ClearPath MSP
ClearWatch

SOLUTION BRIEF

from ClearPath MSP®

CLEARWATCH SOLUTION BRIEF · TP-LINK OMADA

Every Omada site, read through its controller.

How ClearWatch reads an Omada controller and every gateway, switch and access point it manages, and what it checks.

PUBLISHED NOVEMBER 2026 LENGTH 6 PAGES APPLIES TO OMADA HARDWARE AND SOFTWARE CONTROLLERS

EXECUTIVE SUMMARY

Your Omada network, beside everything else you watch

An Omada network is run from its controller. The gateway, switches and access points report there, and somebody has to sign in to that console to notice a circuit that dropped, a switch nearly out of PoE power or a 2.4 GHz band too busy to use. Across several sites and several clients, that is a lot of consoles nobody is looking at.

ClearWatch reads each Omada controller through its Open API, with a read-only Viewer client, from a ClearBridge on the controller's own network. About every ten minutes it brings in every gateway, switch and access point as a ClearWatch device, judges them with built-in checks, and puts them on the same dashboards, maps and alerts as everything else.

KEY TAKEAWAYS

- **Read only, by design:** a Viewer client is refused every change, so ClearWatch cannot alter the network.
- **Each device is a ClearWatch device,** with its own checks, load history and a ping.
- **Internet, PoE, airtime, load and firmware** are judged by built-in checks with sensible defaults.
- **One console for every site and client:** a wireless score, the topology map and the controller's own log.

IN THIS BRIEF

01 **The challenge** — What the controller leaves to you — 2
02 **How ClearWatch connects** — Open API, sites and import — 2
03 **What ClearWatch reads** — Internet, ports, every device — 4
04 **Across every site** — Wireless experience, the log and the map — 5
05 **Checks and alerts** — Built-in checks and defaults — 6
06 **Good to know** — Requirements and limits — 6

WHO THIS IS FOR

MSPs and IT teams running TP-Link Omada networks, at one site or many, for their own organization or across many clients.

AT A GLANCE

ACCESS
Viewer, read only
An Open API client in Client Credentials mode.

SCANS
About every 10 min
Sites, devices, ports, internet, radios and clients.

CHECKS
8 built in
Internet, load, PoE, airtime, firmware and the controller.

DEVICES
Each its own
Gateways, switches and access points, each pinged too.

01 THE CHALLENGE

The controller knows. Somebody has to be looking.

The Omada controller sees every device it has adopted, and its own dashboards are good. But it is one console per controller, often one per site, apart from everything else you watch. A circuit that dropped overnight, a switch close to its PoE budget or an access point whose 2.4 GHz band is full shows up there, and only to somebody who thought to look.

THE QUESTION	THE OMADA CONTROLLER ALONE	CLEARWATCH
Is every site on the internet?	Visible to whoever opens that controller	Each gateway's WANs read every scan: one down **warns**, none up **fails**
Is anything running out?	A dashboard to check, one controller at a time	PoE budget, processor and memory judged against levels, with **90 days** of load history
Why does the Wi-Fi feel slow?	Radio pages, one access point at a time	Airtime **per band**, and one wireless experience score across sites
Are we behind on firmware?	Shown per device in the controller	A warning on each device while the controller lists a **newer release**
Is the controller itself well?	Its own alert log, if somebody reads it	Its log **mirrored** beside it, Error-level alerts counted daily, and the controller pinged

Airtime, not signal

An access point can show every client at full signal and still feel slow, because Wi-Fi is one shared medium: when a band is busy, other people's networks included, every client waits its turn and retries. ClearWatch reads airtime per band from the controller and warns at **70%** held for three scans in a row, so a full 2.4 GHz band shows up before the support call does.

02 HOW CLEARWATCH CONNECTS

Read through the Open API, from inside your network

A ClearBridge (the ClearWatch agent on a machine at the site) signs in to the controller's Open API with a client you create, and reads it about every ten minutes. Nothing is installed on the controller or on the devices it manages, and nothing is opened to the internet.

YOUR NETWORK

Omada controller

An OC200, OC300 or OC400, or the Software Controller, with an Open API client in the Viewer role.

