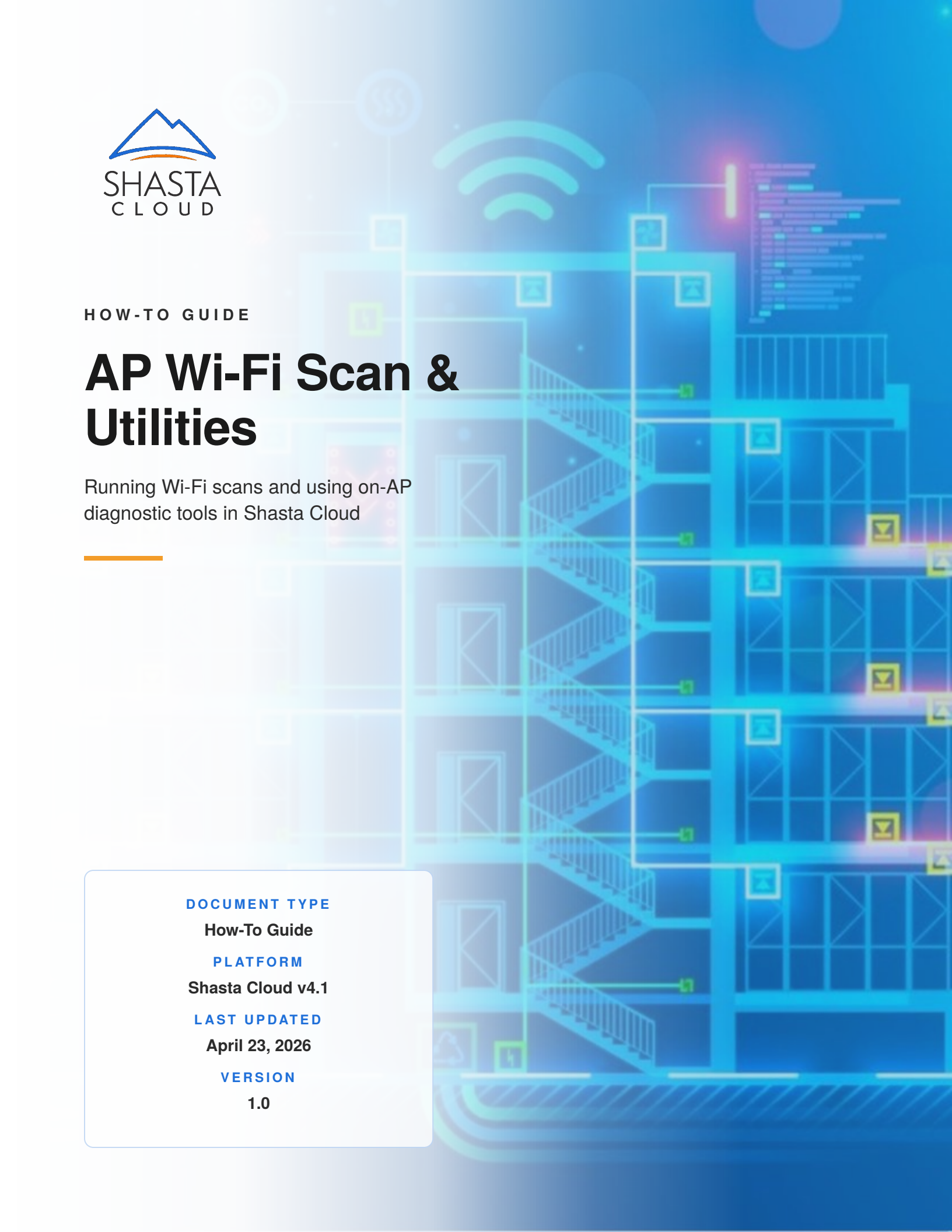
SHASTA CLOUD

HOW-TO GUIDE

AP Wi-Fi Scan & Utilities

Running Wi-Fi scans and using on-AP diagnostic tools in Shasta Cloud



DOCUMENT TYPE
How-To Guide

PLATFORM
Shasta Cloud v4.1

LAST UPDATED
April 23, 2026

VERSION
1.0

Contents

Table of Contents

Overview

Shasta Cloud provides built-in diagnostic and troubleshooting tools directly accessible from each access point's detail page. These tools let administrators run network diagnostics, scan for nearby Wi-Fi networks, and test throughput — all without needing physical access to the device. Live examples throughout this guide come from the **EAP-105** AP in the **Shasta MDU** venue.

Scope: Access Points **Role: MSP-Admin / Org-Admin** **Live Example: EAP-105 / Shasta MDU** **Shasta Cloud Platform**

Section 1 — Overview

Tool	Where to Find It	Use Case
Wi-Fi Scan	Three-dot menu (⋮) → Wi-Fi Scan	Discover nearby SSIDs, channels, and 802.11 information elements from neighboring networks.
Ping	Utilities tab → Ping	Test basic connectivity from the AP to an IP address or hostname.
Trace Route	Utilities tab → Trace Route	Map the network path hop-by-hop from the AP to a destination.
DNS Lookup	Utilities tab → DNS Lookup	Resolve a hostname to IP address(es) using the AP's DNS server.
iperf3	Utilities tab → iperf3	Run a network throughput test to measure bandwidth from the AP.

AP Must Be Online: All tools require the AP to have an **Online** status. Commands sent to offline APs will not execute.

Section 2 — Accessing an Access Point

Navigate to the AP detail page to use Utilities or Wi-Fi Scan:

1. **Click Infrastructure in the left nav.** Expand the Infrastructure menu and click **Infrastructure** to view all devices.
2. **Click the AP name.** Click the name of the access point to open its detail page. You can also navigate via `Venues → [Venue] → Infrastructure`.

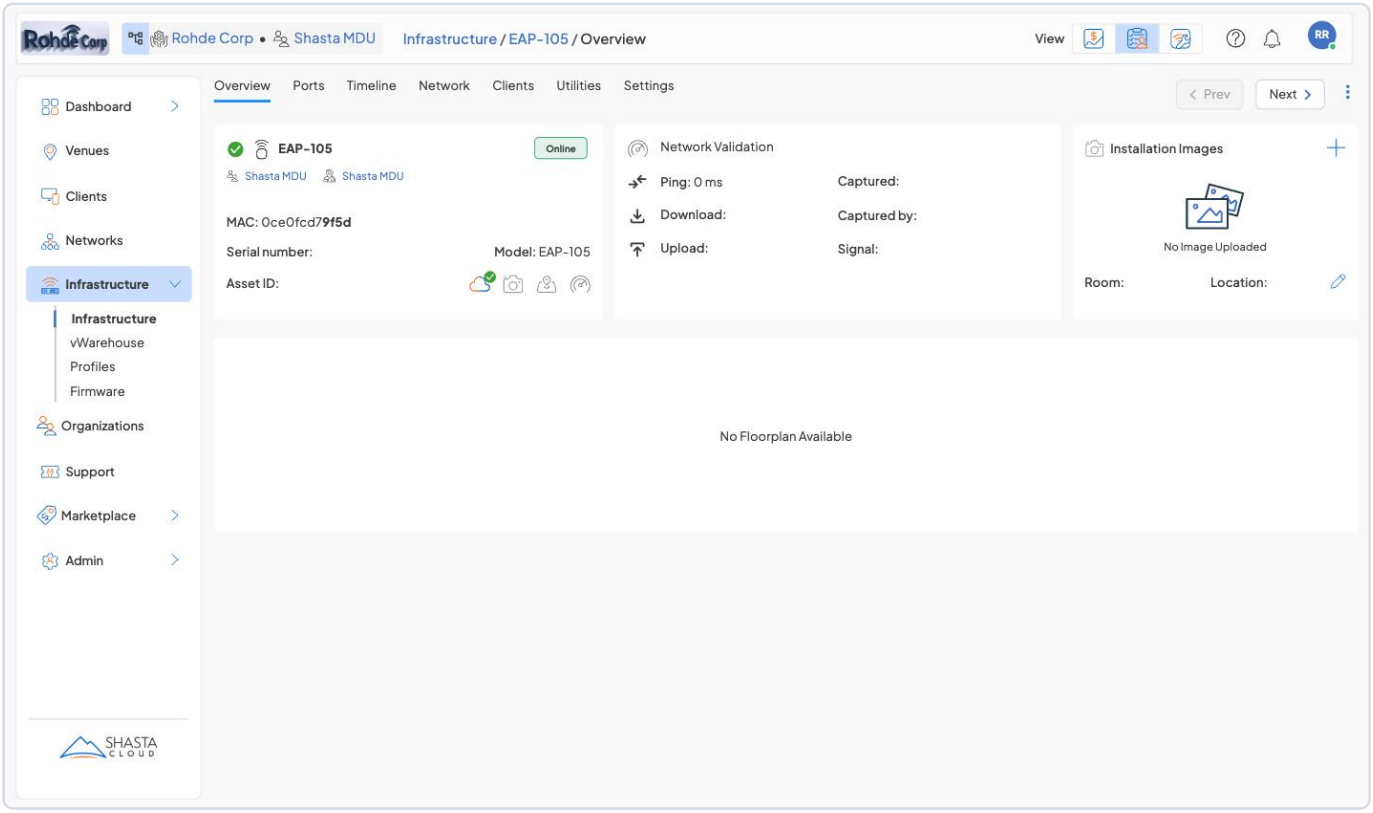


Figure 1 — The EAP-105 detail page in Shasta MDU showing Online status, MAC address, model, and the tab bar including Overview, Ports, Timeline, Network, Clients, Utilities, and Settings.

