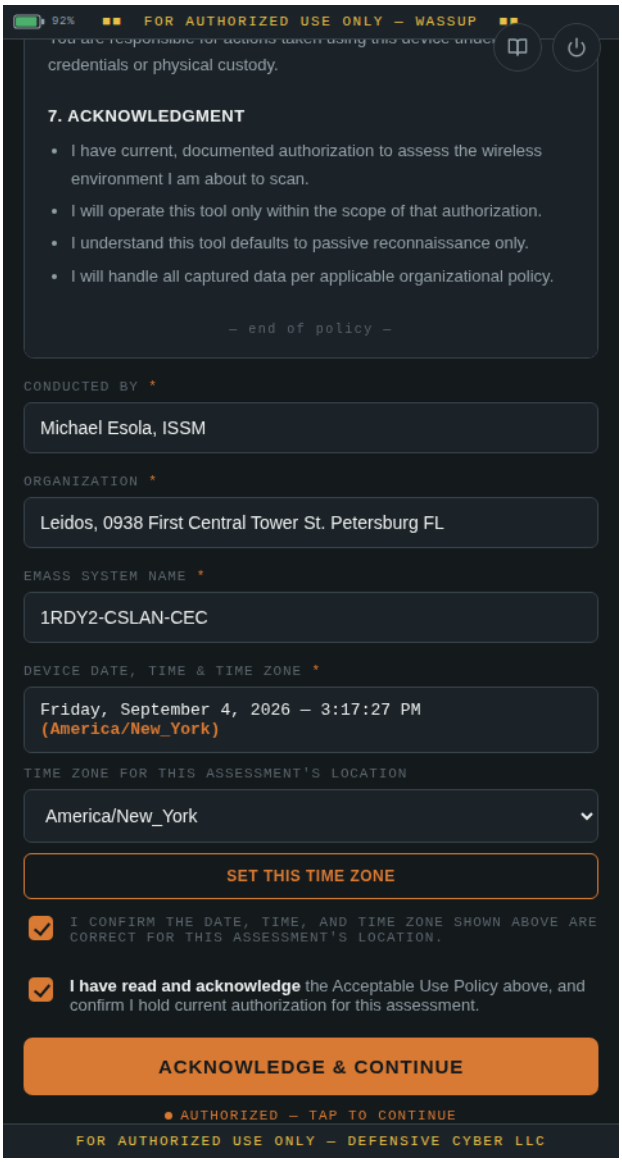


Figure 4 — Ready to continue: every required field complete, including the time zone confirmation, button enabled.

6. Tap **Acknowledge & Continue** to enter the live dashboard.

Power options from this screen

The power button (top-right corner icon) is available on this screen too, offering the same Reboot and Shut Down options covered fully in Section 13 — useful if you need to power off or restart before ever reaching the dashboard.

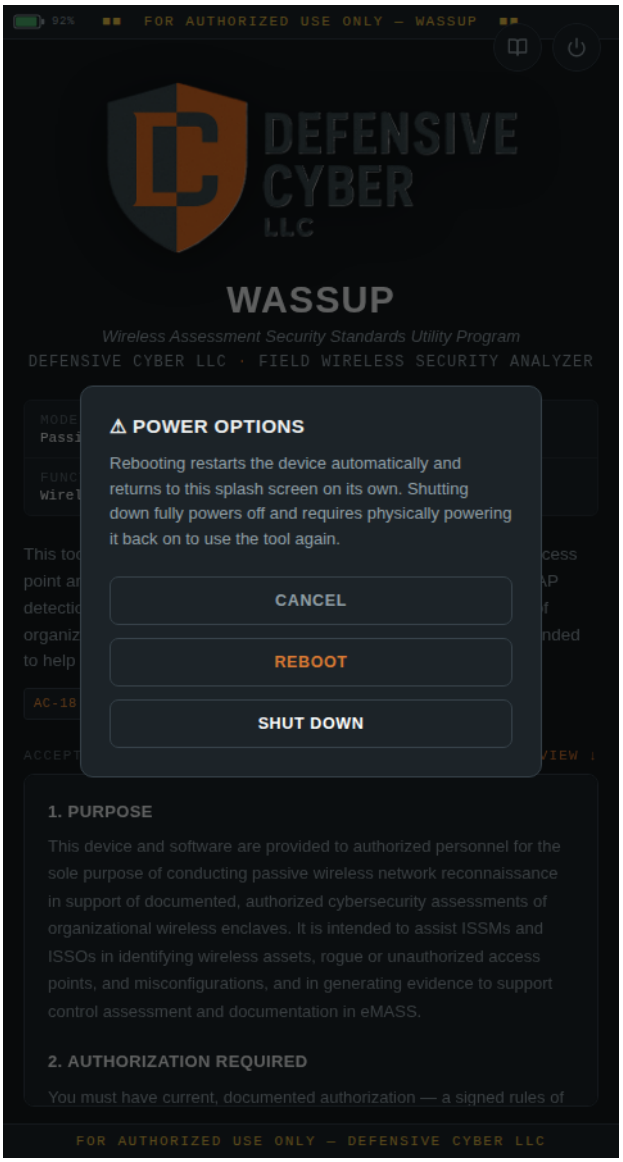


Figure 5 — Power Options, available from the splash screen.

3. The Main Dashboard

After acknowledging the AUP, you land here. Every section below the top status tiles is collapsible — tap any section header to expand or collapse it. This full view shows the layout end to end, including the Access Points checkboxes and Focused Scan controls covered in later sections.

The top tiles show which radios are active and their current channel, how many access points and clients have been found, and a live alert count. **Conducted By**, **Organization**, and **eMASS System Name** stay editable here in case anything needs correcting mid-session. The red alert box shows rogue-AP/evil-twin heuristic findings — a different, lower-severity tier than the Watchlist banner covered in Section 8.

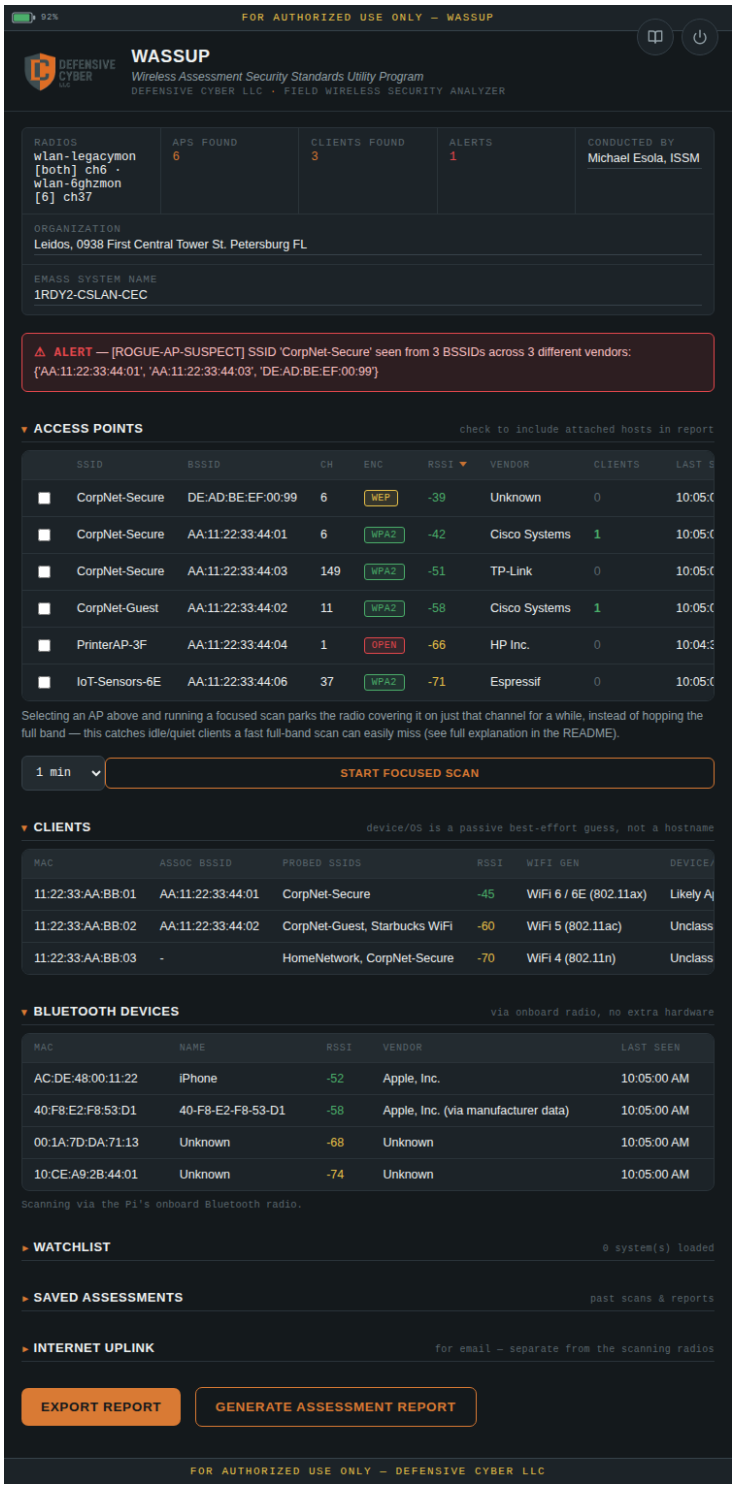


Figure 6 — The full dashboard, shown expanded for reference.

4. Access Points — Sorting & Viewing Connected Clients

The Access Points table lists every discovered network: a checkbox, SSID, BSSID, channel, encryption, RSSI, OUI-resolved vendor, and a **Clients** count. The Clients count shows in bold green when non-zero, dimmed when empty, so it's easy to spot at a glance which access points have devices worth drilling into. **Tap any row** (not the checkbox) to see which client devices are currently associated with that specific access point.

SSID, BSSID, Enc, RSSI, Vendor, and Clients column headers are all tappable to sort the table — a small triangle shows which column is active and which direction. Tapping the same header again reverses direction. Text columns (SSID, BSSID, Enc, Vendor) default to A-Z on a fresh tap; RSSI and Clients default to strongest/most first, since that's typically the more useful starting view for an assessment. Once you've picked a sort, it stays exactly as you left it — the table used to silently re-sort by signal strength on every refresh (every 1.5 seconds), which made rows jump around distractingly as RSSI naturally fluctuated. Now, rows only reorder when you deliberately choose a different sort.

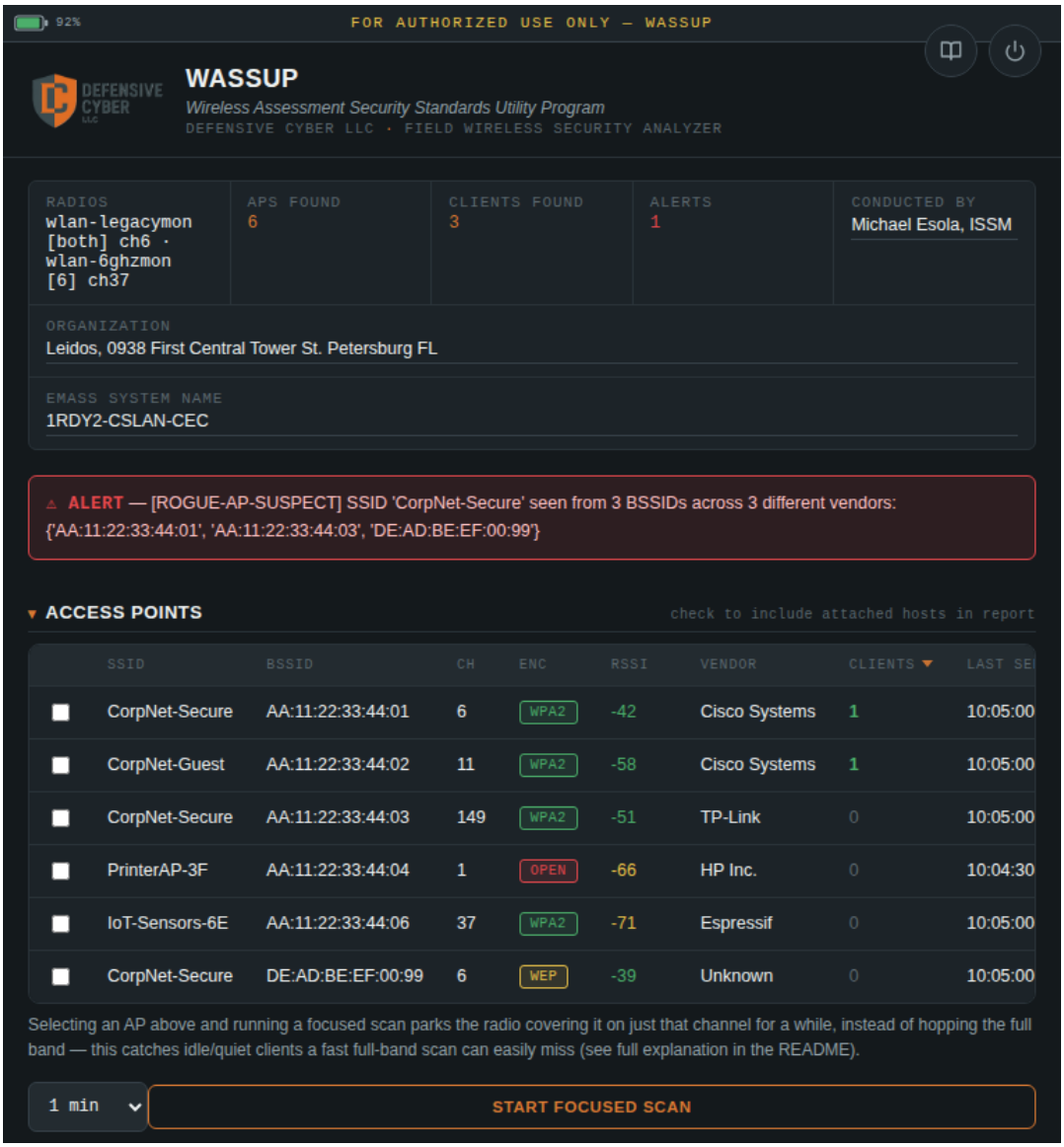


Figure 7 — Access Points sorted by Clients, most-connected first. The orange triangle next to "CLIENTS" shows the active sort column and direction.

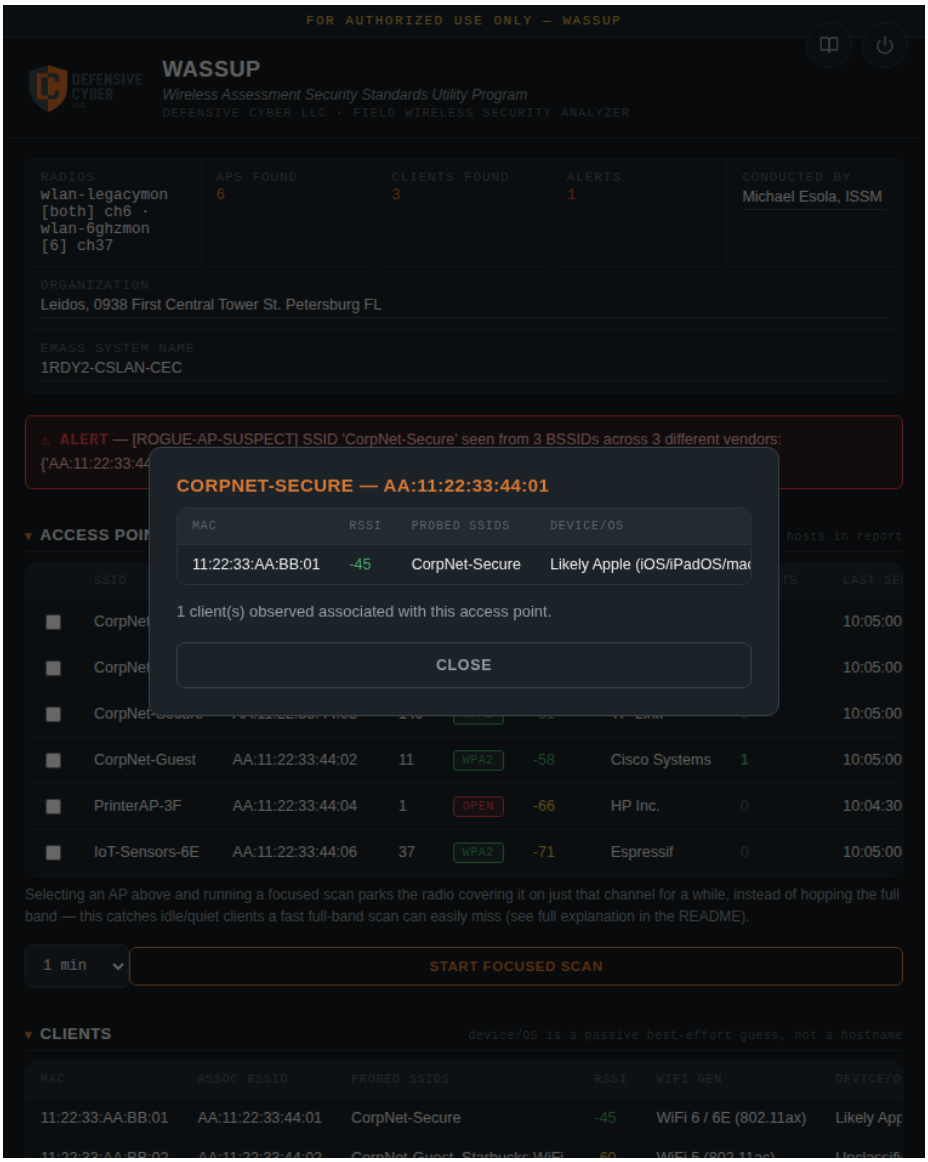


Figure 8 — Tapping an access point row shows its currently associated clients, including a device/OS guess for each one (see Section 5).