→

YOUR NETWORK

ClearBridge

Signs in with the client's ID and secret over HTTPS, reads, and pings each imported device itself.

→

CLEARWATCH

Devices, checks, dashboards

Turns each scan into devices, checks and alerts, the Access points dashboard and the topology map.

02 HOW CLEARWATCH CONNECTS, CONTINUED

A client ID, a secret and a ClearBridge

In the controller, create an Open API client under Global, Settings, Platform Integration, in Client Credentials mode with the Viewer role. In ClearWatch, **Add controller** asks for the controller's address and the ClearBridge that can reach it 1 , then the client's ID and secret 2 , which are sealed in ClearWatch's credential vault.

The port sits under Advanced 3 : an OC200, OC300 or OC400 answers on 443 and the Software Controller on 8043. Pressing Add starts the first scan straight away.

What you provide

- ✓ An Open API client in the Viewer role.
- ✓ A ClearBridge that can reach the controller.
- ✓ A location for each Omada site, before its devices are imported.

What it never does

- ✗ Change a setting, reboot a device or push firmware: a Viewer client is refused every write.
- ✗ Turn SNMP on at a site. It uses SNMP only where a site already has it on.
- ✗ Import a device nobody chose.

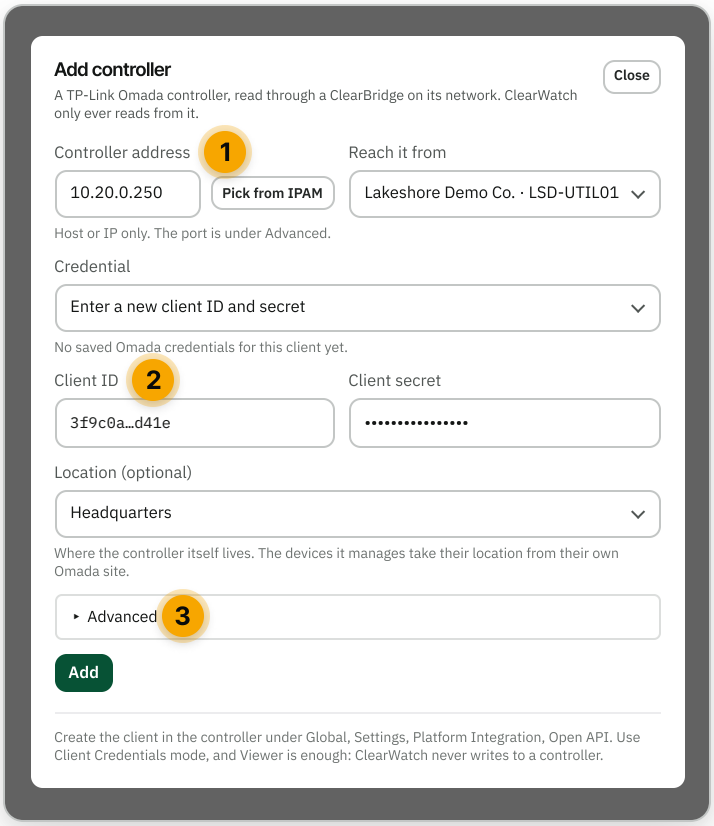


FIGURE 1 Add controller, rebuilt from the ClearWatch console with demo data.