Section 3 — AP Quick Actions (Three-Dot Menu)

Click the ⋮ icon in the upper right of the AP detail page to access quick actions including **Wi-Fi Scan**.

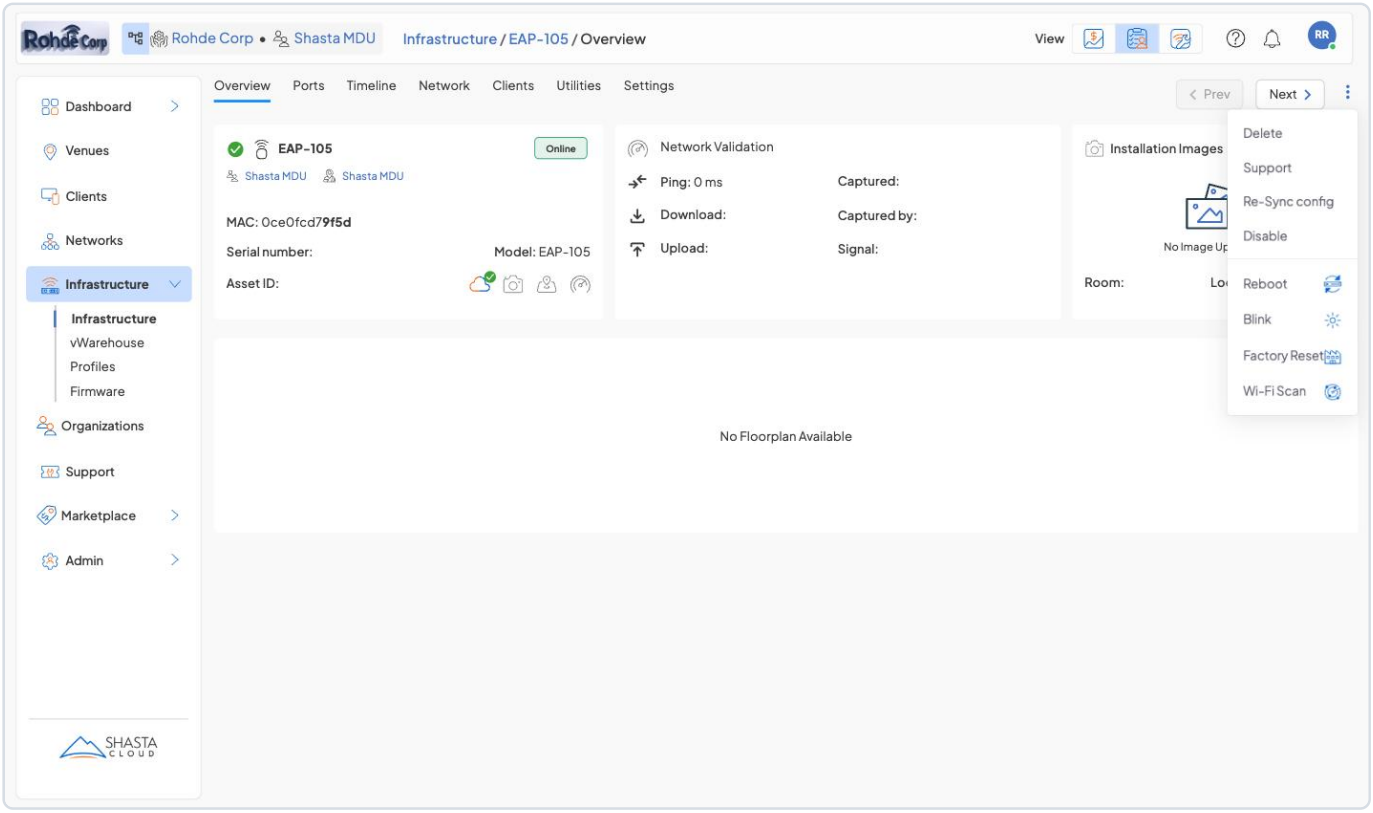


Figure 2 — The three-dot menu on the EAP-105 showing available actions: Delete, Support, Re-Sync config, Disable, Reboot, Blink, Factory Reset, and Wi-Fi Scan.

Action	Description
Delete	Remove the AP from the system. Cannot be undone.
Support	Generate a support bundle for this device.
Re-Sync config	Push current cloud configuration down to the AP to resolve any drift.
Disable	Administratively disable the AP from serving clients.
Reboot	Remotely restart the AP.
Blink	Cause the AP's LEDs to blink for physical identification.
Factory Reset	Reset the AP to factory defaults. Erases all local config.

Action	Description
Wi-Fi Scan	Launch a passive radio scan to detect nearby wireless networks.

Section 4 — Wi-Fi Scan — Configuration

Wi-Fi Scan instructs the AP to perform a passive radio scan of the surrounding wireless environment, reporting nearby SSIDs, channels, and 802.11 information elements. It is useful for **site surveys**, **channel planning**, and **interference detection**.

> **Temporary Radio Interruption:** Running a Wi-Fi Scan briefly takes the AP's radio(s) off-channel. This may cause a momentary interruption for connected wireless clients. Schedule during low-usage periods when possible.

From the AP detail page, click the three-dot icon (⋮) in the upper right, then click **Wi-Fi Scan**. The Wi-Fi Scan configuration modal opens:

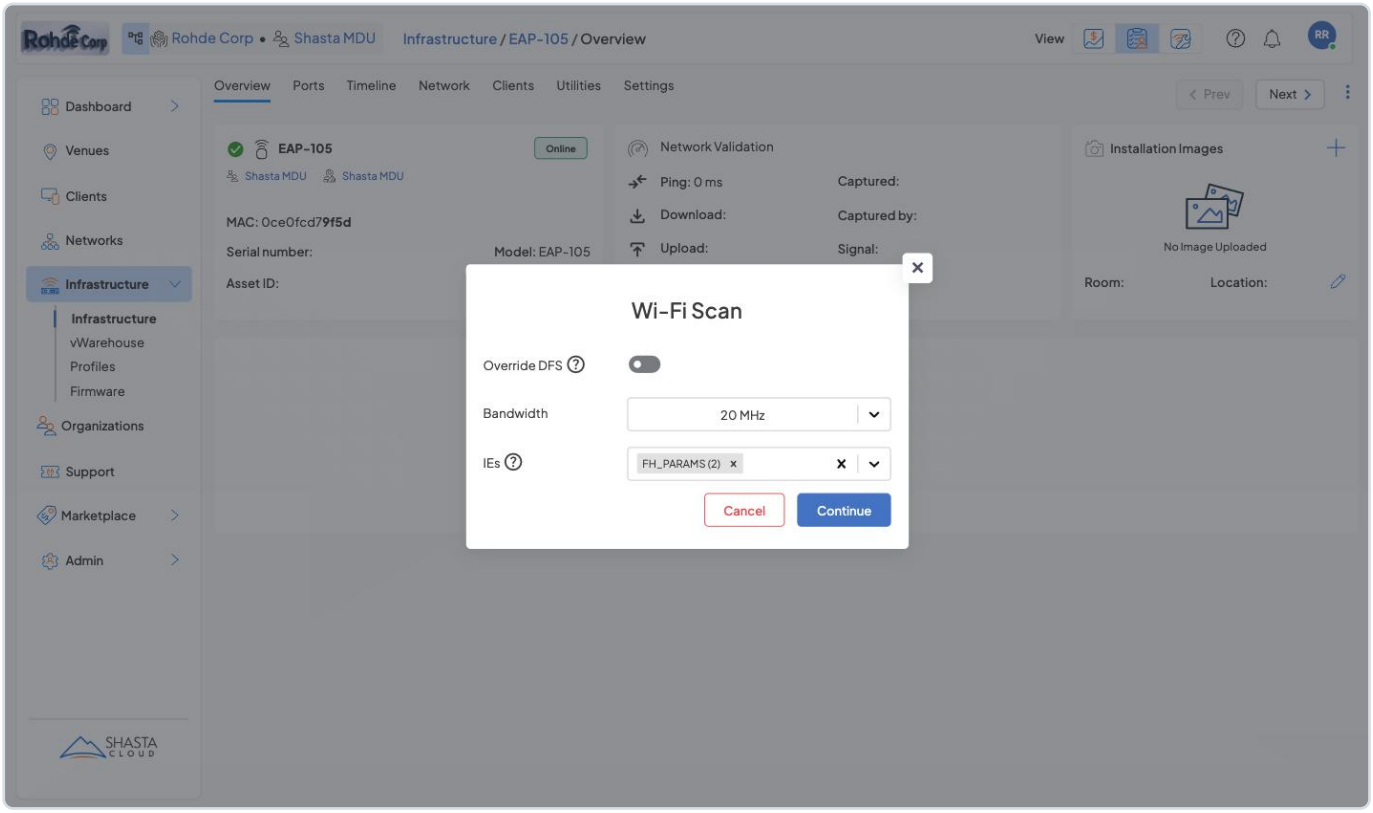


Figure 3 — The Wi-Fi Scan modal with three settings: Override DFS toggle, Bandwidth dropdown, and IEs (Information Elements) multi-select.

Field	Default	Description
Override DFS	`OFF`	When ON, includes DFS channels (52–144 in 5 GHz) in the scan. These channels are restricted by default due to radar detection requirements. Enable only when needed.
Bandwidth	`20 MHz`	Channel width for scanning. `20 MHz` detects the widest range of networks. Options: 20, 40, 80, 160 MHz.
IEs (Information Elements)	`FH_PARAMS (2)`	802.11 IEs to include in scan results. Multiple values can be selected. Common options include SSID (0), DS_PARAMS (3) for channel info, and SUPP_RATES (1).

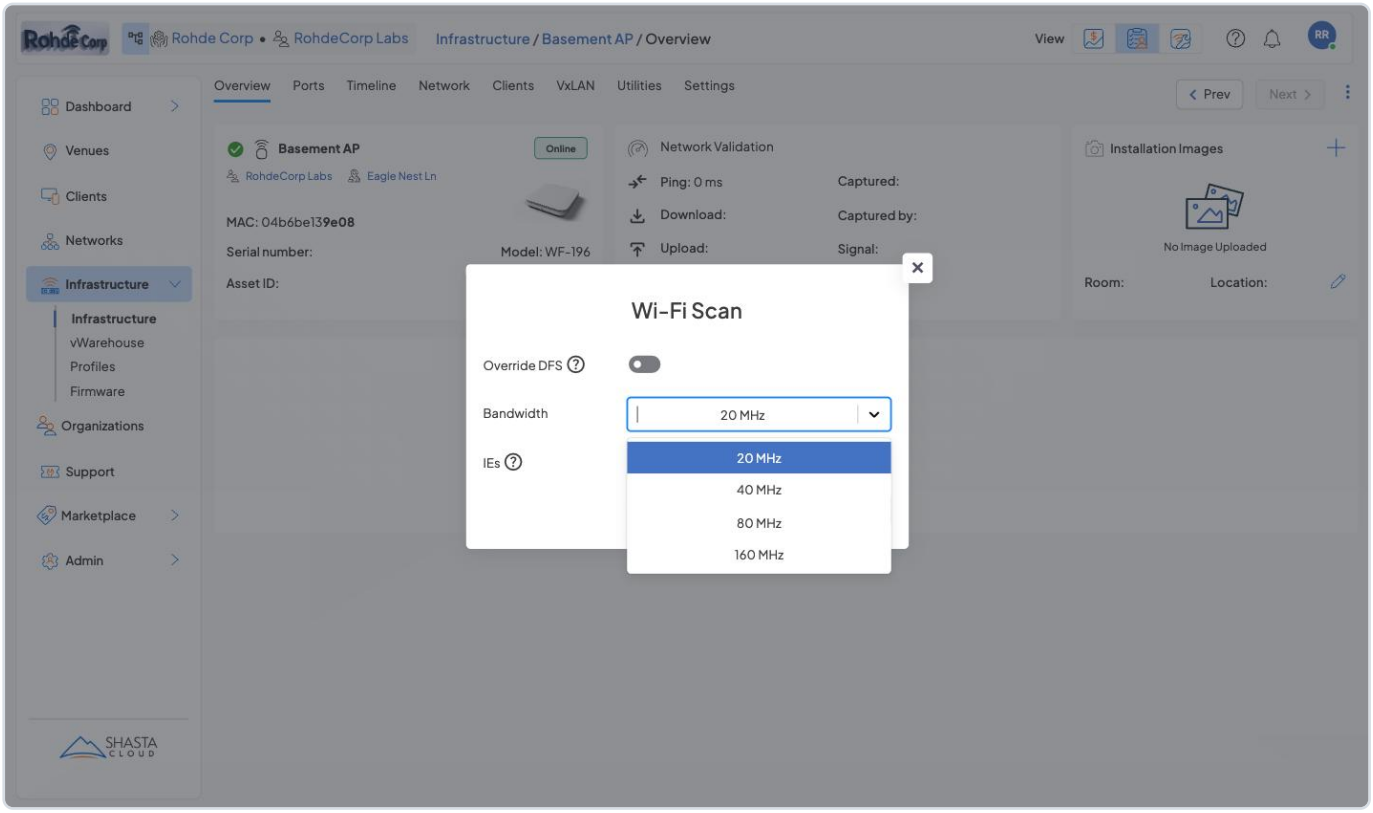


Figure 4 — The Bandwidth dropdown showing 20 MHz, 40 MHz, 80 MHz, and 160 MHz options.