If no clients are shown, or the Clients count reads 0, that reflects passive observation only — a client only counts here while it's actively exchanging frames with that access point during the scan window.

The **checkbox** on each row has two uses, covered in their own sections: including that access point's attached hosts in a generated report (Section 12), and targeting it for a Focused Scan (Section 6).

5. Clients — Passive Device/OS Fingerprinting

The Clients table lists every client device observed, with two columns worth understanding clearly: **WiFi Gen** and **Device/OS Guess**.

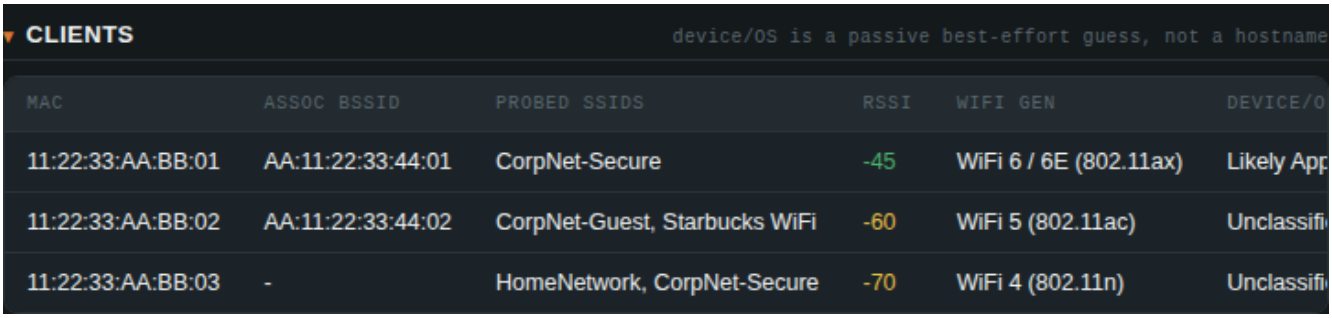


Figure 9 — The Clients table, showing WiFi generation and a device/OS guess for each client.

WiFi Gen (WiFi 4/5/6) is objectively determined from standard, mandatory capability fields every device broadcasts — no guessing involved.

Device/OS Guess is different, and the name is chosen deliberately: it is a best-effort passive inference, not a confirmed identification and never a hostname. A device's actual name (“John's iPhone”) only ever appears in traffic exchanged *after* joining a network, which is encrypted on any WPA2/WPA3 network by the time this tool's radios see it — reading it would require decrypting traffic on a network this tool holds the password for, a materially different and more invasive capability than passive reconnaissance, and outside what this tool's AUP authorizes without separate written authorization.

What passive monitoring genuinely can observe: every client broadcasts probe request frames in cleartext, even ones that will only ever join encrypted networks, since that happens before any security handshake. Those frames carry standard fields describing the client's WiFi capabilities, and sometimes a vendor-specific marker. Currently, only one such marker is used for an actual guess — Apple's own documented vendor identifier, seen on iOS/iPadOS/macOS devices. Anything else reports **Unclassified** rather than stacking weaker signals into a false-confident guess.

Treat Device/OS Guess as a lead worth investigating further, not a fact. It appears with this same wording and caveat in the generated assessment report (Section 12).

6. Focused Scan — Catching Idle/Quiet Clients

Normal scanning hops across every channel in the 2.4/5/6GHz range quickly, spending only a fraction of a second on each one. A client only shows up as associated with a specific access point once the tool captures an actual data frame from it — and a genuinely idle device (screen off, no background activity) can go a long stretch without transmitting anything at all. Put those two together, and an idle client has a real chance of being missed during a short scan.

Focused Scan fixes this: check the box next to one or more access points, choose a duration, and tap **Start Focused Scan**. Whichever radio covers the selected access point(s) parks on just those channel(s) with a much longer dwell time instead of hopping the full band — dramatically increasing the odds of catching an infrequently-transmitting client. Radios not involved in the selection keep scanning normally the whole time.

1. Check the box next to one or more access points in the table.
2. Tap the duration dropdown to choose how long to focus: 30 sec, 1 min, 2 min, or 5 min.

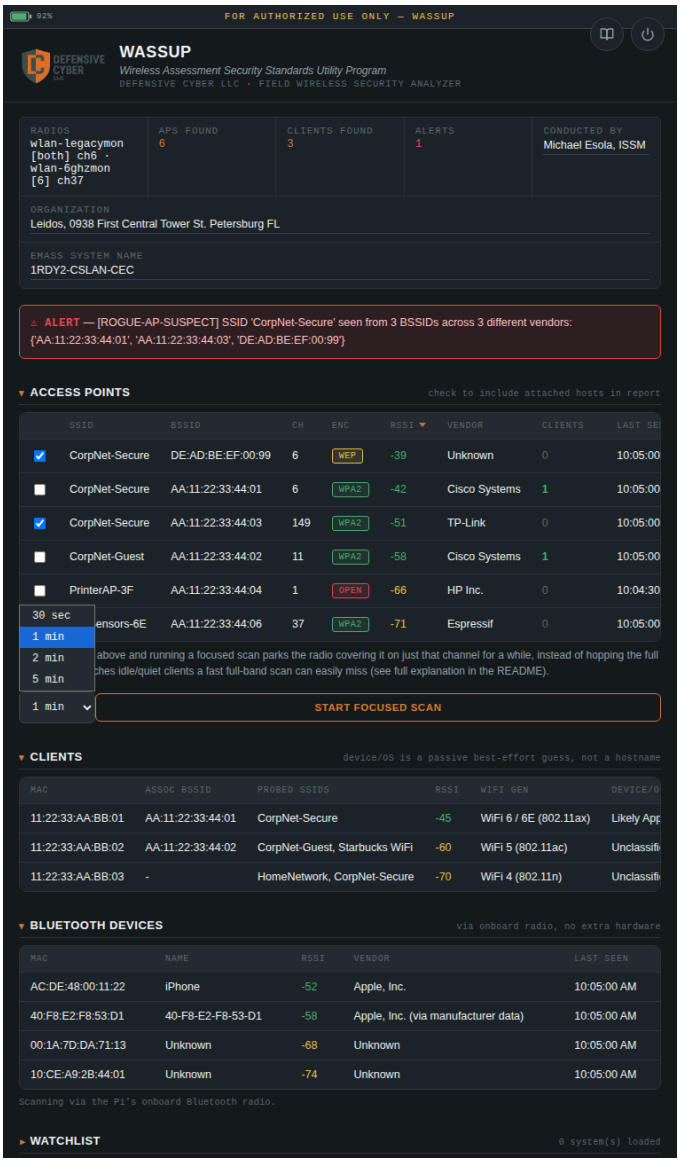


Figure 10 — Two access points selected, with the duration options (30 sec / 1 min / 2 min / 5 min) open.

3. Tap **Start Focused Scan**. A status bar replaces the controls, showing how many access points are targeted and time remaining, with a **Stop** button to cancel early. It reverts to normal scanning automatically once the duration elapses.

7. Bluetooth Devices

Uses the Raspberry Pi's own onboard Bluetooth radio — a completely separate physical layer from the two WiFi scanning radios, and no additional hardware required. Lists every Bluetooth device (BLE and Classic) discovered nearby. This is passive discovery only; the tool never pairs with or connects to anything it finds. **Tap the MAC column header** to sort the table alphabetically; tap again to reverse direction.

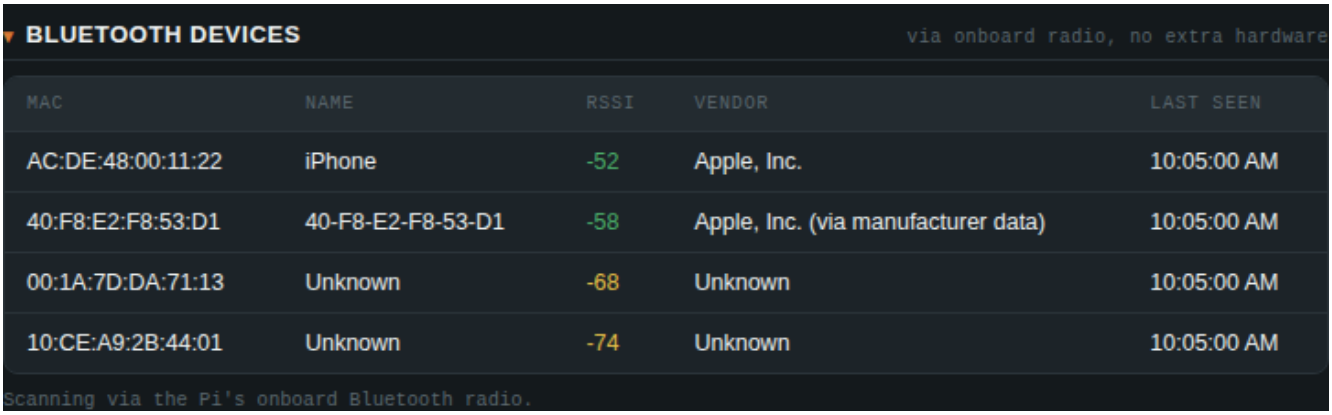


Figure 11 — Bluetooth Devices, sorted by MAC address. Two different vendor-identification methods are visible here side by side.

Two independent ways a vendor gets identified

Direct OUI match (e.g. "Apple, Inc.", "iPhone" above) — the device's Bluetooth address itself is genuinely registered to that manufacturer. This is the most common, straightforward case.

Manufacturer data match (shown as "...(via manufacturer data)") — a separate, independent identification path for devices using randomized Bluetooth addresses, a genuine, increasingly common privacy feature on modern devices that deliberately prevents any address-based lookup from working at all. Some devices additionally broadcast a Bluetooth SIG "Company Identifier" code in their own advertising data — a completely separate numbering system from the address itself. This tool currently recognizes Apple's code with high confidence; confirmed on real hardware that devices broadcasting it consistently show a randomized, address-unmatched MAC, proving the two mechanisms are genuinely independent.

"Unknown" for a device you can visually confirm is a real, recognizable product (a mouse, a headset, etc.) usually isn't a database gap — it's almost always that specific device using a randomized address with no manufacturer-data broadcast this tool currently recognizes. No OUI database, however large or current, can resolve an address that was never derived from the manufacturer's real registered identity in the first place.

8. The Watchlist — High-Priority Alerting

Import a CSV of specific systems — known-stolen assets, devices that shouldn't be present in a given enclave, or any other “flag if seen” list — from a USB drive. The tool cross-references every currently observed WiFi and Bluetooth MAC address against this list on every refresh cycle. Any match fires an immediate banner pinned at the very top of the page, above even the header.

CSV format (header row required): Computer Name, Asset Tag, WiFi MAC Address, Bluetooth MAC Address. Not every row needs every column.

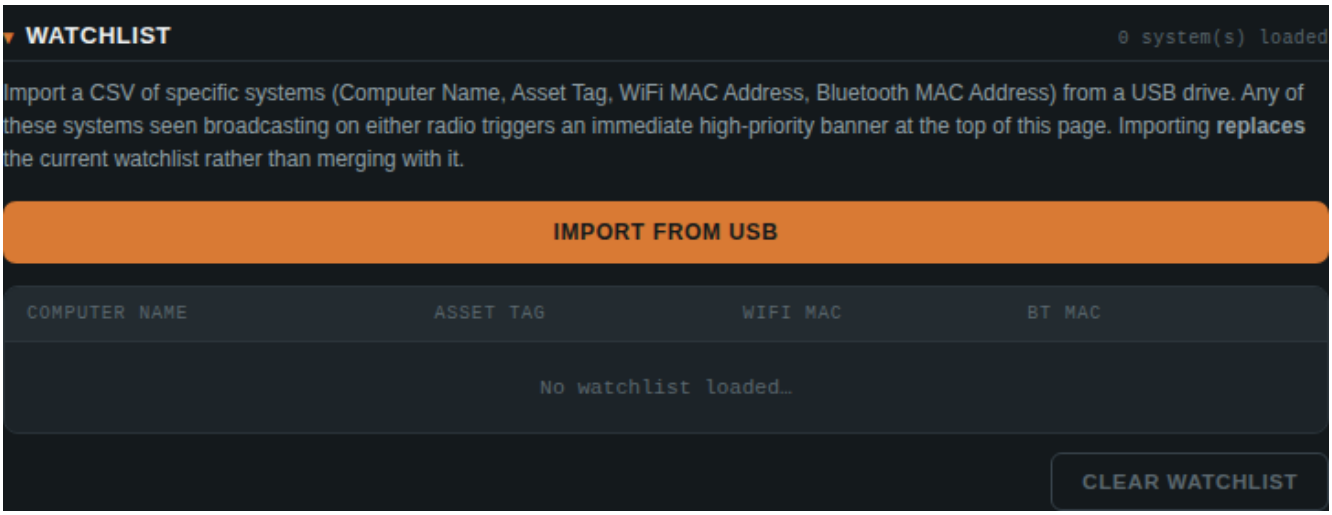


Figure 12 — The Watchlist section before anything is imported.