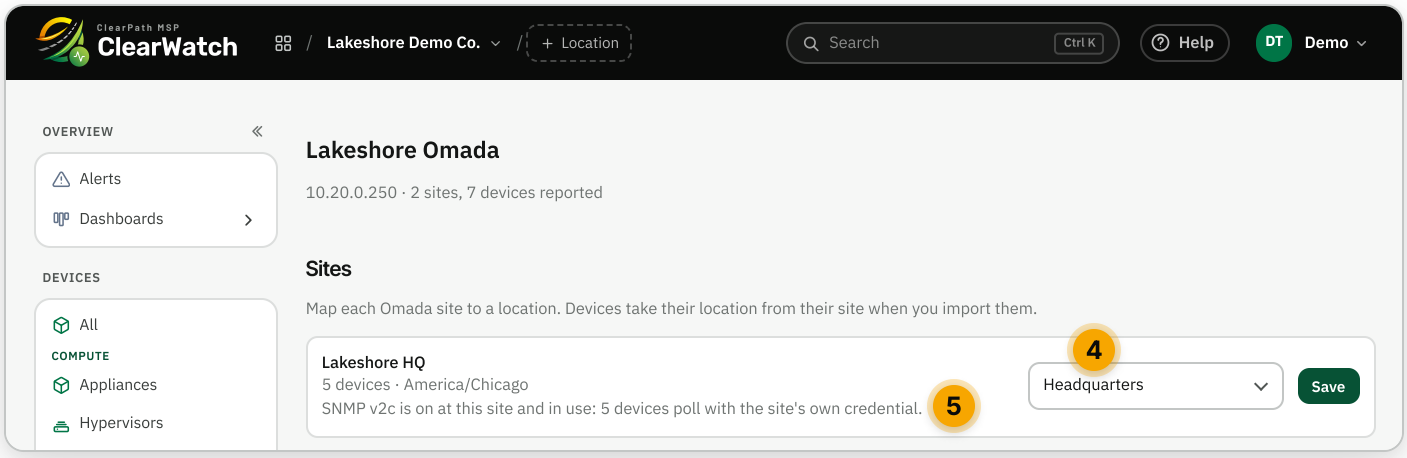


FIGURE 2 A controller's page under Manage, Integrations: each Omada site mapped to a location.

Each Omada site is mapped once to a ClearWatch location 4 , and every device in it takes that location when it is imported. Where a site already has SNMP on, ClearWatch copies its credential and the site's devices poll with it as well; where SNMP is off, the page says so and leaves it off 5 .

Below the sites, the controller's gateways, switches and access points are listed, and you choose which to import. Each becomes a ClearWatch device (a gateway is filed as a firewall), takes one license, and gets a **Ping** check from the ClearBridge, so it is watched directly as well as through the controller.

03 WHAT CLEARWATCH READS

Every gateway, switch and access point, in the controller's words

An imported device's page shows what its controller last said and when, beside the checks that judge it. Where the controller reported nothing on a subject, the page draws nothing rather than an empty table.

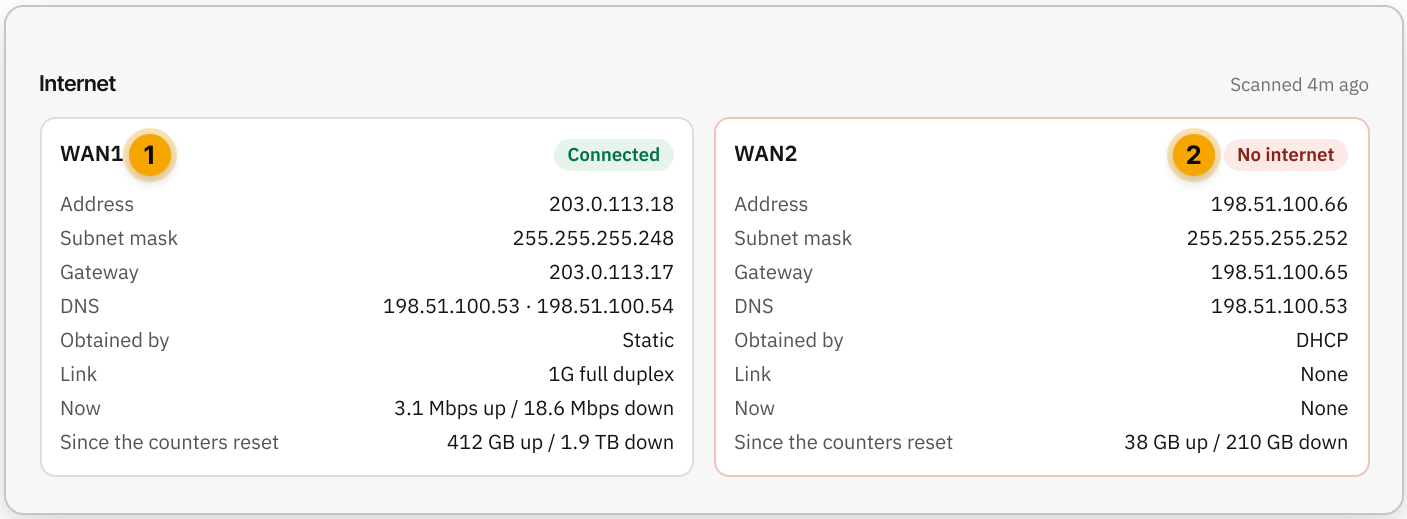


FIGURE 3 The Internet panel at the top of a gateway's Overview.