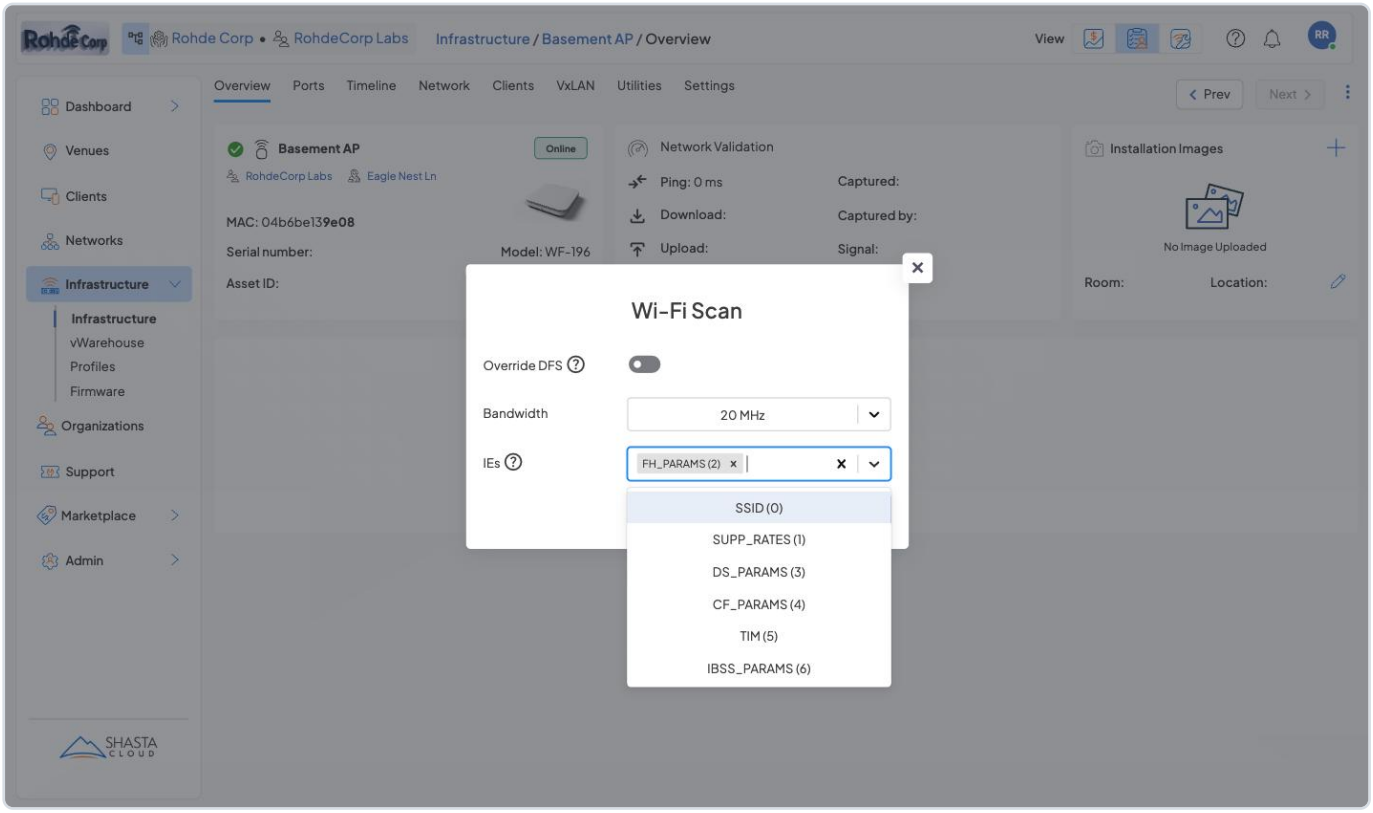


Figure 5 — The IEs multi-select dropdown exposing the full list of 802.11 Information Elements available to capture.

For most use cases, the defaults (**Override DFS:** OFF, **Bandwidth:** 20 MHz, **IEs:** FH_PARAMS) work well for a standard site survey. Click **Continue** to initiate the radio scan. A loading spinner appears on the button. The scan typically completes in 15–60 seconds.

Section 5 — Wi-Fi Scan — Reading Results

Once the scan completes, results are displayed in a table directly in the modal showing every wireless network detected by the AP's radio(s). The following screenshots show actual scan results captured from the **EAP-105** in the **Shasta MDU** venue. The AP detected 13 unique networks across channels 1 (2.4 GHz) and 44 (5 GHz):

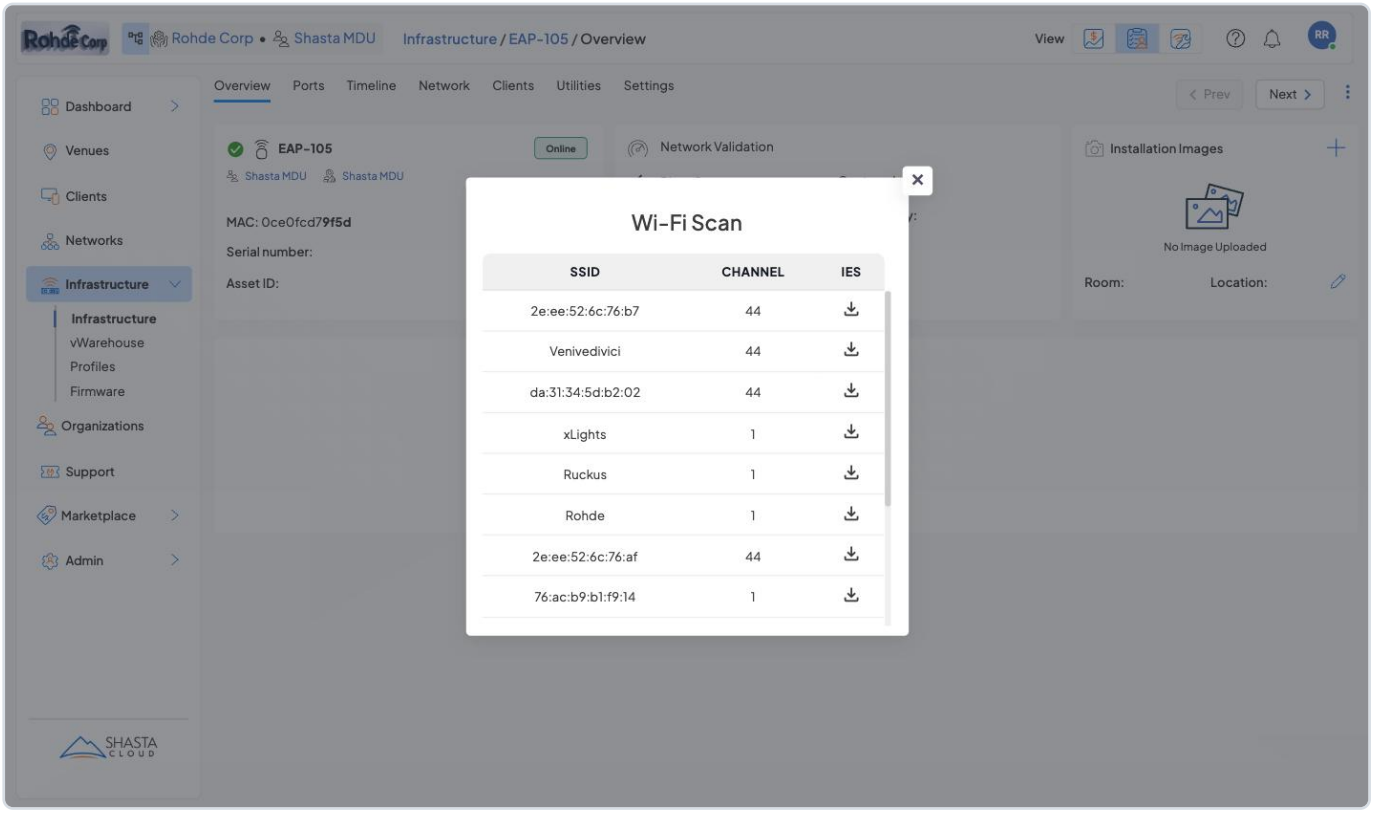


Figure 6 — Wi-Fi Scan results (top). Networks detected on channels 44 (5 GHz) and channel 1 (2.4 GHz), including Venivedivici, xLights, Ruckus, Rohde, and several MAC-only entries.