Importing a watchlist

1. Plug in a USB drive containing the CSV file, then tap **Import from USB** and select the drive.

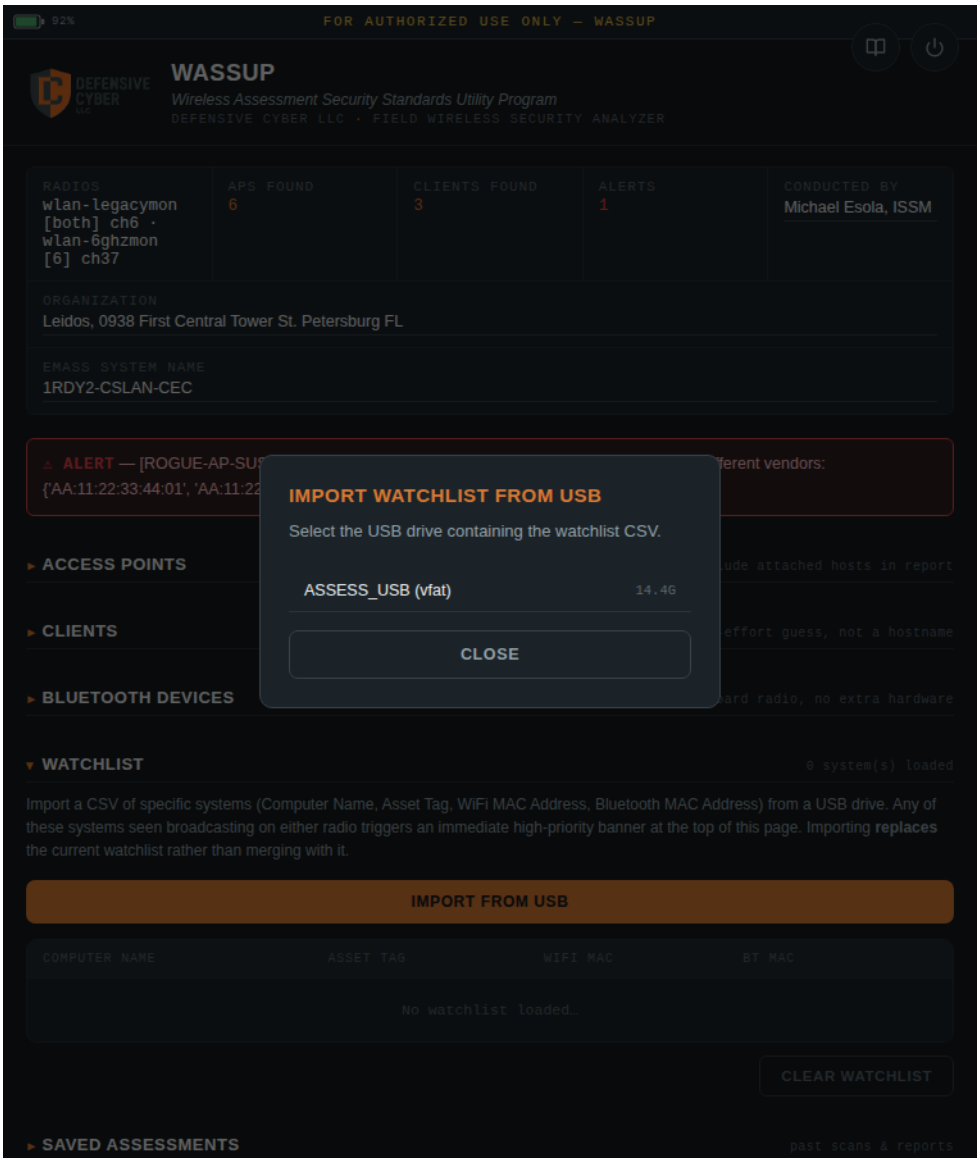


Figure 13 — Step 1: select the USB drive.

2. Select the specific CSV file from that drive.

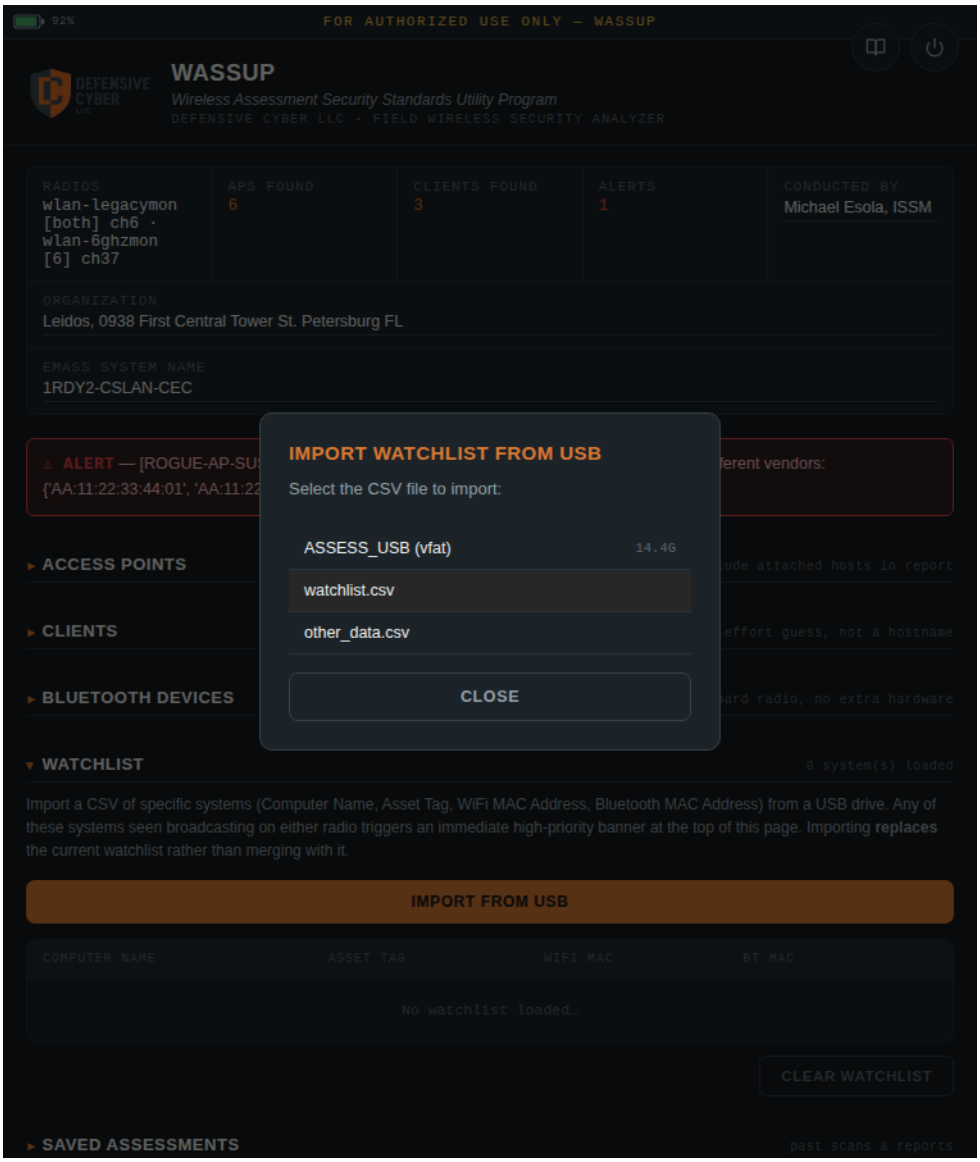


Figure 14 — Step 2: select the CSV file to import.

3. The import result confirms how many systems were loaded.

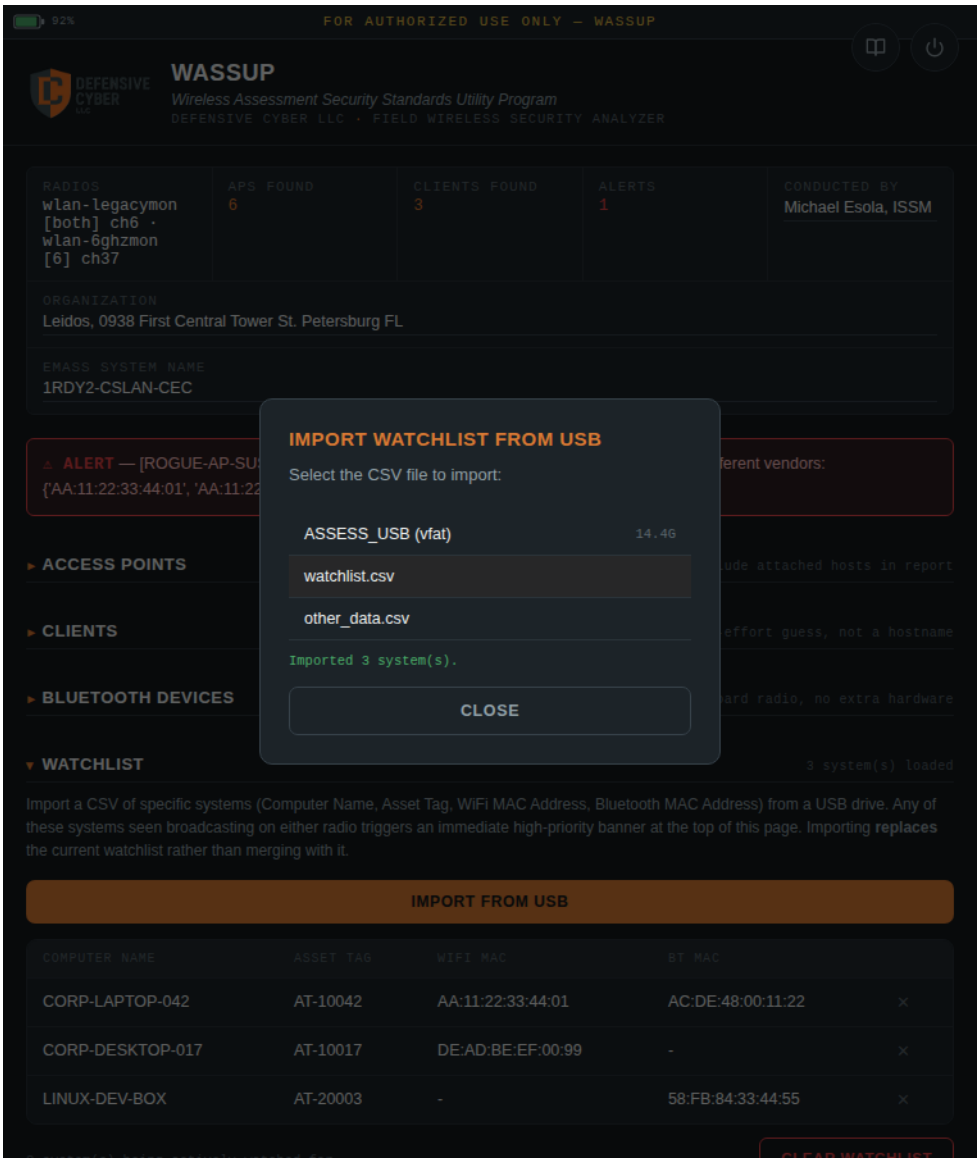


Figure 15 — Import confirmed.

Importing REPLACES the current watchlist — it does not merge with it. Re-import a combined CSV if you want to add to an existing list.

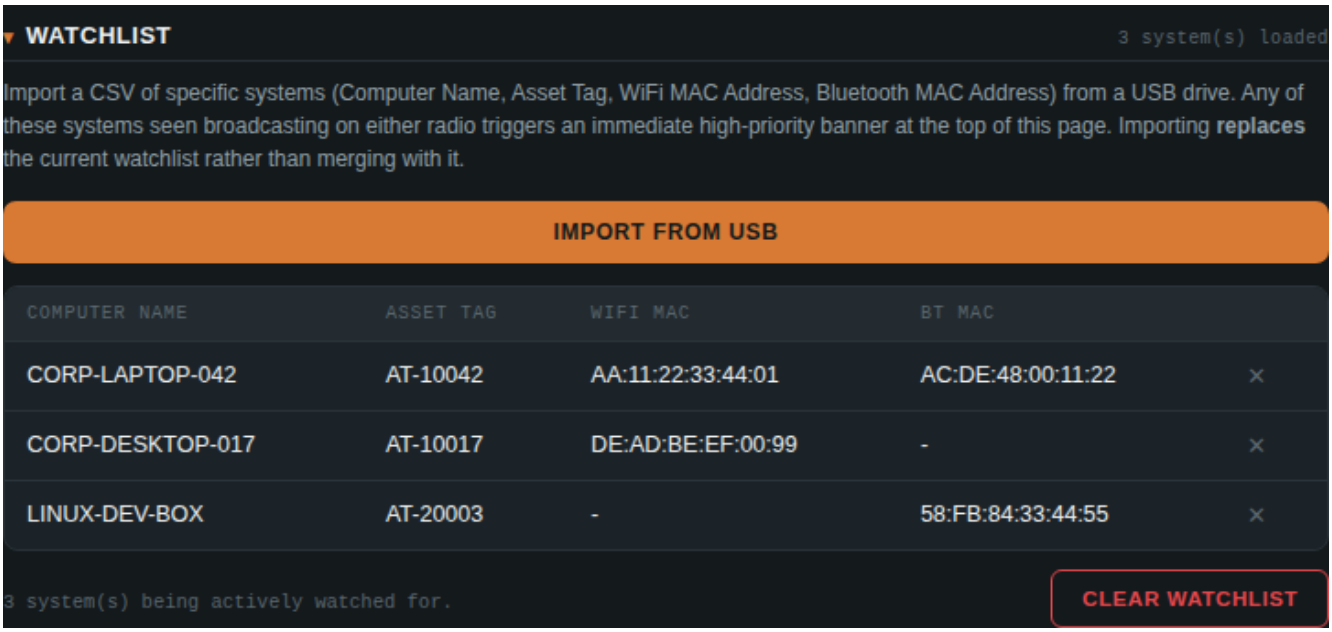


Figure 16 — The Watchlist section with systems loaded.

When a watchlisted system is detected

This is the single highest-priority thing the tool can show you. The banner is solid red, gently pulsing, and sits above even the page header. Each line identifies the computer name, asset tag, how it was seen (WiFi or Bluetooth), and its MAC address.

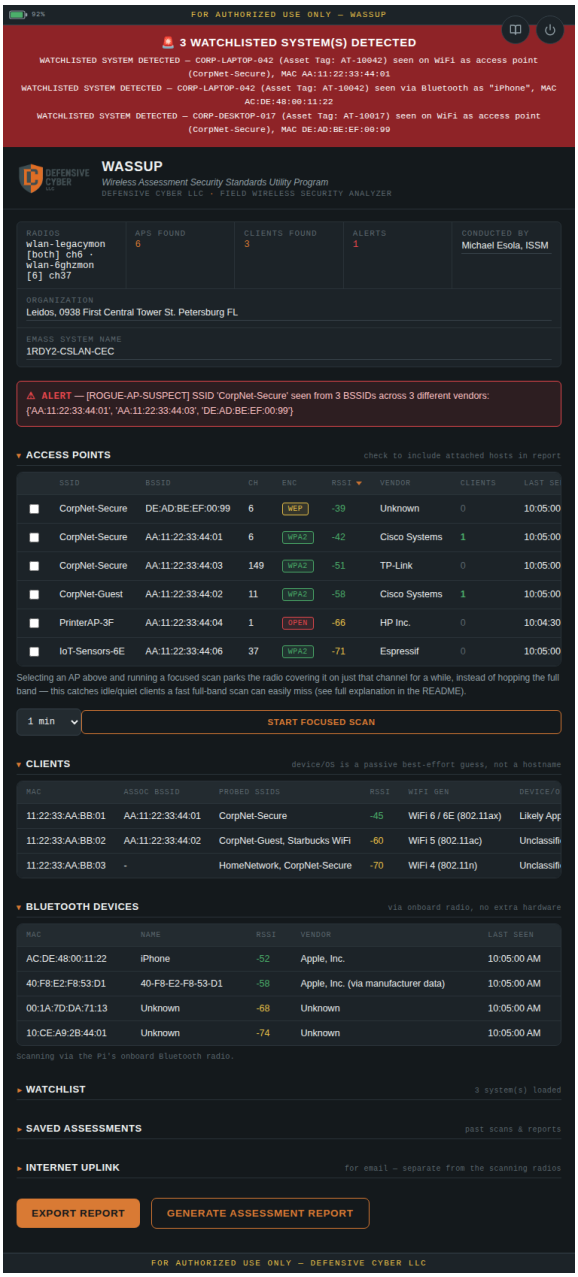


Figure 17 — A live watchlist match: the high-priority banner pinned at the top of the page.

9. Saved Assessments

Lists every scan export and generated report saved on the device, with per-file actions: Download, Email, copy to a USB drive, and delete.