The internet connection

A gateway's page opens on its Internet panel: a card per WAN with its address, gateway, DNS, how the address was obtained and the link (1). A WAN without internet is outlined in red (2). A state the controller reports that ClearWatch does not recognize is shown as Unknown with the controller's own code, never guessed as up or down.

A WAN you set aside on the Ports tab as not in use is listed but not judged, so a spare port does not raise an alert.

Ports and cables

Switches and gateways get a picture of the box with each port's link, speed and PoE, and the device plugged into it. Access points get their wired uplink. Each port opens a card with its facts.

As the controller sees it

Under the ports sits the controller's view of the device: processor, memory and temperature, PoE drawn against the switch's own budget, and the running firmware, with an update chip when the controller lists a newer release (3).

Below it come the tables the controller keeps for that kind of device: LLDP neighbors (4), the routing table and VLAN interfaces for a switch, DHCP leases for a gateway, and each radio's channel, width, power and airtime for an access point.

The same figures fill the CPU and memory columns of the device lists, and the device header says whose number it is and how old: *from the controller 3 minutes ago*.

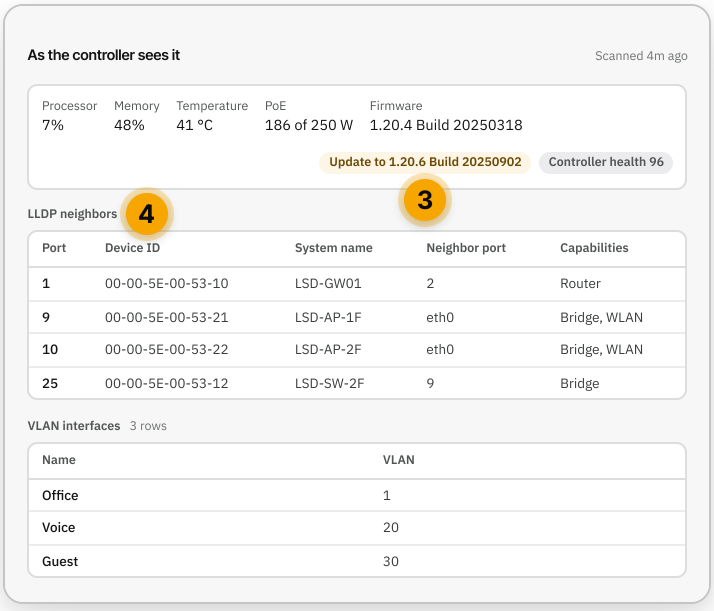


FIGURE 4 A switch's Ports tab: the controller's own view of the core switch.

04 ACROSS EVERY SITE

Every access point, every site, one wireless score

The same scans feed the console's dashboards and maps, so an Omada site sits beside every other client's network instead of in a console of its own.