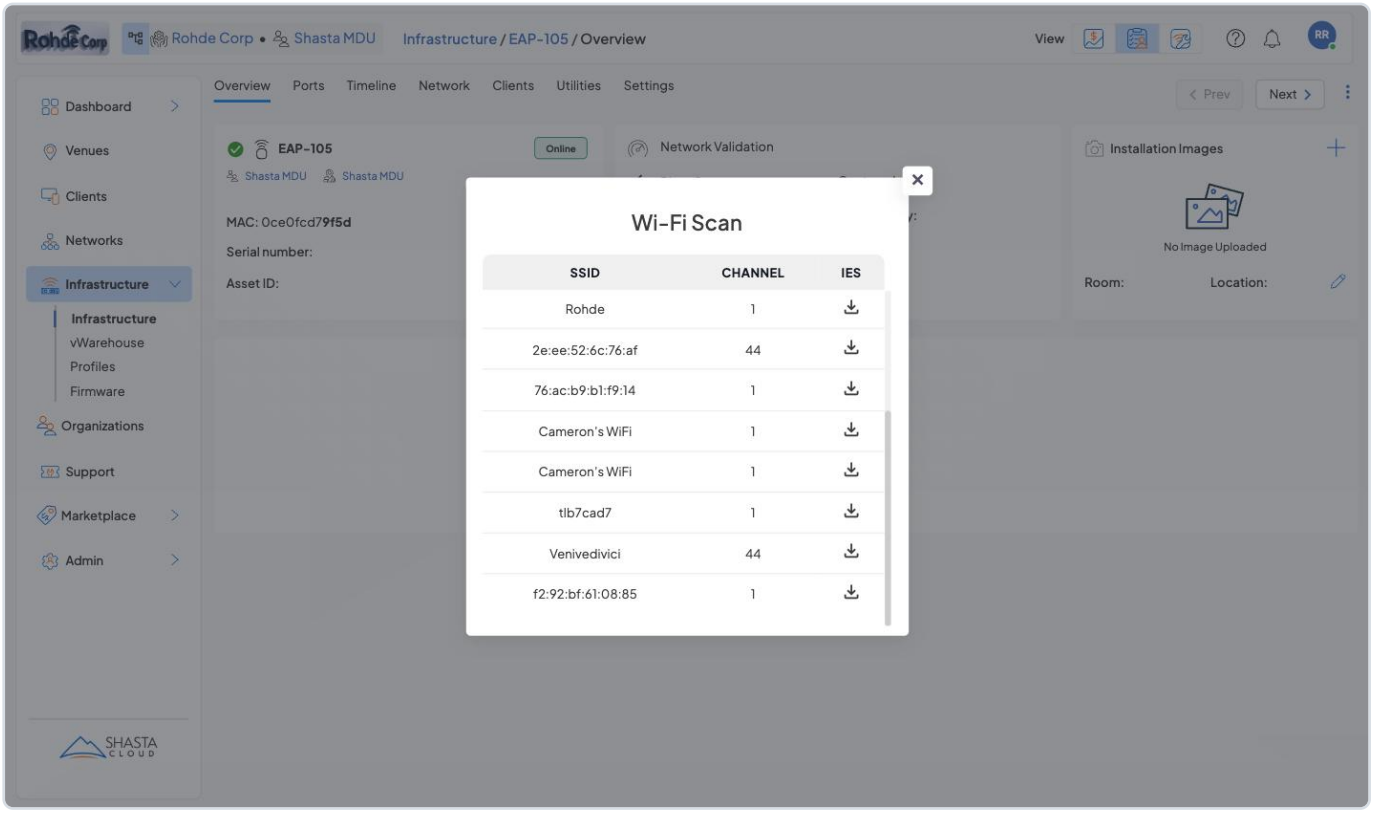


Figure 7 — Wi-Fi Scan results (continued). Additional networks including Cameron's WiFi (x2), tlb7cad7, and more co-channel detections on channels 1 and 44.

Understanding the Results Table

Column	Description
SSID	The network name (SSID) broadcast by the neighboring AP. Some entries show a MAC address instead of a name — this indicates a hidden network or a network that doesn't broadcast its SSID.
Channel	The Wi-Fi channel the neighboring AP is operating on. Channel 1 is in the 2.4 GHz band; Channel 44 is in the 5 GHz band.
IEs	A download icon (⇓) that lets you download the raw 802.11 Information Elements captured from that specific network's beacon frames.

Interpreting the Shasta MDU Scan Results

Observation	Interpretation
Multiple networks on Channel 1 (2.4 GHz)	High co-channel interference risk on 2.4 GHz Channel 1. Networks detected: *xLights*, *Ruckus*, *Rohde*, *Cameron's WiFi* (×2), *tlb7cad7*, and others. Consider moving the EAP-105 to Channel 6 or 11 to reduce overlap.
Multiple networks on Channel 44 (5 GHz)	Several 5 GHz networks co-located on Channel 44. This could indicate co-channel interference in the 5 GHz band as well.
Networks showing MAC instead of SSID	MAC-only entries (e.g., `2e:ee:52:6c:76:b7`) are hidden networks or probe responses that don't include an SSID IE in this scan. They are still physical devices transmitting on the channel.
Ruckus network visible	A competing vendor AP (Ruckus) is in range on Channel 1. Useful context for a mixed-vendor environment.

Download Individual IE Data: Click the download icon (⇓) next to any network to export the raw 802.11 Information Elements captured from that network's beacons. This provides detailed technical data including supported rates, capabilities, and vendor-specific elements for deeper analysis.

Section 6 — Utilities Tab Overview

The **Utilities** tab is accessible from the AP detail page tab bar. It provides an interface for running diagnostic commands directly from the AP — no CLI access required.

1. Navigate to the AP detail page (any online AP).
2. Click the **Utilities** tab. The Command selector and AP Output area will load.

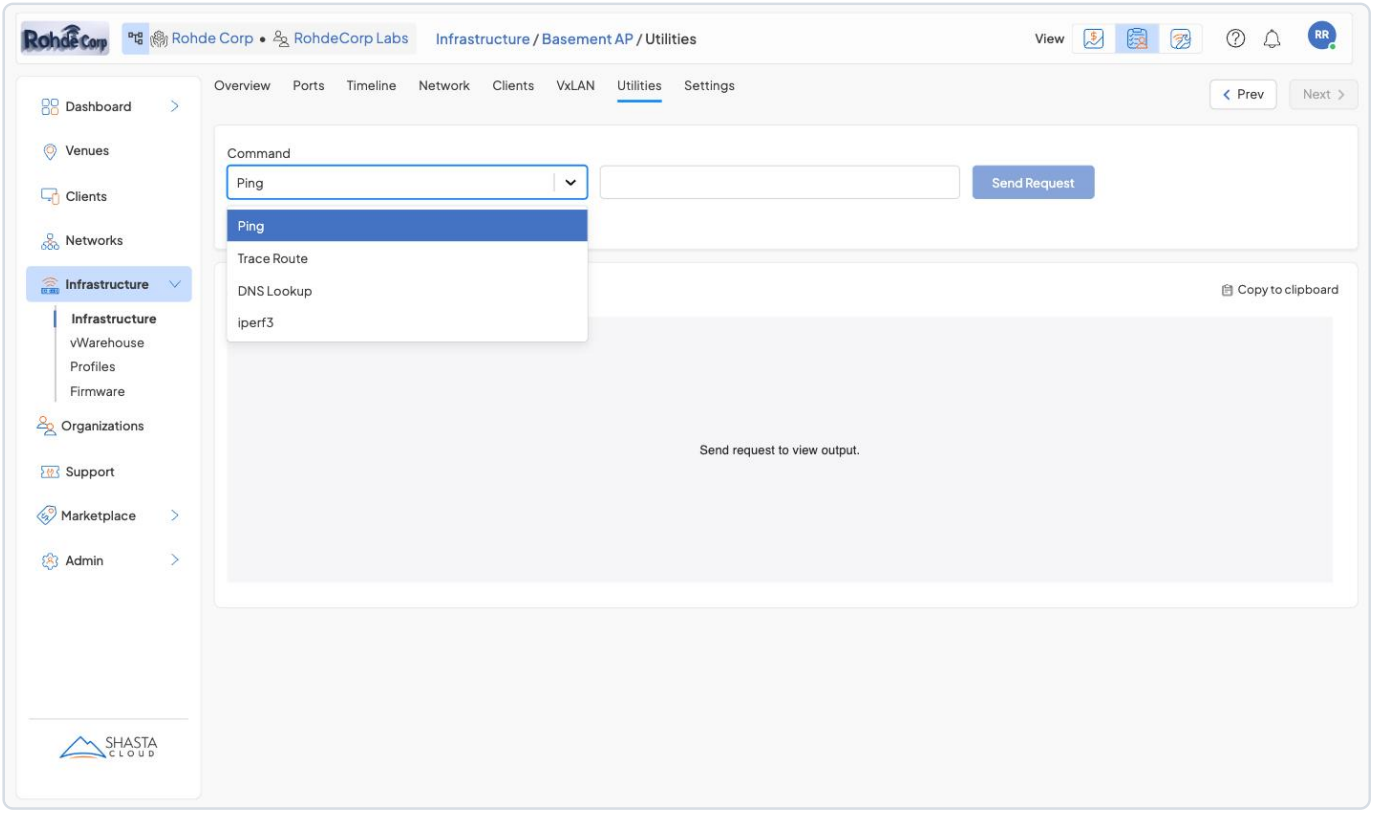


Figure 8 — The Utilities tab with the Command dropdown open, showing the four available commands: Ping, Trace Route, DNS Lookup, and iperf3.

Select a command, fill in the required parameters, click **Send Request** (or **Run Test** for iperf3), and results appear in the **AP Output** area. Use **Copy to Clipboard** to export output.

Section 7 — Ping

Sends ICMP echo requests from the AP to a target IP or hostname to verify connectivity and measure round-trip latency.

To run Ping: Select **Ping**, enter target IP/hostname (e.g., `8.8.8.8` or `google.com`), and click **Send Request**.