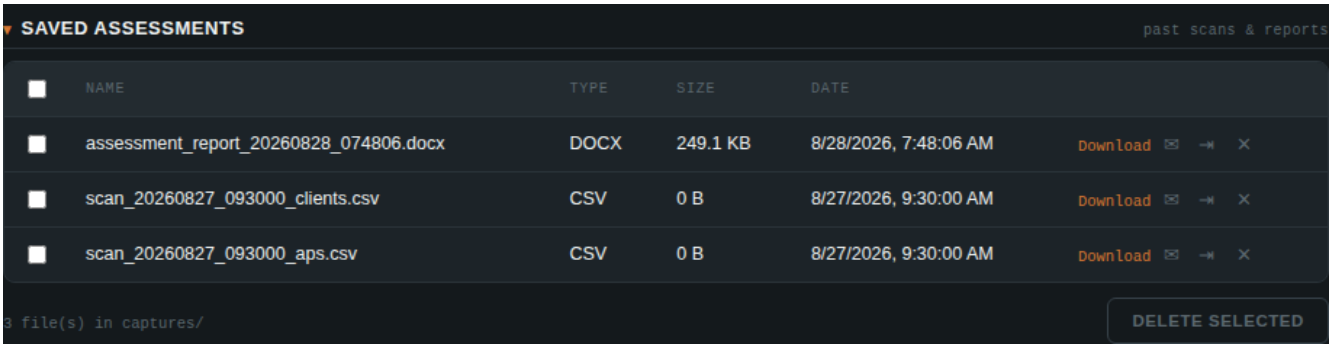


Figure 18 — Saved Assessments, listing past scan exports and reports.

Emailing a report

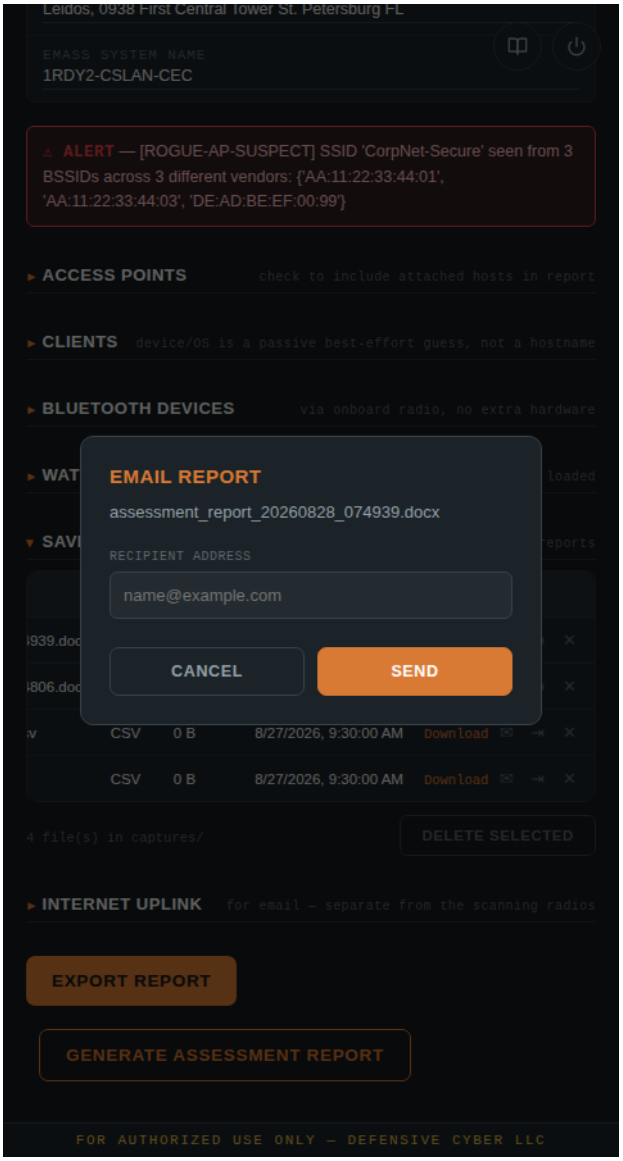


Figure 19 — Emailing a saved file to a recipient address.

Copying to a USB drive

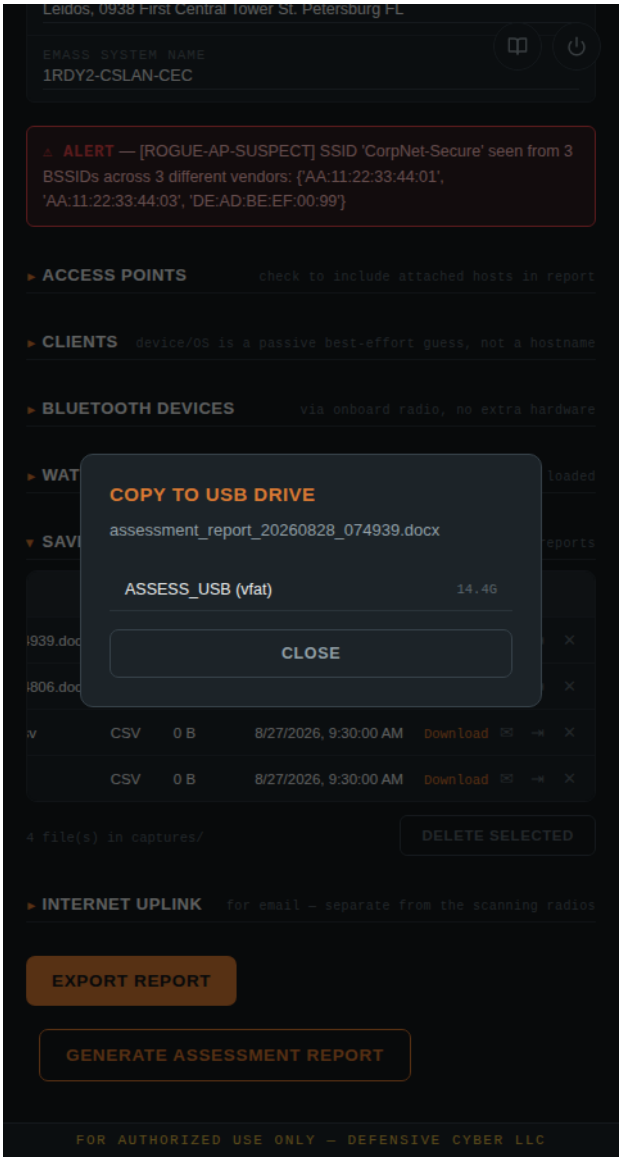


Figure 20 — Copying a report to a USB drive.

Deleting old files

Deletion is always confirmed via a modal before anything is permanently removed.

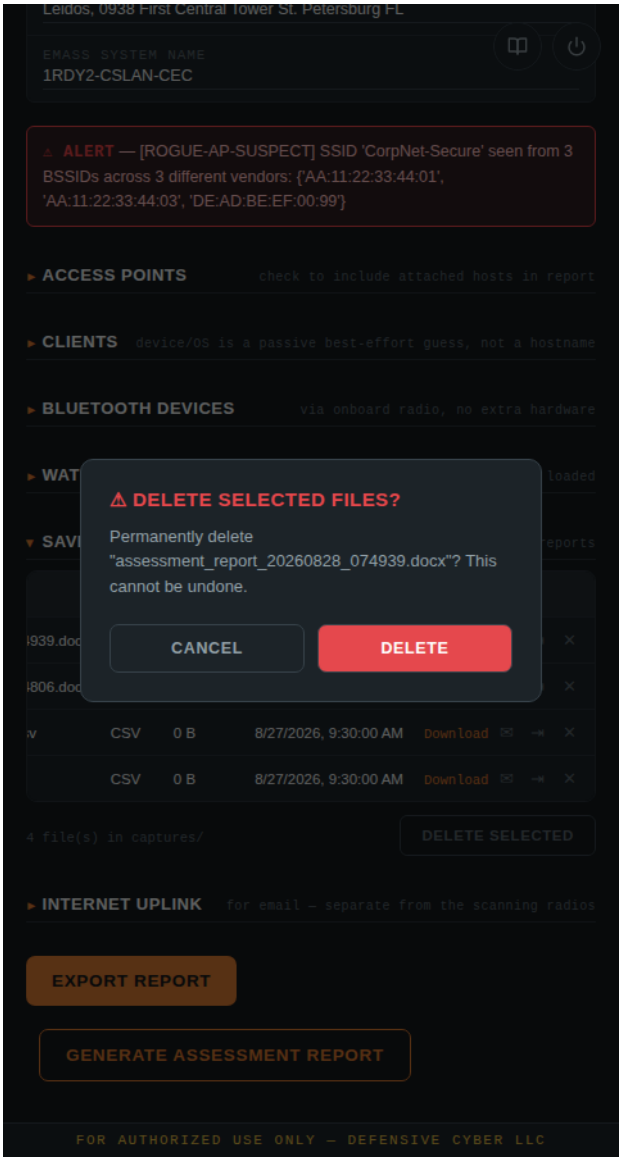


Figure 21 — Deletion requires explicit confirmation.

10. Internet Uplink — Network Details, Guest Sign-In & Saved Networks

This connects the Raspberry Pi's own **onboard** WiFi radio to a hotspot or access point for internet access — needed to send email. It is completely separate from the two scanning radios; connecting here never affects or interrupts an active scan.

1. Toggle **Onboard WiFi** on, then tap **Scan for Networks**.

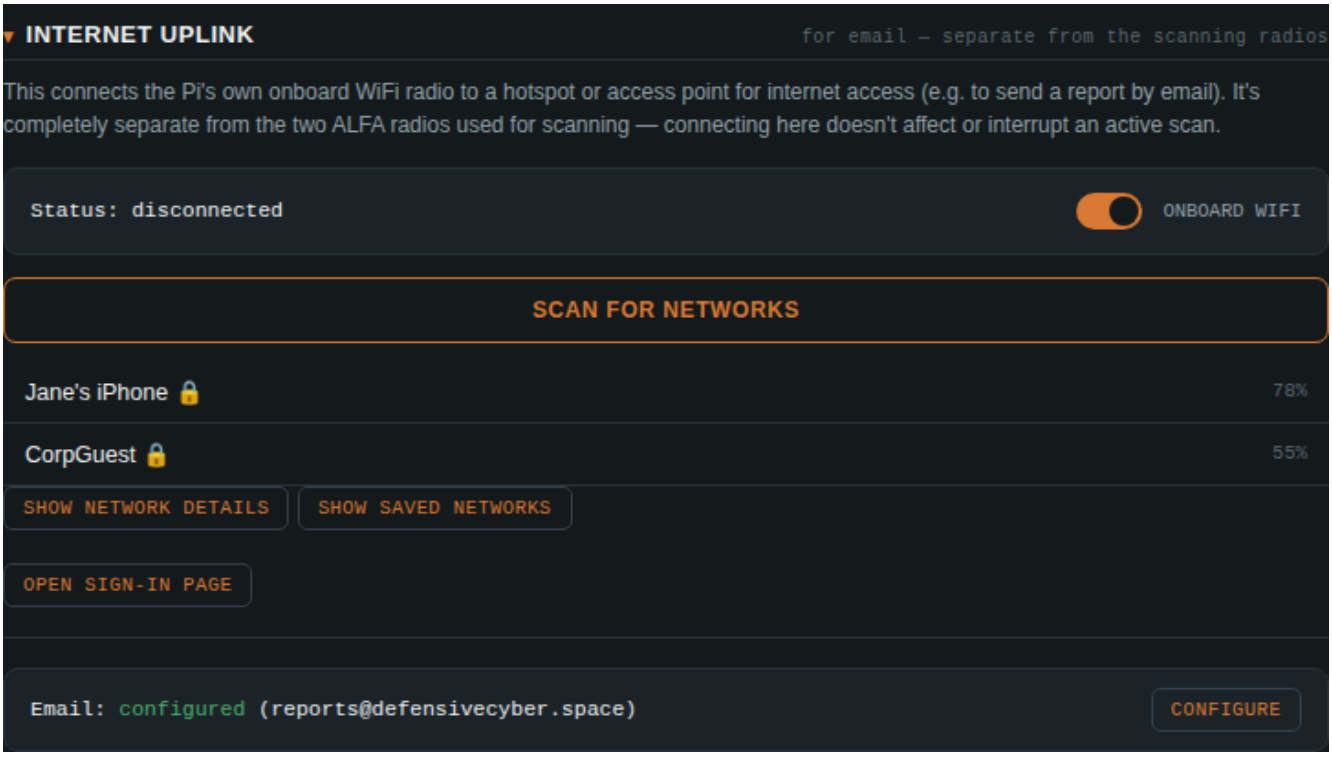


Figure 22 — Internet Uplink: onboard WiFi status and scan results.

2. Tap a network, enter the password (leave blank for open networks), and tap Connect.

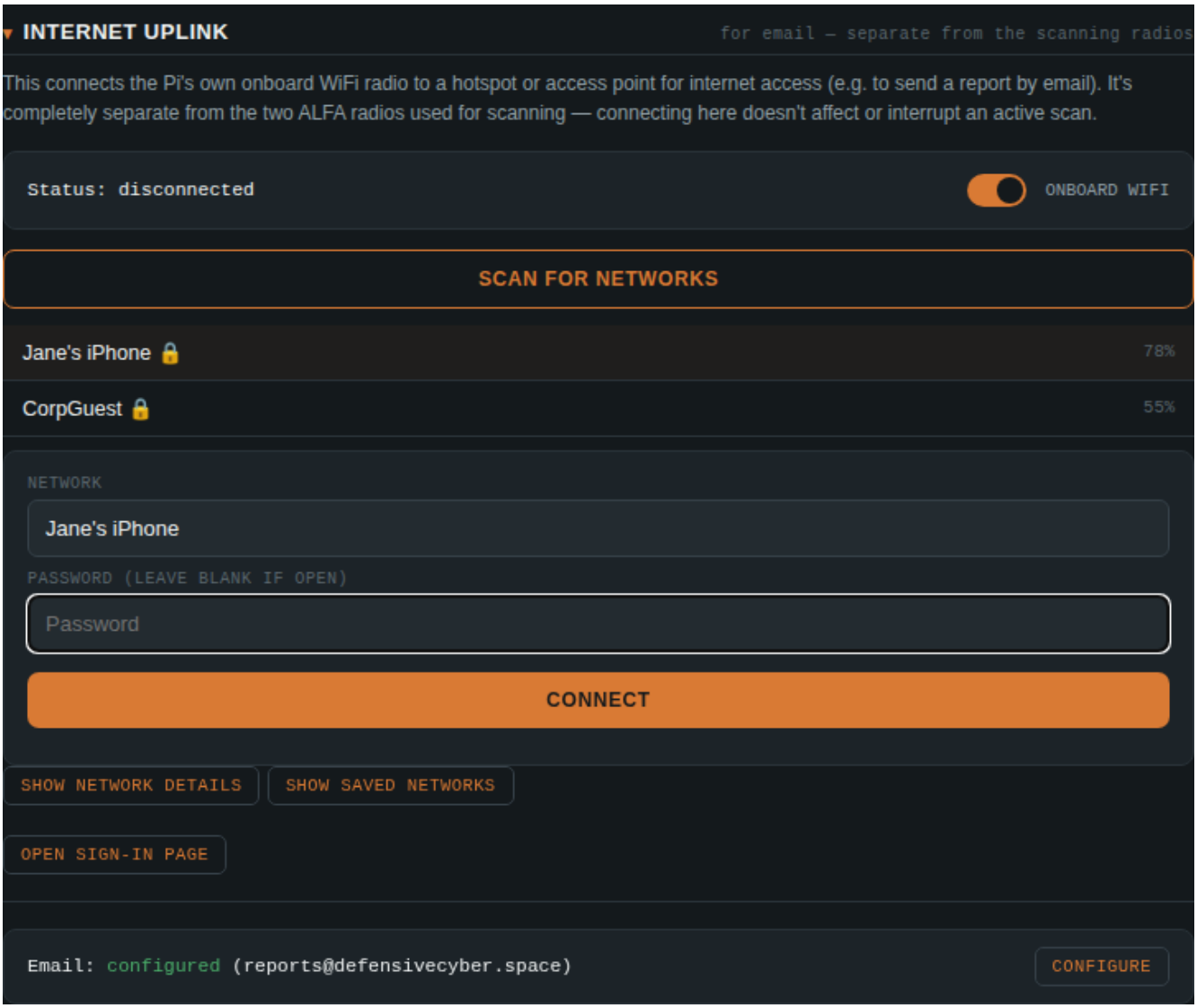


Figure 23 — Connecting to a selected network.

Viewing network details

Tap **Show Network Details** to reveal the IP address, subnet mask, and default gateway currently assigned to the onboard connection — useful for troubleshooting or confirming connectivity without needing SSH access.