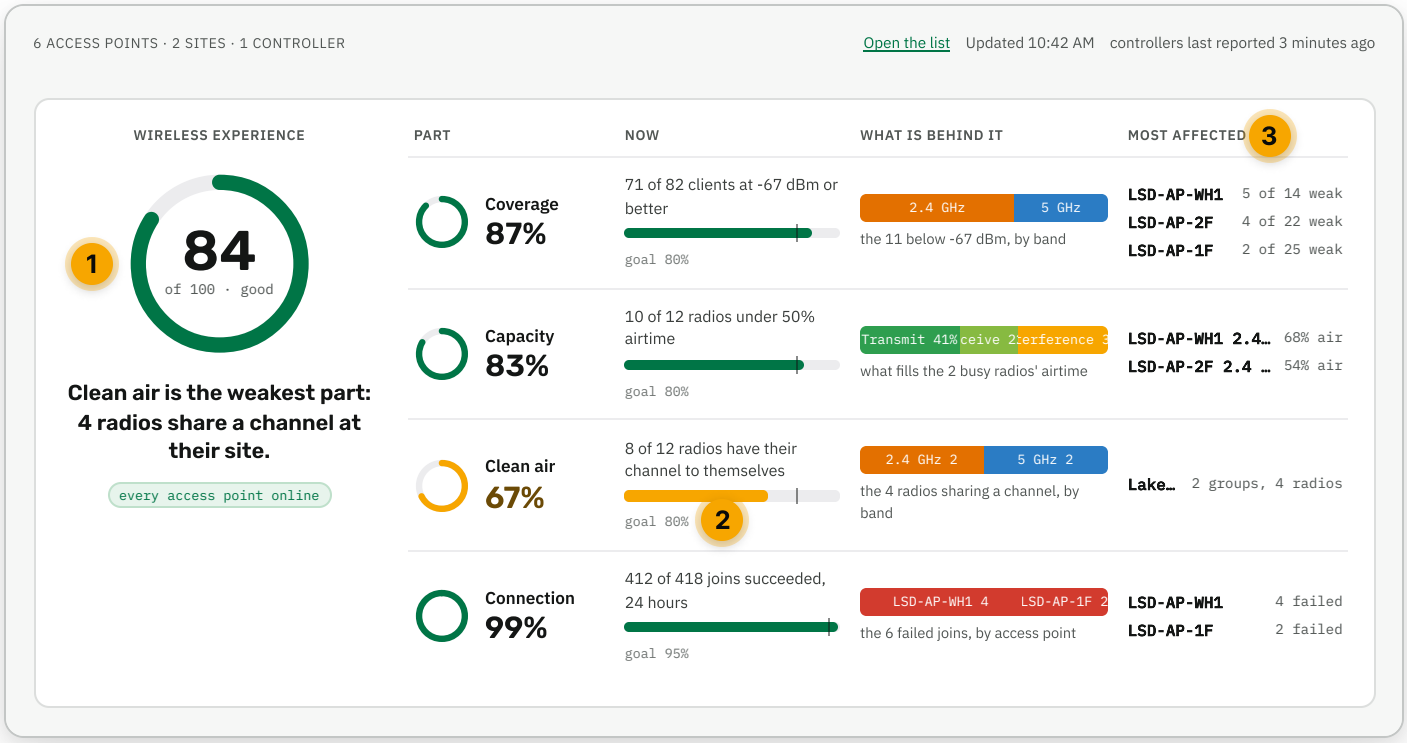


FIGURE 5 The Access points dashboard's wireless experience, across one client's two Omada sites.

The **Access points** dashboard scores the wireless experience across every controller in view 1 , as the average of four parts: Coverage (clients at -67 dBm or better), Capacity (radios under 50% airtime), Clean air (radios with their channel to themselves) and Connection (joins that succeeded, from the controller's log). Each is drawn against its goal 2 with the access points or sites it affects most 3 . Below come signal by band, struggling clients, a day of clients and a tile per access point, grouped by site.

The controller's own log

Each controller's alerts and events, kept 30 days, sit on its page beside the clients it reports, so nobody signs in to a second console to read them. The log is shown as the controller wrote it; what raises an alert is the daily count of Error-level entries 4 .

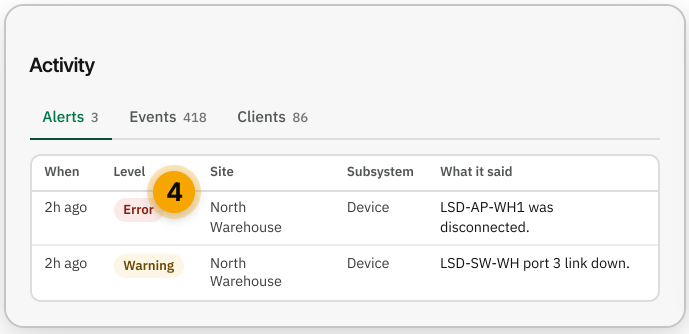


FIGURE 6 Activity on a controller's page. The log lines are made up.