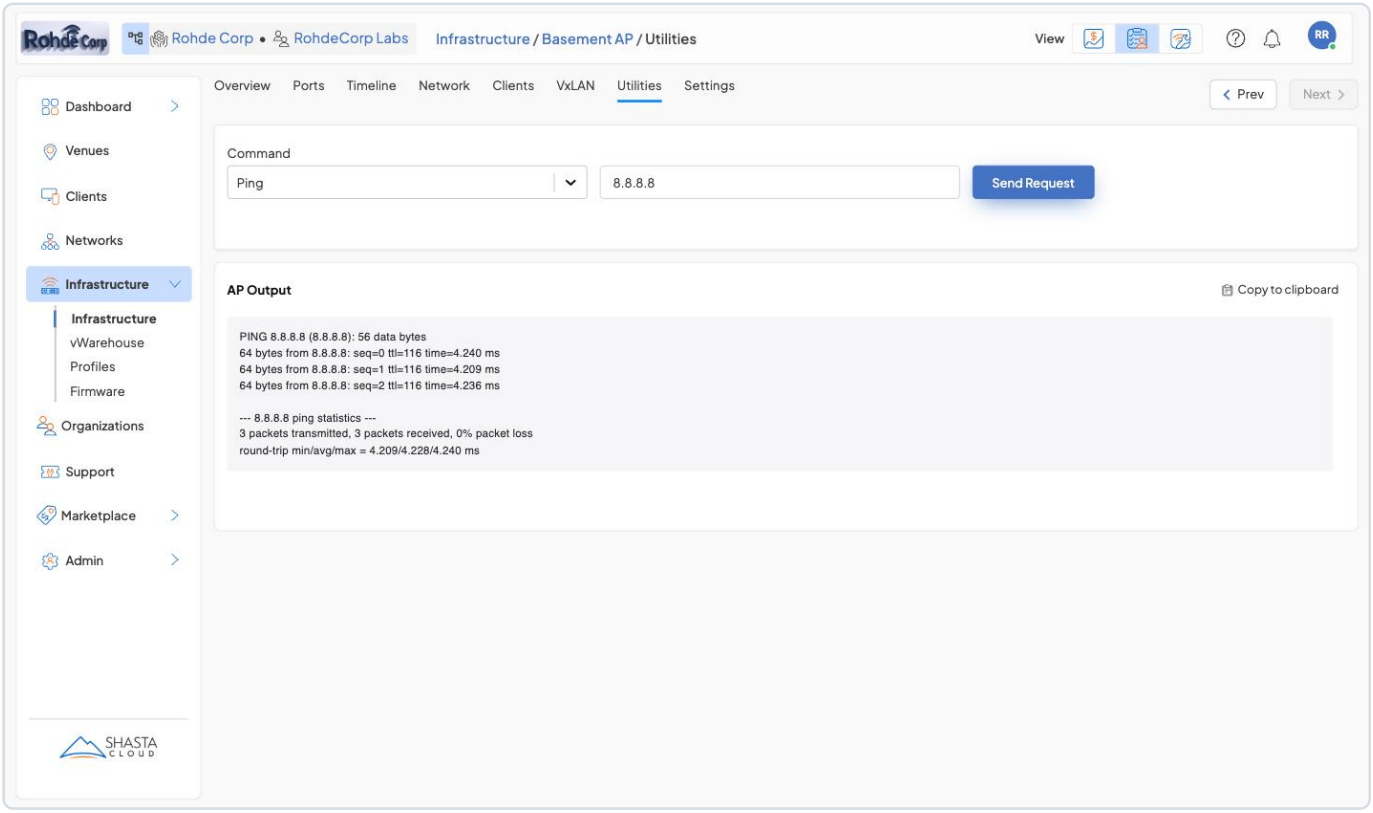


Figure 9 — Ping results from the AP to 8.8.8.8 showing 3 packets transmitted / 3 received, 0% packet loss, and round-trip latency statistics (min/avg/max ≈ 4.2 ms).

Output Field	Meaning
`time=N ms`	Round-trip latency per packet. Lower is better.
`0% packet loss`	All packets received — healthy connectivity.
`>0% packet loss`	Packets dropped — possible network instability or firewall blocking ICMP.
`round-trip min/avg/max`	Latency statistics across all 3 packets.

Section 8 — Trace Route

Maps the network path from the AP to a destination, showing each hop router and latency. Use it to identify where delays or failures occur along the route.

To run Trace Route: Select **Trace Route**, enter target, optionally enable **Reverse DNS Lookup**, and click **Send Request**. Reverse DNS Lookup resolves each hop's IP to a hostname for easier identification.

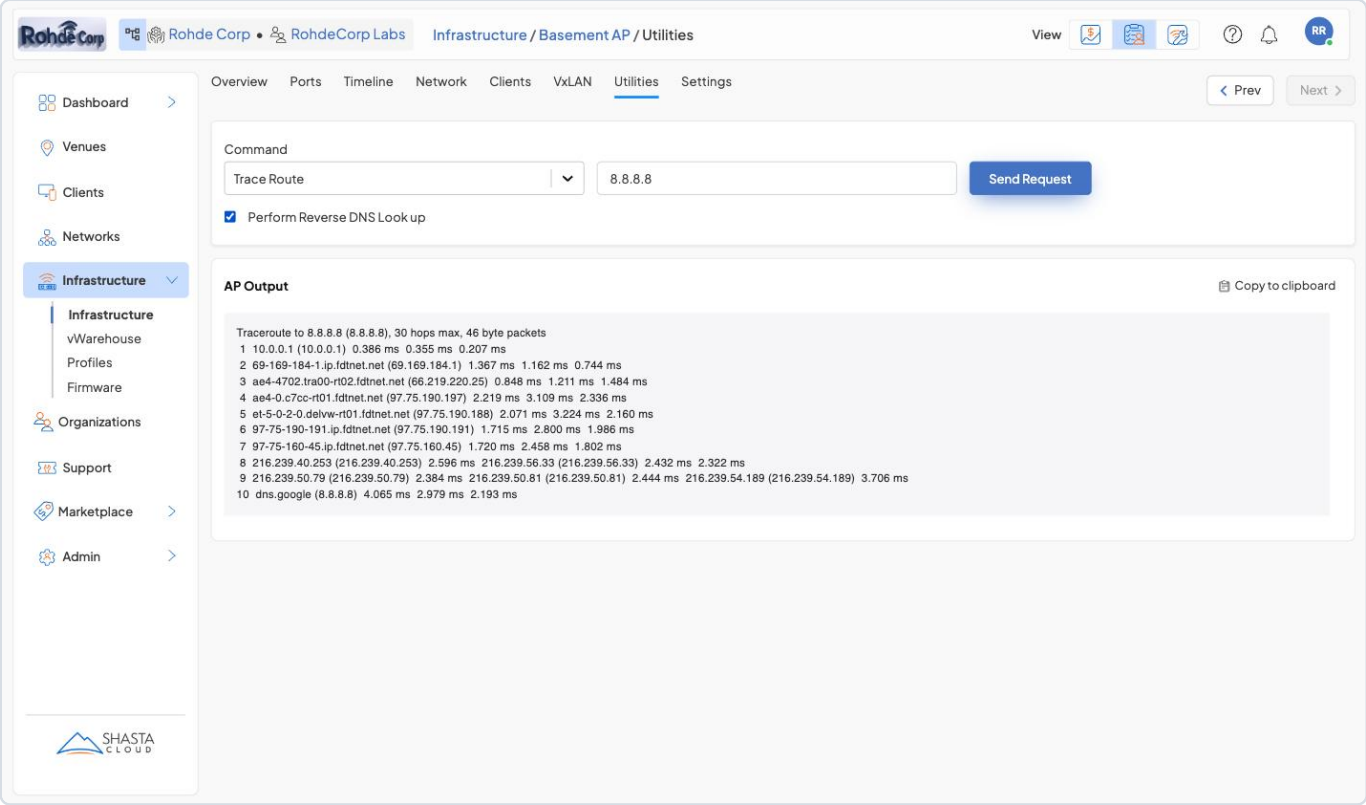


Figure 10 — Trace Route output showing each hop along the path from the AP to the destination, including resolved hostnames and per-hop latency measurements.

Output	Meaning
`N hostname (IP) Xms Xms Xms`	Hop number, resolved hostname, IP, and three latency measurements.
`* * *`	No response from this hop — router is not responding to traceroute (normal for many ISP routers).
Large latency jump at one hop	Possible slow link or congestion between that hop and the next.
Trace stops mid-path	Traffic is blocked or unreachable beyond that point.

Section 9 — DNS Lookup

Queries the AP's DNS server to resolve a hostname to its IP address(es). Use it to verify DNS is working from the AP's network perspective.

To run DNS Lookup: Select **DNS Lookup**, enter a hostname (e.g., `google.com`), and click **Send Request**. Results show the DNS server used and all resolved addresses (IPv4 and IPv6).