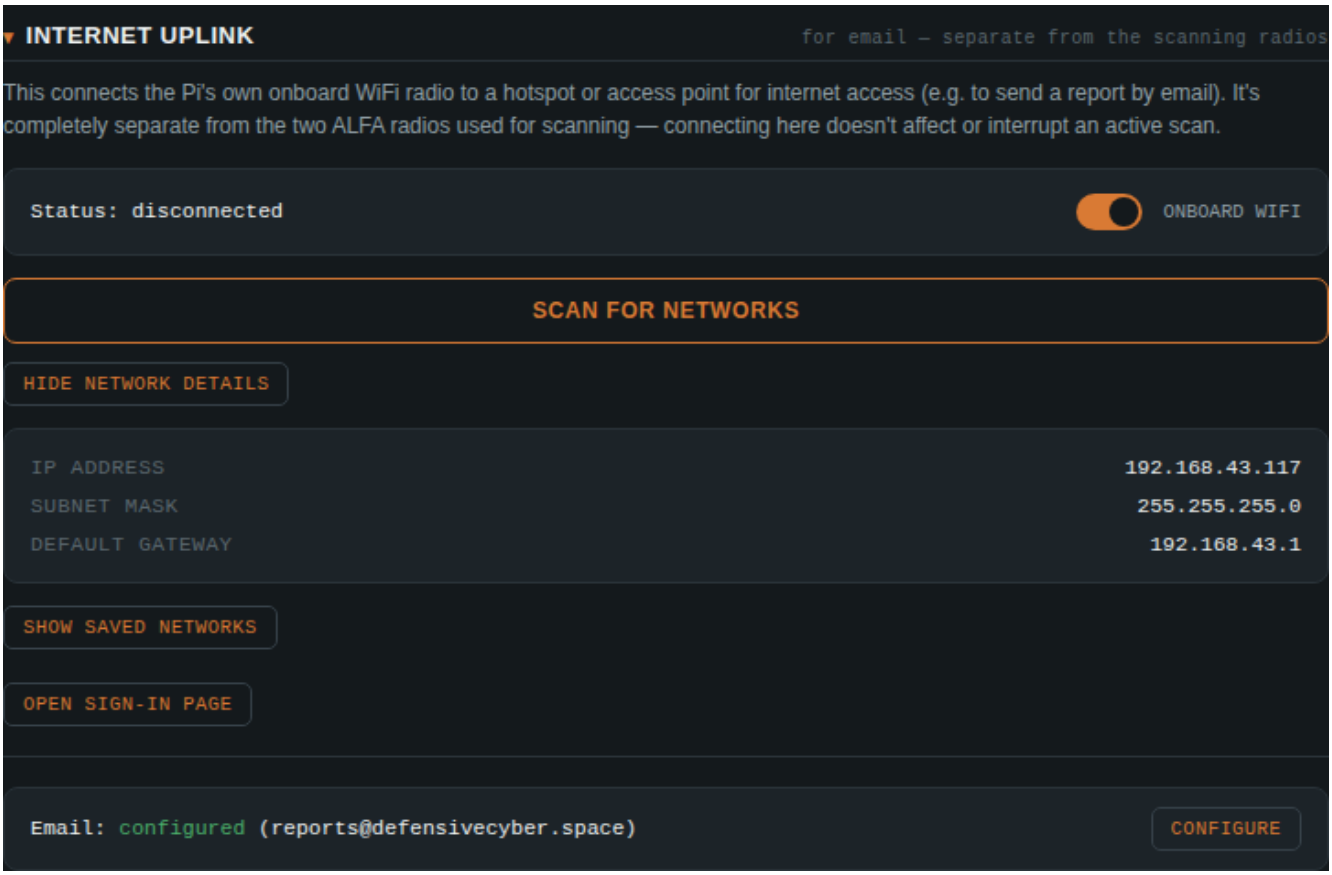


Figure 24 — IP Address, Subnet Mask, and Default Gateway, shown below the connection controls.

Managing saved networks

Tap **Show Saved Networks** to see every network this device has connected to before, each with a checkbox. Since this device is used across many different locations, this list can grow — **Forget Selected** permanently removes the saved password(s) for whichever networks you check, requiring the password to be re-entered (and any guest sign-in page re-completed) to connect again.

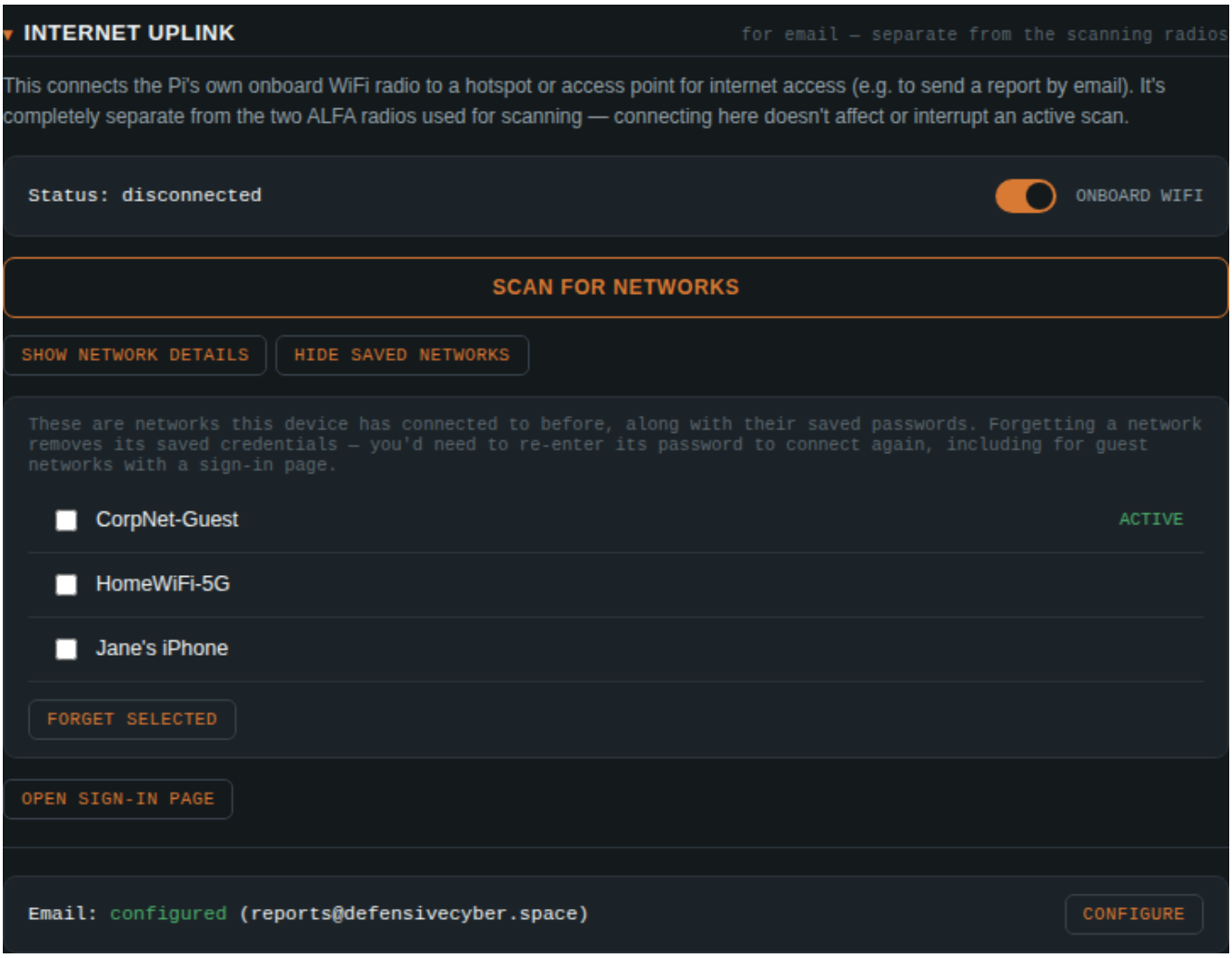


Figure 25 — Saved networks, with the currently-connected one clearly marked ACTIVE.

Forgetting the network you're currently connected through disconnects this device immediately. The confirmation dialog explicitly calls this out whenever it applies, rather than letting it happen silently.

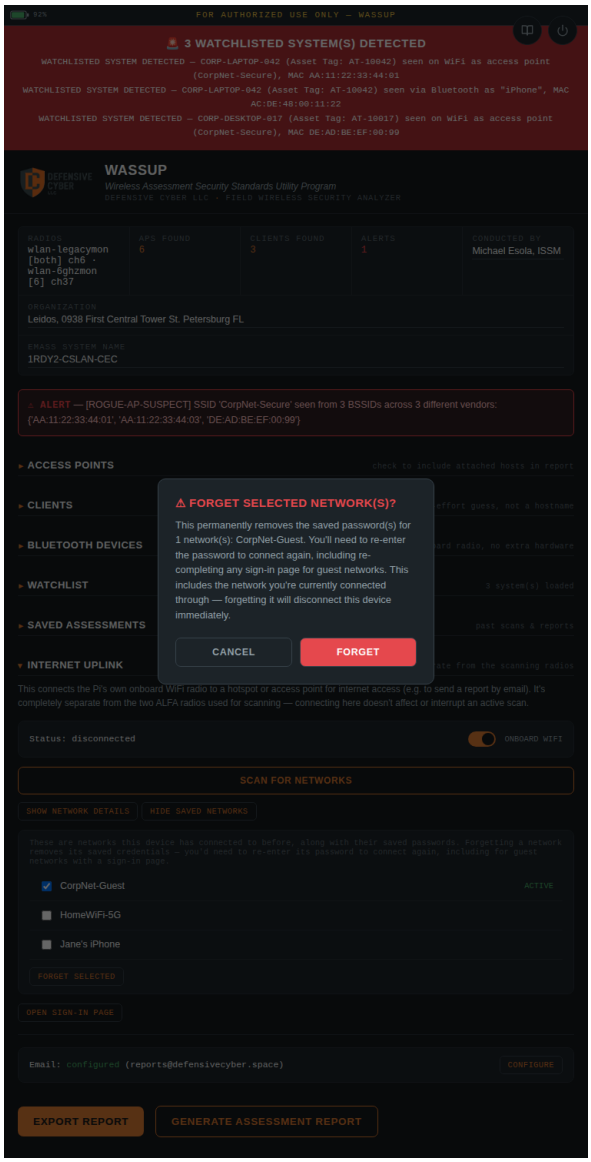


Figure 26 — The confirmation dialog explicitly names which network(s) are selected, and warns when the active connection is among them.

Signing in to guest networks

Many guest, hotel, and conference networks block real internet access until you sign in through the network's own web page — this tool detects that condition automatically a few seconds after connecting, and shows a banner here when it applies.

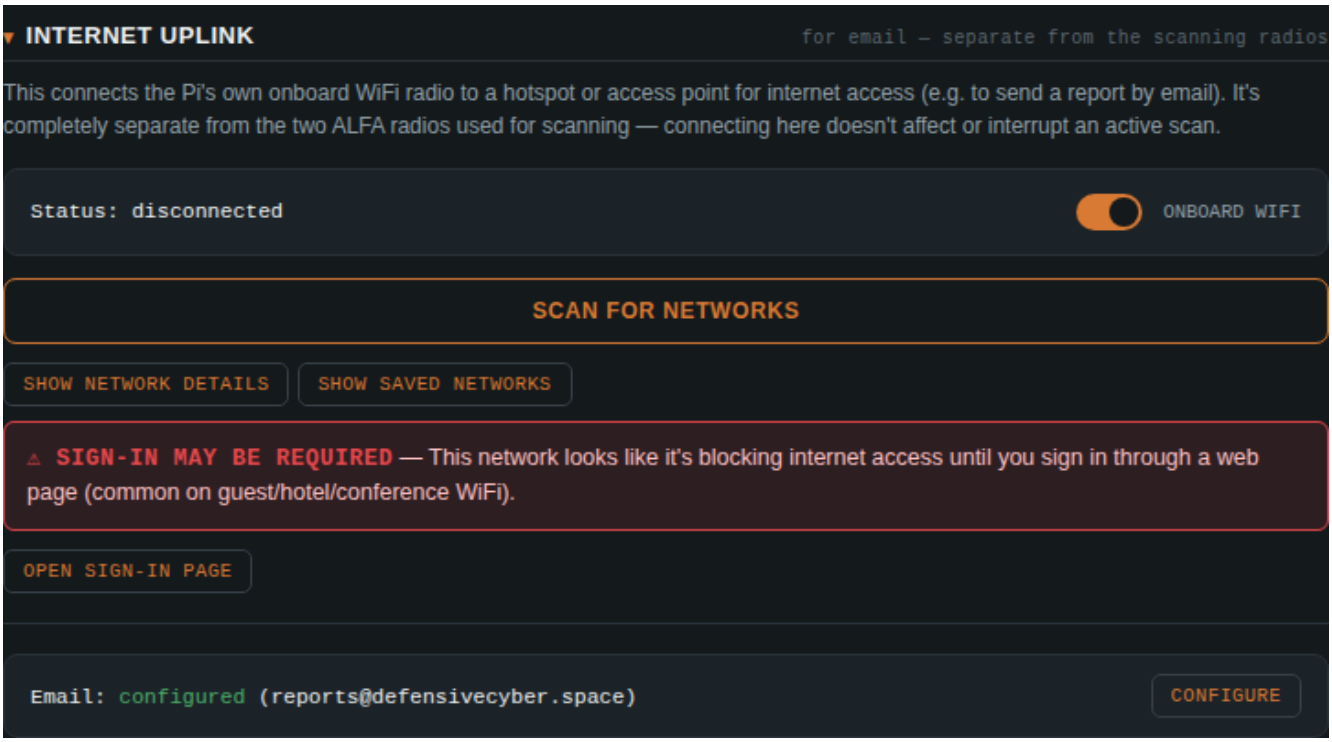


Figure 27 — A guest network's sign-in requirement, detected automatically after connecting.

Tap **Open Sign-In Page** any time — whether or not the banner above is showing — to bring up the network's own login/agreement page in a dedicated window over the dashboard. A red banner appears at the top of the screen the entire time this window is open, with two controls: a **Keyboard** toggle for typing into the sign-in page's own fields (this page is a completely different site, so the dashboard's own automatic keyboard doesn't apply to it), and a tap-anywhere area to close the window once you're done.

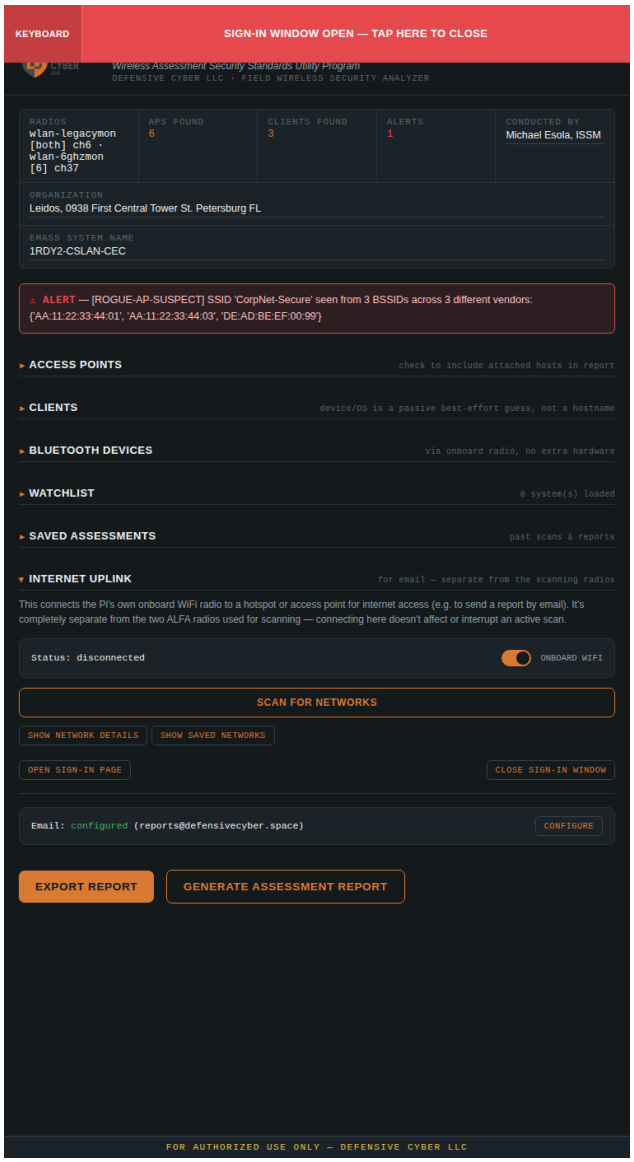


Figure 28 — The sign-in window open, with the Keyboard toggle and close banner both always reachable regardless of what the guest network's own page looks like.