On the topology map

Every cable the controller knows, from switch ports and each access point's uplink, is drawn on the location's topology map, matched to its far end by MAC. Cable thickness follows how busy the port is.

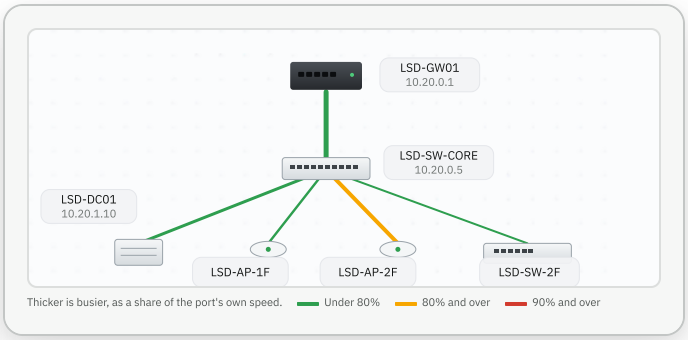


FIGURE 7 Headquarters on the topology map. The artwork is simplified.

05 CHECKS AND ALERTS

Eight checks and a ping for every Omada network

Every level is a default you can change for everyone or for one device. The internet connection and the controller's alerts are watched from the start; the switch, access point and gateway templates are switched on when you are ready.

CHECK	APPLIES TO	WARNING	FAILED
Internet connection	Gateways	One WAN of several has no internet	No WAN has internet
WAN ports without internet	Gateways	1	2
Processor (%), from the controller	Every device	80%, held three scans	95%, held three scans
Memory used (%), from the controller	Every device	85%	95%
PoE budget used (%)	Switches	80%	90%
Wireless airtime busy (%)	Access points, per band	70%, held three scans	80%, held three scans
Firmware update available	Every device	While a newer release is listed	Never fails
Controller alerts (last day)	The controller	1 Error-level alert	5 Error-level alerts

Every imported device and the controller itself also carry a **Ping** check from the ClearBridge, so a device that stops answering is caught even while the controller is down. A device the controller calls disconnected is not judged on figures it sent before it went.

Load, kept for 90 days

Each scan's processor and memory reading is kept for 90 days and drawn on the device's Overview, the processor as average and peak, beside any SNMP graphs 1 . Alerts follow your notification policies like any other check.

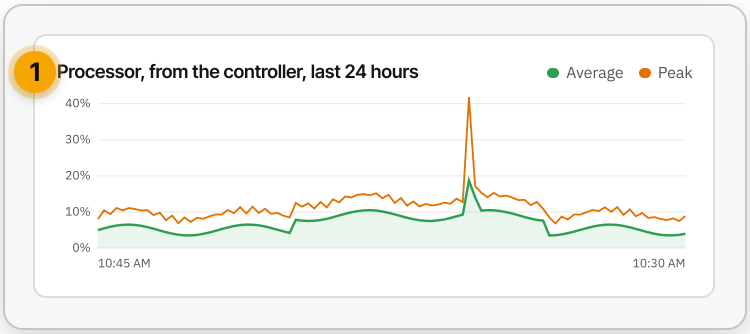


FIGURE 8 A switch's processor over a day, from the controller's readings.

06 GOOD TO KNOW

Requirements

- An Omada Hardware Controller (OC200, OC300 or OC400) or the Omada Software Controller, reachable from a ClearBridge.
- An Open API client in Client Credentials mode with the Viewer role.
- One license for the controller and one for each device imported.

Limits

- Readings come through the controller: while it is down, only the Ping checks report.
- The Open API gives no fan or power supply state, and no processor or memory figure for the controller itself.
- The Omada Cloud-Based Controller is not read; the controller must be on your network.

See every Omada site on one console.
Start a free trial, or ask us to add your first controller with you.
clearwatch.com

ClearWatch™ is a trademark of ClearPath MSP. TP-Link and Omada are trademarks of TP-Link. Screens show demo data.