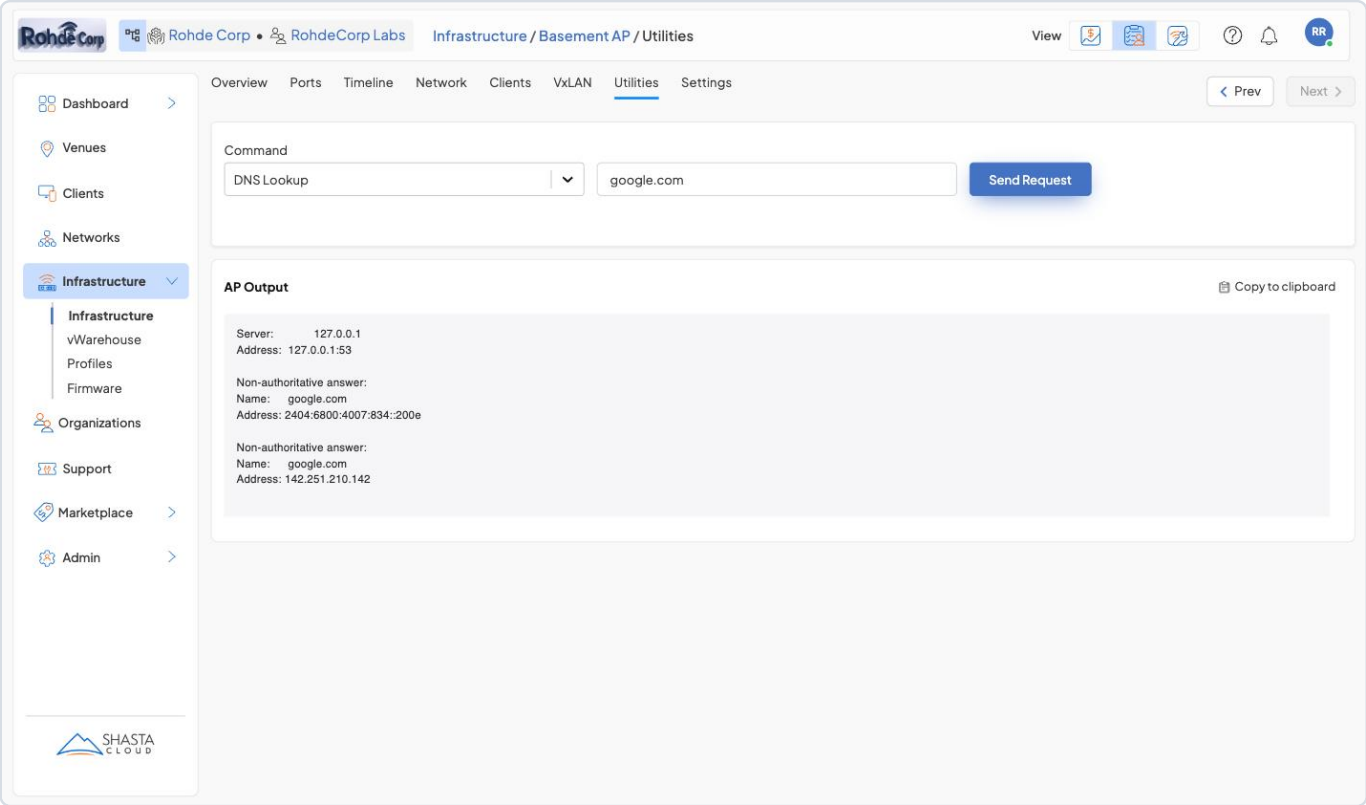


Figure 11 — DNS Lookup results showing the DNS server queried, a non-authoritative answer, and all resolved IP addresses (both IPv4 and IPv6 where available).

Output Field	Meaning
Server / Address	The DNS server IP and port (typically `:53`) the AP queried.
Non-authoritative answer	Response from a recursive/caching DNS server — normal for most lookups.
Address	

Output Field	Meaning
	The resolved IP address(es). Multiple entries = multiple DNS records (load balancing or IPv4 + IPv6).

Section 10 — iperf3 Throughput Test

Runs a bandwidth test between the AP and an iperf3 server. Requires a running iperf3 server reachable from the AP.

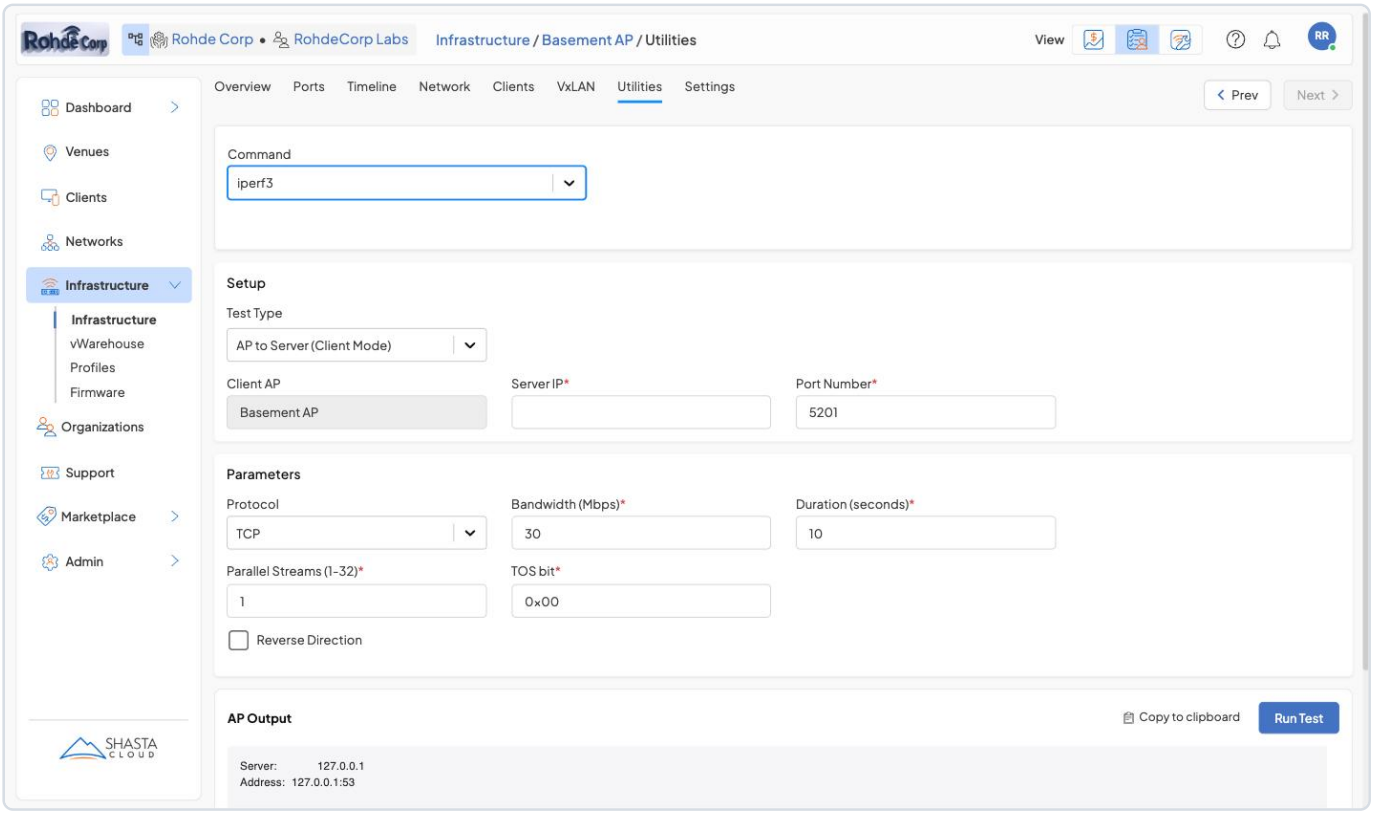


Figure 12 — The iperf3 setup panel with fields for Test Type, Server IP, Port Number, Protocol, Bandwidth, Duration, Parallel Streams, and Reverse Direction.

Configuration Fields

Field	Default	Description
Test Type		

Field	Default	Description
	AP to Server	**AP to Server** (Client Mode): AP sends traffic to server — measures upload. **Server to AP** (Server Mode): AP listens — measures download. **AP to AP**: between two Shasta-managed APs.
Server IP	—	IP address of the iperf3 server.
Port Number	`5201`	Port the iperf3 server is listening on.
Protocol	TCP	TCP for realistic throughput. UDP for fixed-rate testing with packet loss/jitter metrics.
Bandwidth (Mbps)	`30`	Target bandwidth. For TCP this is a guideline; for UDP this is the exact send rate.
Duration (seconds)	`10`	How long to run the test. 30–60 seconds gives more stable averages.
Parallel Streams	`1`	Number of simultaneous streams. Increase to 4–8 for high-bandwidth link testing.
Reverse Direction	`Off`	Reverses traffic flow — server sends to AP instead. Tests download in Client Mode.