The sign-in page is designed by whoever runs that network, not by this tool — it may not always display perfectly on this device's narrow screen. The window also closes itself automatically after a few minutes as a safety net, even if it's never manually dismissed.

Configuring email

Tap **Configure** next to the Email status line. The password is never sent back to the browser once saved — leaving it blank on a later edit keeps whatever password is already stored.

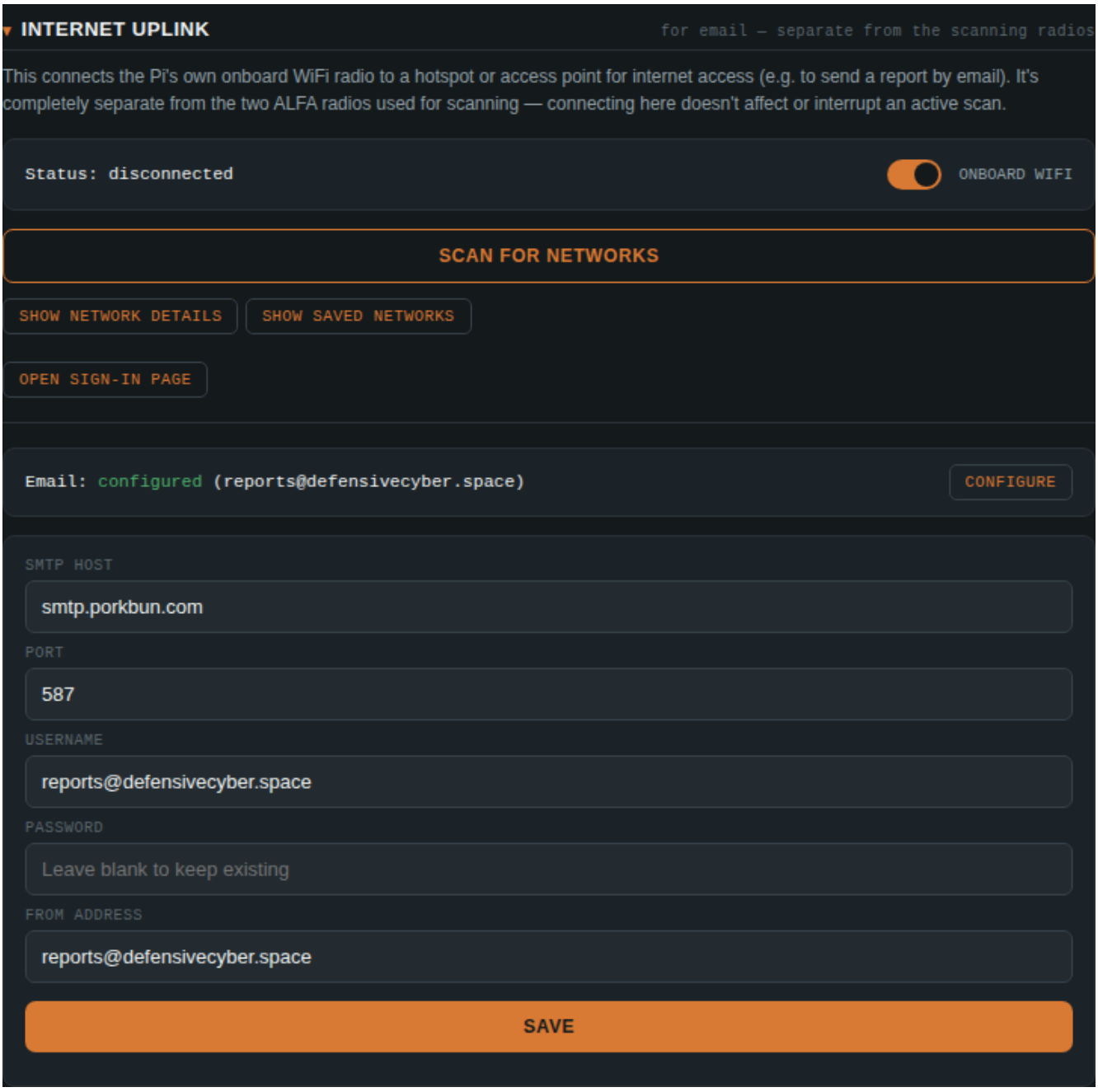


Figure 29 — Email configuration form.

11. The On-Screen Keyboard

Tapping into any text field automatically shows the on-screen keyboard and shrinks the page to make room for it; tapping away from the field automatically hides the keyboard and restores the full screen. This happens without any manual toggling.

The on-screen keyboard does not support a Caps Lock / shift-lock function — this is a limitation of the keyboard software itself, confirmed directly with its developers. For fields needing several sequential capital letters, either tap Shift before each one, or use an external USB keyboard if one is connected, which has a normal working Caps Lock key.

12. Generating Reports & What They Contain

Two buttons sit at the bottom of the dashboard:

- **Export Report** — downloads the raw scan data as CSV/JSON files.
- **Generate Assessment Report** — produces the full branded .docx report. Requires the Conducted By name to be filled in.

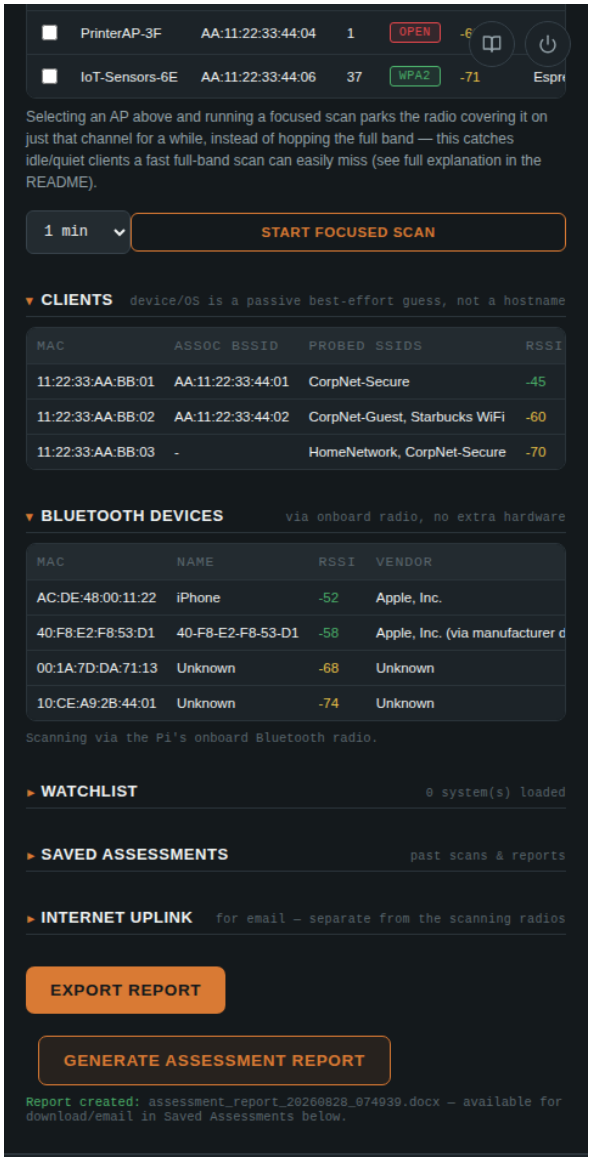


Figure 30 — After generating a report, a plain confirmation appears (not a clickable link) pointing to Saved Assessments.

Any access points checked in Section 4 have their attached hosts included in a dedicated report section automatically. The report's cover page also records the **Device Time Zone** confirmed at session start (Section 2) — every timestamp elsewhere in the report is relative to that time zone, so it's captured explicitly rather than left ambiguous.

What the Generated Report Looks Like

The pages below are a sample report (shown here with a watchlist match and two access points selected for attached-host reporting, to illustrate every section the report can contain).

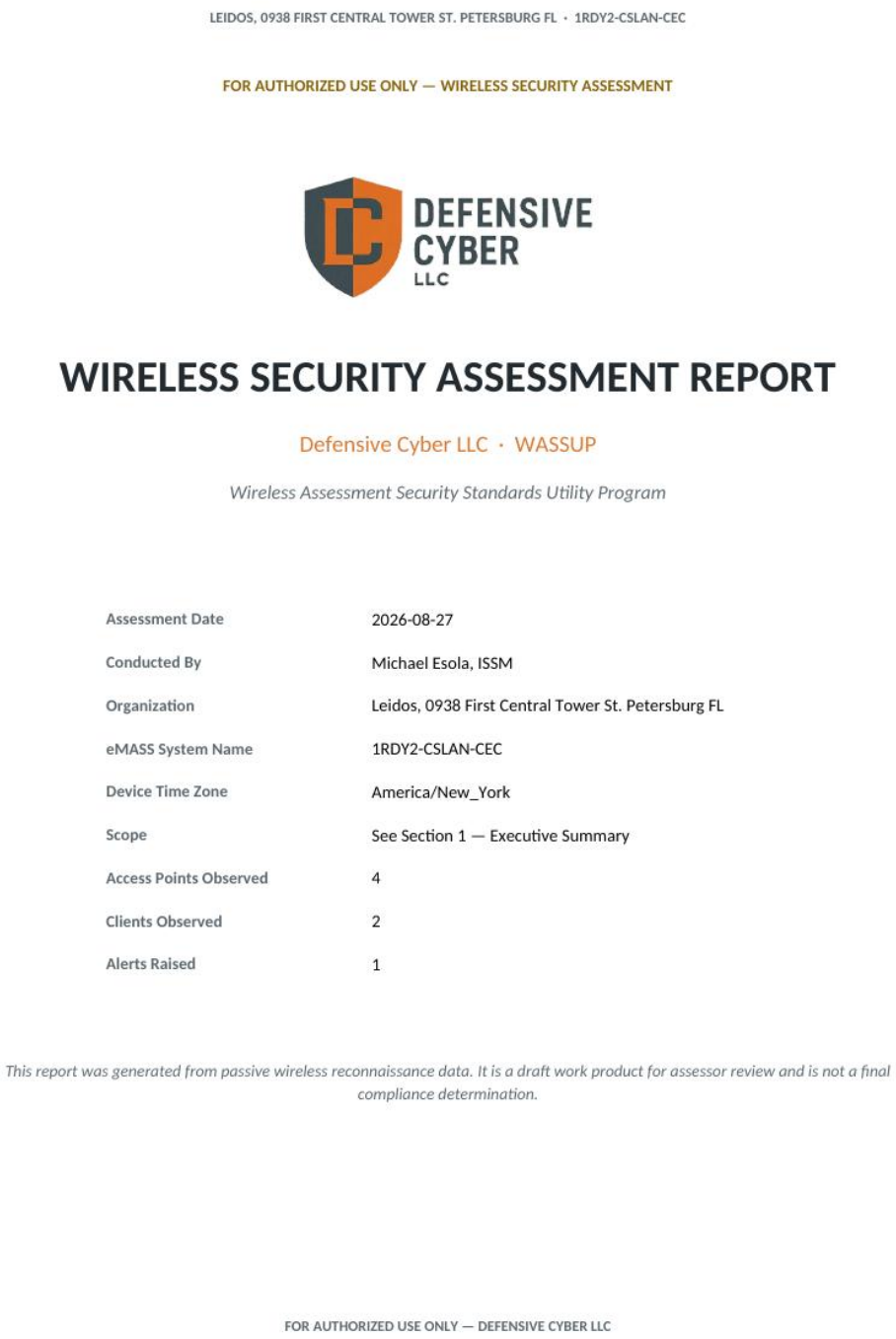


Figure 31 — Report cover page, including the confirmed Device Time Zone.

1. EXECUTIVE SUMMARY

This report summarizes the results of a passive 802.11 wireless reconnaissance session conducted on 2026-08-27 using the WASSUP. The tool discovered 4 access point(s) and 2 wireless client device(s) across the 2.4GHz, 5GHz, and 6GHz bands. 1 condition(s) were flagged for assessor follow-up.

- 2 access point(s) observed using open or WEP encryption.
- 1 potential rogue/unauthorized access point indicator(s).

2. WATCHLIST ALERTS

1 system(s) from the imported watchlist were detected during this session. This is a high-priority finding — review immediately.

Computer Name	Asset Tag	Match Type	MAC Address
CORP-LAPTOP-042	AT-10042	WIFI	AA:11:22:33:44:01

3. ACCESS POINT INVENTORY

SSID	BSSID	Ch	Encryption	RSSI	Vendor	Last Seen
CorpNet-Secure	DE:AD:BE:EF:00:99	6	WEP	-39	Unknown	2026-08-27 10:05:00
CorpNet-Secure	AA:11:22:33:44:01	6	WPA2	-42	Cisco Systems	2026-08-27 10:05:00
CorpNet-Secure	AA:11:22:33:44:03	149	WPA2	-51	TP-Link	2026-08-27 10:05:00
PrinterAP-3F	AA:11:22:33:44:04	1	OPEN	-66	HP Inc.	2026-08-27 10:04:30

4. SELECTED ACCESS POINTS — ATTACHED HOSTS

The access points below were specifically flagged for attention during the assessment. Each is shown with the client devices observed associated with it during this session. "Device/OS Guess" is a best-effort passive inference from the device's own WiFi capability broadcasts (not a hostname, and not a confirmed identification) -- treat it as a lead worth investigating further, not a fact.

CorpNet-Secure — AA:11:22:33:44:01

Encryption: WPA2 Vendor: Cisco Systems

MAC	RSSI	Probed SSIDs	Device/OS Guess	Last Seen
11:22:33:AA:BB:01	-45	CorpNet-Secure	Likely Apple (iOS/iPadOS/macOS)	2026-08-27 10:05:00
11:22:33:AA:BB:02	-55	CorpNet-Secure, Starbucks WiFi	Unclassified	2026-08-27 10:05:00

PrinterAP-3F — AA:11:22:33:44:04

Figure 32 — Executive Summary, Watchlist Alerts, Access Point Inventory, and Selected Access Points — Attached Hosts.

Encryption: OPEN Vendor: HP Inc.

No clients were observed associated with this access point during this session.

5. ALERTS

⚠️ [ROGUE-AP-SUSPECT] SSID 'CorpNet-Secure' seen from 3 BSSIDs across 3 different vendors: {'AA:11:22:33:44:01', 'AA:11:22:33:44:03', 'DE:AD:BE:EF:00:99'}

6. BLUETOOTH DEVICES

Passive Bluetooth discovery via the device's onboard Bluetooth radio -- a separate physical layer from the 802.11 wireless survey above. This inventories what was advertising/discoverable nearby during the session; it does not pair with or connect to any device.

MAC	Name	RSSI	Vendor	Last Seen
AC:DE:48:00:11:22	iPhone	-52	Apple, Inc.	2026-08-27 10:05:00
40:F8:E2:F8:53:D1	40-F8-E2-F8-53-D1	-58	Apple, Inc. (via manufacturer data)	2026-08-27 10:05:00

Figure 33 — Alerts and Bluetooth Devices, including a manufacturer-data vendor match appearing in the report exactly as it does on the dashboard.

7. RMF CONTROL ASSESSMENT (EMASS TEST RESULT ENTRIES)

DRAFT — ASSESSOR REVIEW REQUIRED. The Compliance Status shown below for each control is system-suggested from scan data using simple heuristics (encryption types observed, rogue-AP indicators). It is NOT a compliance determination. Review the Test Results narrative, complete the Assessor Determination field for each control, and sign before this information is entered into eMASS. Field names follow common DoD SAR/eMASS terminology; confirm against your organization's actual eMASS field configuration, as exact field names and allowed values vary by instance and control set version.

AC-18 — Wireless Access

Control ID	AC-18
Control Name	Wireless Access
eMASS System Name	1RDY2-CSLAN-CEC
Date Tested	2026-08-27
Tested By	Michael Esola, ISSM
Test Results	A passive wireless survey identified 4 access point(s) in range across the 2.4/5/6GHz bands. 2 access point(s) were observed using open or WEP encryption. 1 potential rogue/unauthorized access point condition(s) were flagged for follow-up (see Section 5).
Suggested Status	**Non-Compliant (system-suggested — see notice above)**
Assessor Determination	_____
Assessor Signature / Date	_____

CA-7 — Continuous Monitoring

Control ID	CA-7
Control Name	Continuous Monitoring
eMASS System Name	1RDY2-CSLAN-CEC
Date Tested	2026-08-27
Tested By	Michael Esola, ISSM
Test Results	Wireless spectrum monitoring was performed on 2026-08-27 using an automated passive scanning tool as one input to the organization's continuous monitoring activities. This single session provides point-in-time evidence; it does not by itself establish an ongoing monitoring cadence, which is a program-level determination.

Figure 34 — The RMF Control Assessment section: the draft/review notice, followed by the AC-18 control block in full.

Suggested Status	**Partial Evidence (system-suggested — see notice above)**
Assessor Determination	_____
Assessor Signature / Date	_____

CA-8 — Penetration Testing

Control ID	CA-8
Control Name	Penetration Testing
eMASS System Name	1RDY2-CSLAN-CEC
Date Tested	2026-08-27
Tested By	Michael Esola, ISSM
Test Results	This tool performs passive 802.11 reconnaissance only. No active exploitation, deauthentication, association, or frame injection was performed during this session. This control was NOT tested by this tool; a separately authorized penetration test is required to address this control.
Suggested Status	**Not Tested by This Tool (system-suggested — see notice above)**
Assessor Determination	_____
Assessor Signature / Date	_____

RA-5 — Vulnerability Monitoring and Scanning

Control ID	RA-5
Control Name	Vulnerability Monitoring and Scanning
eMASS System Name	1RDY2-CSLAN-CEC
Date Tested	2026-08-27
Tested By	Michael Esola, ISSM
Test Results	2 access point(s) were observed using open or deprecated (WEP) encryption, representing a potential wireless configuration vulnerability. 1 rogue/unauthorized access point indicator(s) were also observed. See Section 3 for the full access point inventory.

Figure 35 — CA-8 (Penetration Testing) is always marked “Not Tested by This Tool” — this tool is passive-only by design.

Suggested Status	**Non-Compliant (system-suggested — see notice above)**
Assessor Determination	_____
Assessor Signature / Date	_____

SC-40 — Wireless Link Protection

Control ID	SC-40
Control Name	Wireless Link Protection
eMASS System Name	1RDY2-CSLAN-CEC
Date Tested	2026-08-27
Tested By	Michael Esola, ISSM
Test Results	Of 4 access point(s) observed: 2 used WPA/WPA2, 1 used WEP, and 1 were open/unencrypted.
Suggested Status	**Non-Compliant (system-suggested — see notice above)**
Assessor Determination	_____
Assessor Signature / Date	_____

SI-4 — System Monitoring

Control ID	SI-4
Control Name	System Monitoring
eMASS System Name	1RDY2-CSLAN-CEC
Date Tested	2026-08-27
Tested By	Michael Esola, ISSM
Test Results	Passive RF/802.11 monitoring and channel-utilization data collection were conducted as part of system monitoring activities during this session; detailed results are included in the attached scan data exports (CSV/JSON).
Suggested Status	**Partial Evidence (system-suggested — see notice above)**
Assessor Determination	_____

Figure 36 — The final two controls, showing the range of suggested statuses the report can produce.

The Compliance Status suggested for each RMF control is a starting point based on simple heuristics — not a compliance determination. Every control block includes a blank Assessor Determination field and signature line for you to complete before anything goes into eMASS.

13. Shutting Down & Rebooting

The power button (top-right corner icon) is available on both the splash screen and the dashboard, and now offers two different actions.

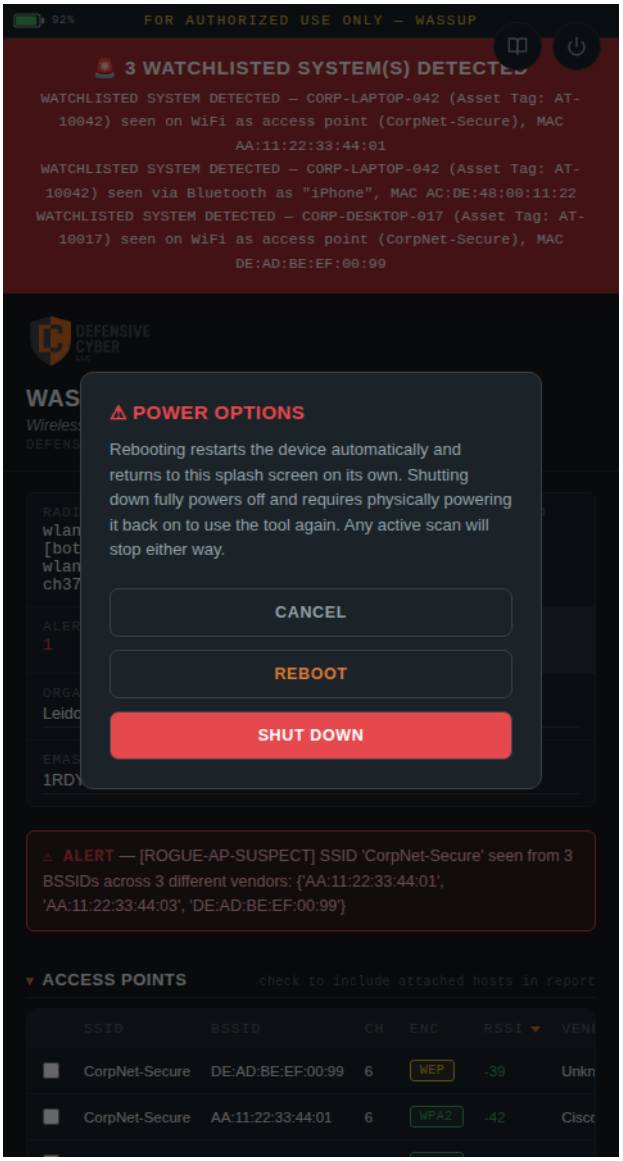


Figure 37 — Power Options: Cancel, Reboot, or Shut Down.

Reboot restarts the device automatically and returns to the splash screen on its own — no physical power switch needed. Useful after a config change, or if the tool needs a quick fresh start between assessments.

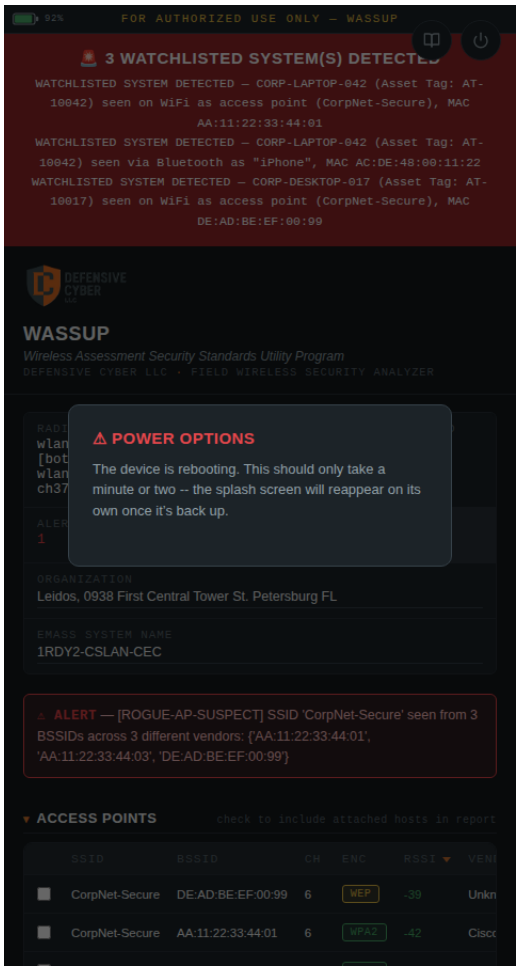


Figure 38 — After tapping Reboot, a confirmation replaces the button row while the device restarts.

Shut Down fully powers off and requires physically powering the device back on to use it again — the same full power-down procedure as before.

Full power-down procedure

1. Tap the power button, then tap **Shut Down** and confirm.
2. **Wait for the device's activity LED to go solid/off** before doing anything else.
3. Only then, flip the physical power switch to remove power from the battery.

Never remove power before the activity LED confirms shutdown has completed. Doing so risks corrupting the SD card. This caution applies only to Shut Down — Reboot handles the restart itself, with no physical switch involved.

14. Reading This Guide On the Device

This guide doesn't have to live only on a laptop or in printed form — it's also available directly on the device itself, on both the splash screen and the dashboard. Look for the book icon in the top-right corner, next to the power button.

Figure 39 — The User Guide icon (left) and power icon (right), top-right on both the splash screen and dashboard.

Tap it to open this same guide in a full-screen, scrollable viewer right on the device — read through it, scroll at your own pace, and tap **Close** to return to exactly whatever screen you were on before, with nothing lost.

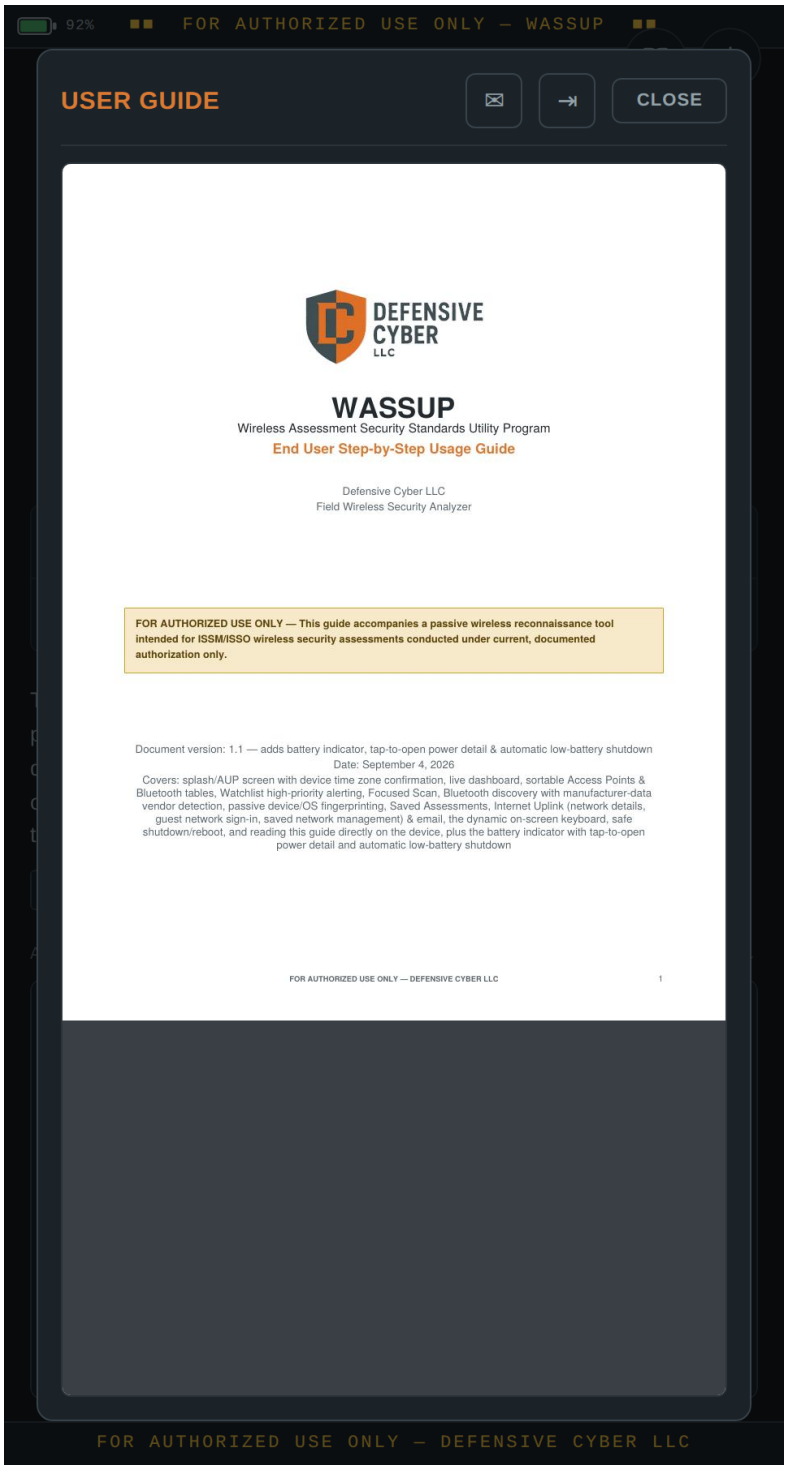


Figure 40 — The guide open in its in-app viewer. The actual guide content fills the area shown here blank in this screenshot.

The two icons next to **Close** let you get a copy of the guide itself off the device, using the exact same Email and USB export tools already covered for reports in Section 9 — nothing new to learn, just applied to this file too.

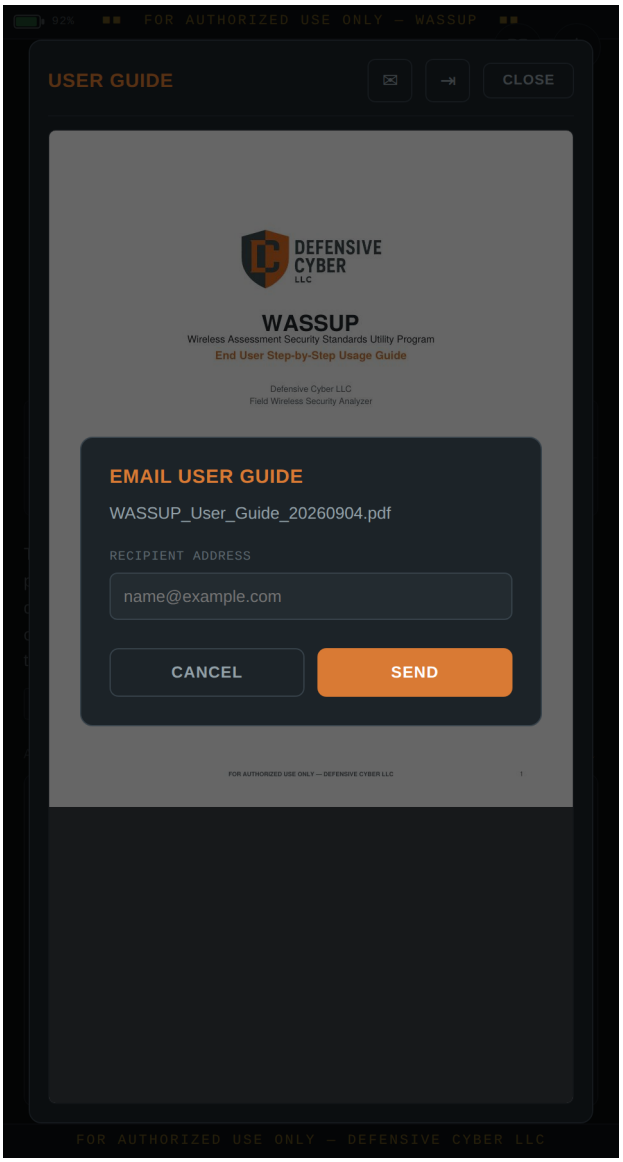


Figure 41 — Emailing the guide works identically to emailing a report, just retitled so it's clear what's being sent.

One detail worth knowing: this feature always shows whichever dated guide file is currently installed on the device — if a newer guide is ever deployed later, this icon picks it up automatically, with nothing else to reinstall or reconfigure. And since this device is never connected to a printer, the viewer deliberately hides the print button along with the rest of its built-in toolbar — scrolling through the guide works normally either way.