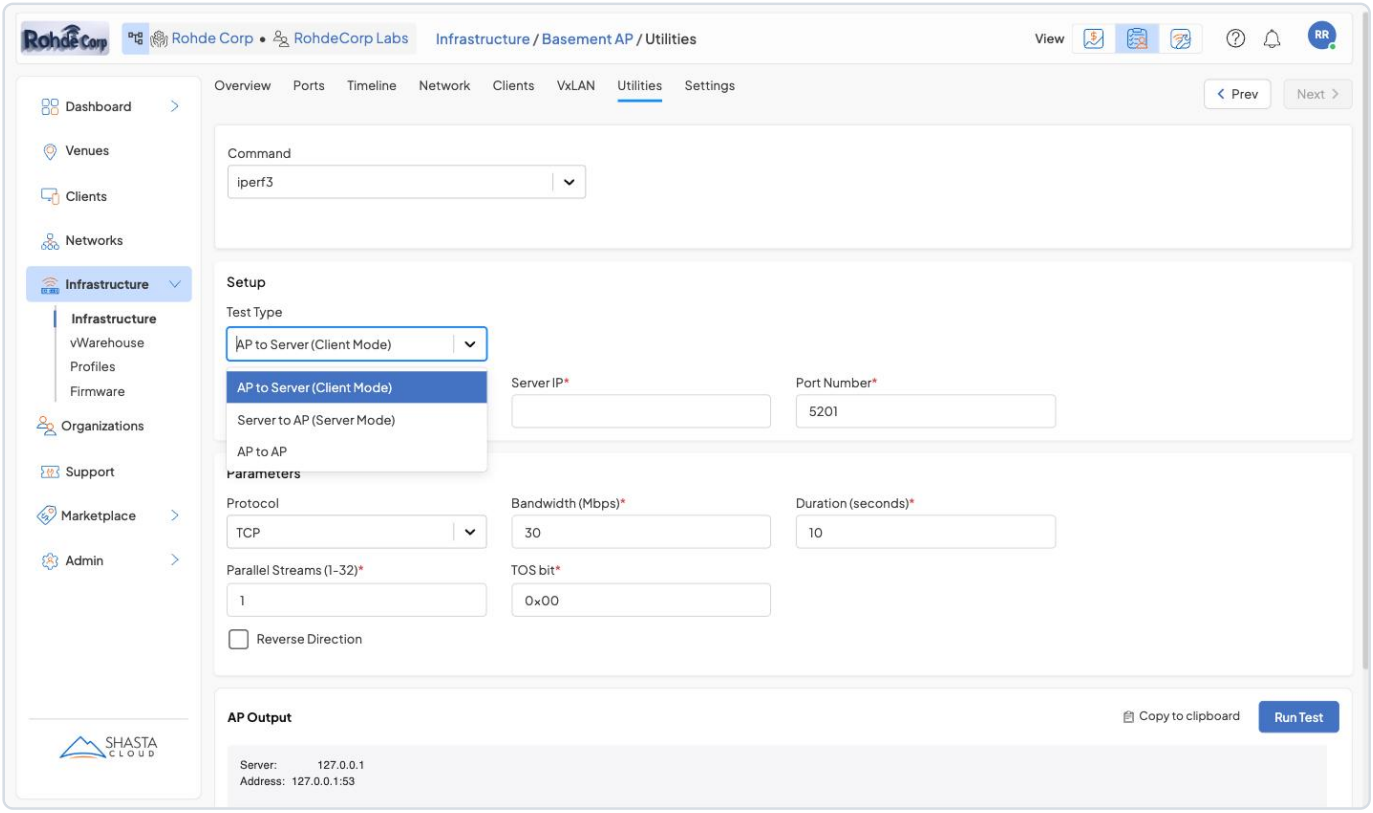


Figure 13 — The Test Type dropdown with AP to Server, Server to AP, and AP to AP options.

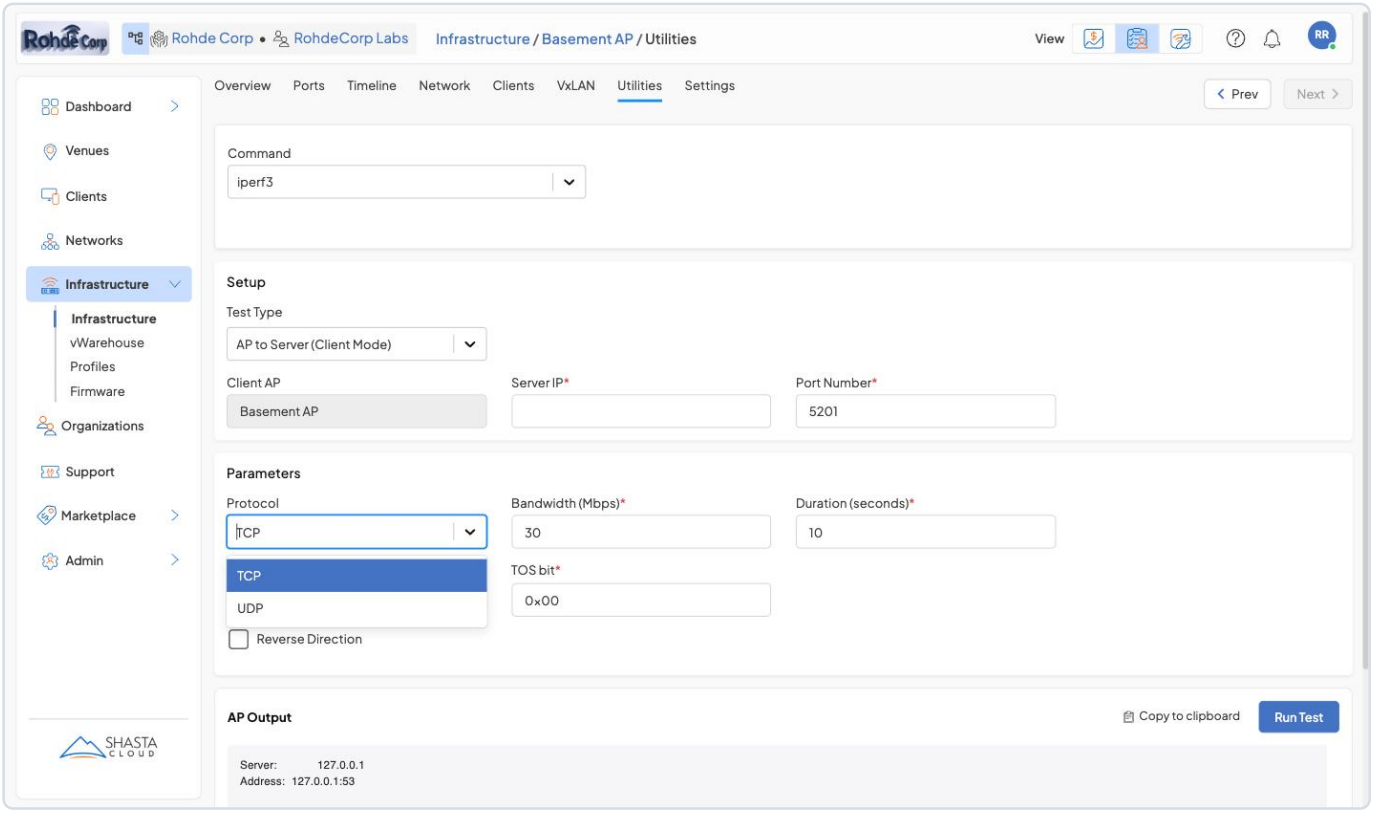


Figure 14 — The Protocol dropdown showing TCP and UDP options.

Section 11 — Quick Reference

Tool	Access Path	Input	Best For
Wi-Fi Scan	AP Overview → ⋮ → Wi-Fi Scan	Bandwidth, DFS, IEs	Site survey, channel planning, interference detection
Ping	Utilities → Ping	IP or hostname	Connectivity check, latency measurement
Trace Route	Utilities → Trace Route	IP or hostname	Path analysis, routing troubleshooting
DNS Lookup	Utilities → DNS Lookup	Hostname	DNS resolution verification

Tool	Access Path	Input	Best For
iperf3	Utilities → iperf3	Server IP, protocol, etc.	Bandwidth testing, QoS validation

For further assistance, contact Shasta Cloud Support by creating a support ticket from the **Support** section of the platform.