15. Battery Indicator & Power Monitoring

When the optional Waveshare UPS HAT is installed, WASSUP shows a live battery indicator at the top-left of the header on every screen — on the splash/AUP screen and the live dashboard alike. It sits on the same line as the centered **FOR AUTHORIZED USE ONLY — WASSUP** banner, opposite the power and guide buttons.

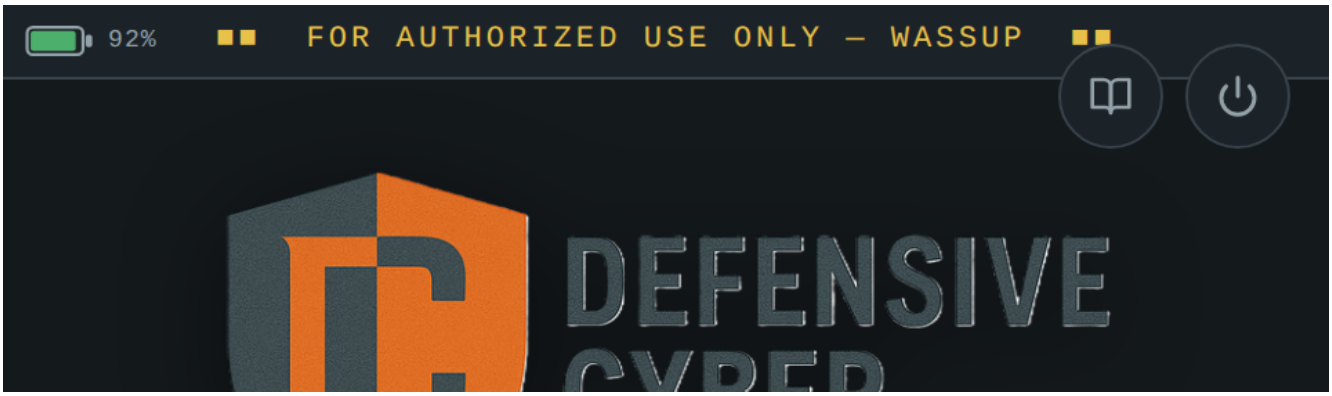


Figure 43 — The battery indicator sits at the top-left of the header.

The indicator shows the pack's charge level as a small battery icon and a single percentage for the whole pack. It is green when healthy, amber as it gets lower, and red when the battery is nearly empty. While the device is charging, a lightning bolt appears over the icon.

Tapping for battery detail

Tapping the battery icon opens a detail popover directly beneath it. It shows the pack percentage, the estimated time remaining before an automatic safe shutdown, the pack voltage, the current draw in milliamps and watts, and the individual voltage of each of the four battery cells. Tap the icon again, the ×, or anywhere outside the popover to close it.

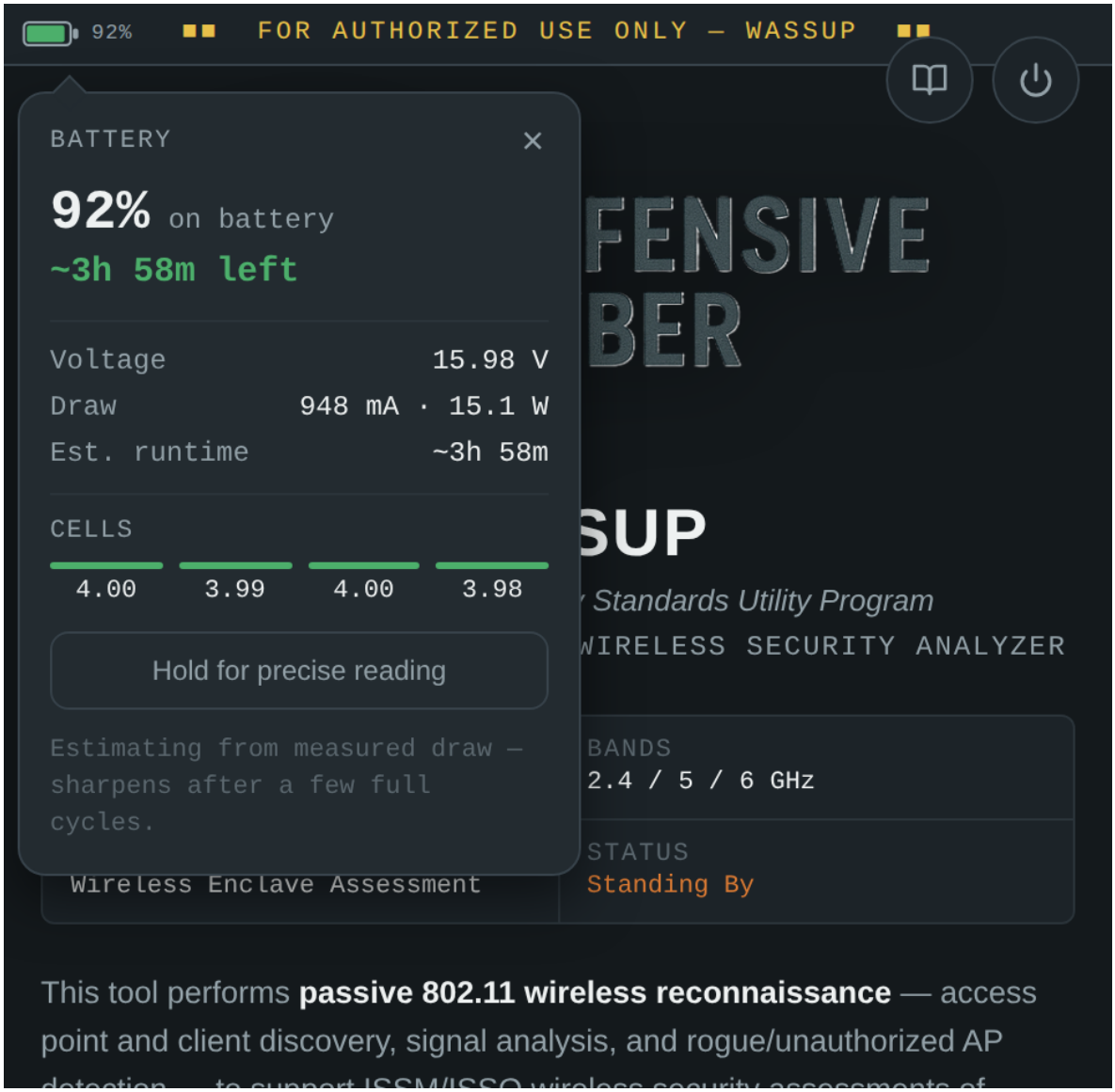


Figure 44 — The battery detail popover, opened by tapping the indicator.

Getting a precise reading

The live time-remaining figure is a moving estimate that reflects the current load, so it shifts as the radios, Bluetooth, and fan draw more or less power. For a deliberate, settled number, press and hold the **Hold for precise reading** control at the bottom of the popover. It samples the actual draw for 60 seconds, then writes a precise time-remaining figure and the averaged draw back into the popover. The reading is forgiving — once it starts it keeps counting even if your finger drifts off, and a tap anywhere cancels it.

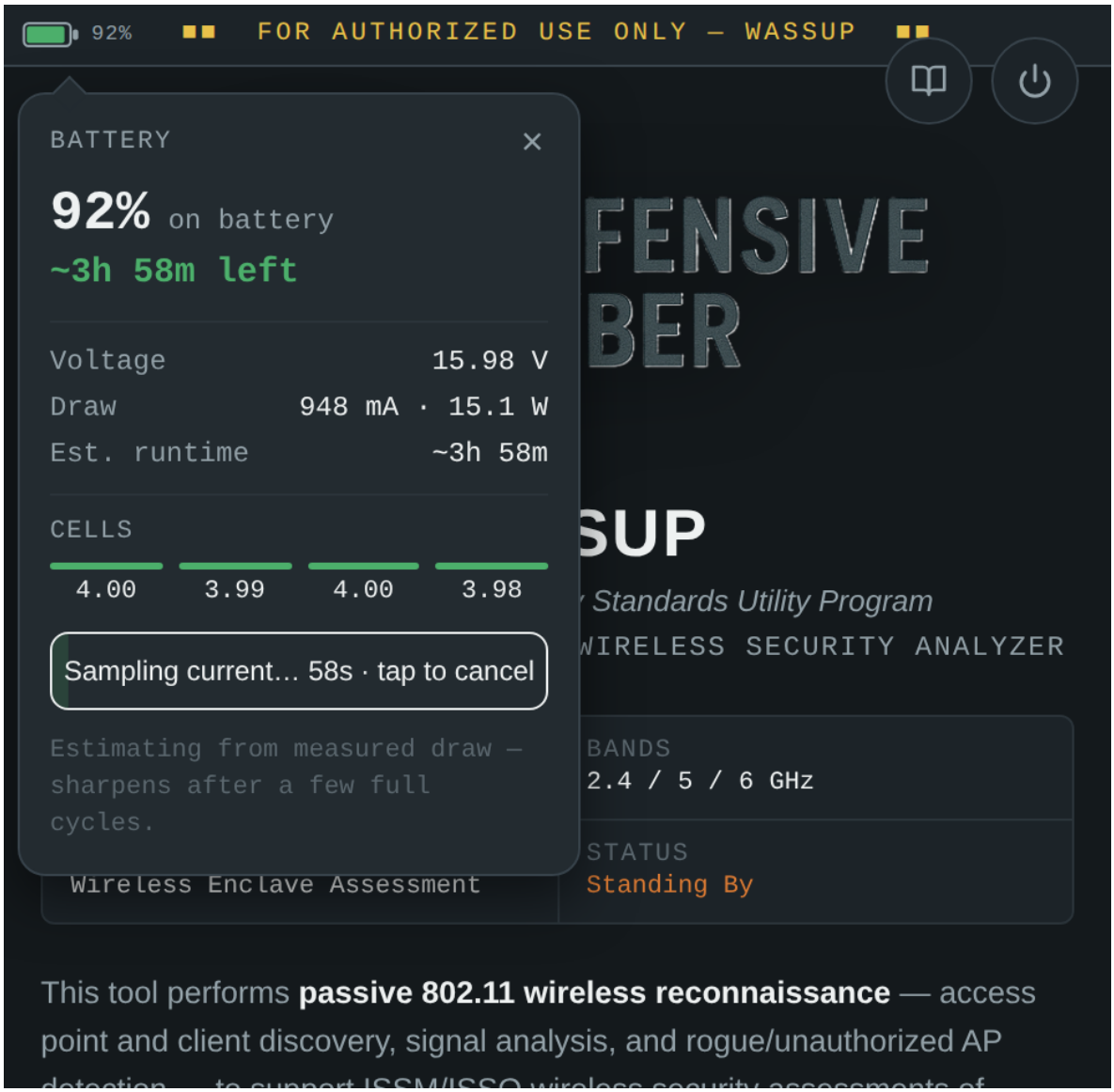


Figure 45 — Holding for a precise 60-second averaged reading.

Automatic low-battery shutdown

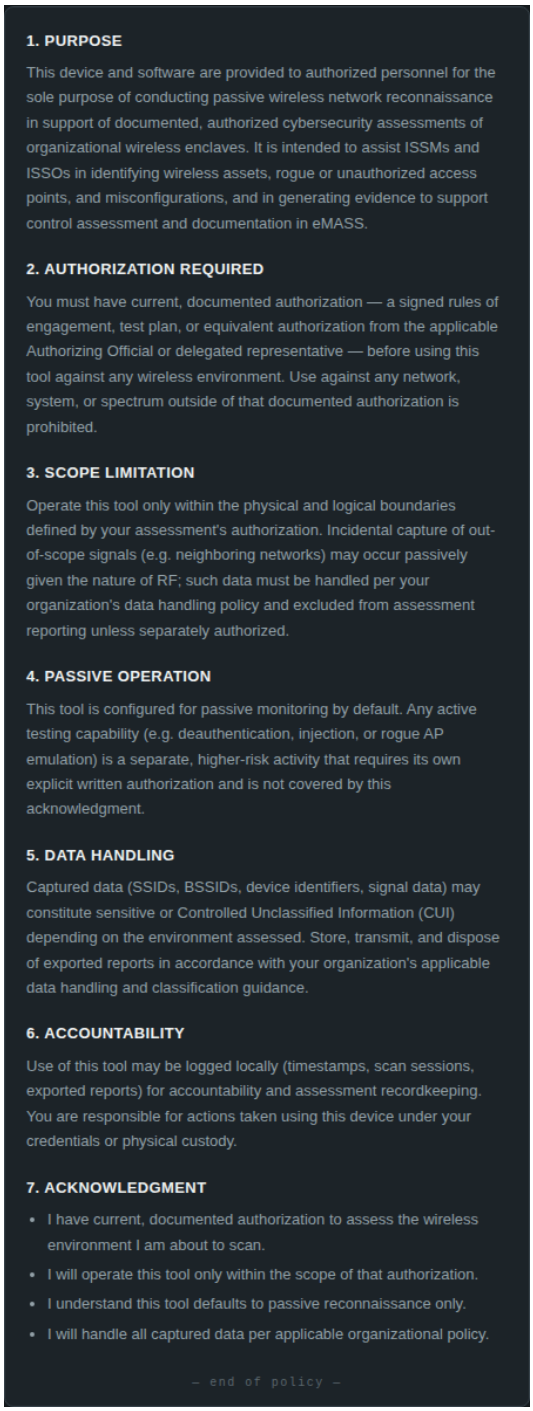
Independently of the on-screen indicator, WASSUP watches the pack and shuts the device down cleanly when the battery gets too low to keep running safely, flushing saved data to the SD card first so nothing is corrupted by a sudden loss of power. This runs in the background whether or not anyone is looking at the screen. If the device is plugged back in afterward, it powers itself back on automatically.

Note: the estimated time remaining and the pack percentage become more accurate after the battery has been through a few full charge and discharge cycles, which lets the gauge learn the pack’s true capacity. The live voltage, current, and per-cell readings are always accurate.

Appendix A

Full Acceptable Use Policy Text

This is the complete policy text shown on the splash screen, which must be scrolled through in full before the acknowledgment checkbox becomes available.



1. PURPOSE

This device and software are provided to authorized personnel for the sole purpose of conducting passive wireless network reconnaissance in support of documented, authorized cybersecurity assessments of organizational wireless enclaves. It is intended to assist ISSMs and ISSOs in identifying wireless assets, rogue or unauthorized access points, and misconfigurations, and in generating evidence to support control assessment and documentation in eMASS.

2. AUTHORIZATION REQUIRED

You must have current, documented authorization — a signed rules of engagement, test plan, or equivalent authorization from the applicable Authorizing Official or delegated representative — before using this tool against any wireless environment. Use against any network, system, or spectrum outside of that documented authorization is prohibited.

3. SCOPE LIMITATION

Operate this tool only within the physical and logical boundaries defined by your assessment's authorization. Incidental capture of out-of-scope signals (e.g. neighboring networks) may occur passively given the nature of RF; such data must be handled per your organization's data handling policy and excluded from assessment reporting unless separately authorized.

4. PASSIVE OPERATION

This tool is configured for passive monitoring by default. Any active testing capability (e.g. deauthentication, injection, or rogue AP emulation) is a separate, higher-risk activity that requires its own explicit written authorization and is not covered by this acknowledgment.

5. DATA HANDLING

Captured data (SSIDs, BSSIDs, device identifiers, signal data) may constitute sensitive or Controlled Unclassified Information (CUI) depending on the environment assessed. Store, transmit, and dispose of exported reports in accordance with your organization's applicable data handling and classification guidance.

6. ACCOUNTABILITY

Use of this tool may be logged locally (timestamps, scan sessions, exported reports) for accountability and assessment recordkeeping. You are responsible for actions taken using this device under your credentials or physical custody.

7. ACKNOWLEDGMENT

- I have current, documented authorization to assess the wireless environment I am about to scan.
- I will operate this tool only within the scope of that authorization.
- I understand this tool defaults to passive reconnaissance only.
- I will handle all captured data per applicable organizational policy.

– end of policy –

Figure 42 — The complete Acceptable Use Policy, in full.