SMARTTILE · DEVICEAUTOMATE™ · UBIQUITI UNIFI NETWORK

UniFi Network, watched from the console out

Connect a UniFi console once and every gateway, switch and access point on its mapped sites is imported, checked every 60 seconds, reported DOWN when the controller stops listing it, and ticketed in the IT Service Management (ITSM) system your team already uses.

SMARTTILE INTEGRATES WITH

Ubiquiti UniFi Network — UniFi OS consoles and self-hosted controllers — through the Network Integration API (API key), the classic controller API (login or the same key), UniFi Site Manager at api.ui.com, or the Site Manager cloud connector (no VPN).

HOW SMARTTILE AUTOMATES IT

SmartTile mirrors each mapped site's devices, imports the ones you tick, marks a device DOWN when the controller reports it offline or stops listing it (reboots counted from the boot counter), and opens one ticket per location after about 6 minutes — closing Rev.io tickets once every device is stably back.

CATEGORY

Device
DeviceAutomate™

UniFi's own dashboards tell a site what is wrong; they do not open a ticket, and they do not tell your NOC. SmartTile reads the console the way the UniFi app does — sites, devices, boot counters, ports, radios and WAN health — and holds itself to one rule: **a device counts as present only when the controller lists it in this poll.** An AP that drops off the list, a gateway whose controller stops answering, an AP that reboots between two checks — each is recorded as an outage, counted in availability, and ticketed.

What the connection turns on

Site-by-site mapping

Each UniFi site is mapped to a SmartTile location. A multi-site cloud console's devices are attributed to sites by a person on the **Map** screen — never guessed.

Choose, then import

Import preview labels every unit *new*, *imported* or *offline*. You tick what comes in; offline gear is never imported and a unit already in through another connection is matched by MAC, not duplicated.

DOWN from the truth

Offline in the controller, or missing from its list for 5 minutes, is DOWN. The statistics heartbeat is kept separate, so a stale stats reply can never keep a dead AP green.

Reboots and blind controllers

A boot counter going backwards is a reboot, recorded DOWN→UP with its real duration; 3 in 60 minutes opens a ticket. A controller that stops answering turns its devices UNKNOWN (grey) — a self-hosting gateway goes DOWN.

Full console telemetry

With a Controller API key: WAN latency and loss per monitor target, ISP and speed test, every switch port (link, PoE, errors, LLDP), every radio and SSID, temperature, storage, site health — 35 days of history.

Clients and top talkers

Per-AP client lists and an API NetFlow view of LAN top talkers (and application mix where the controller runs DPI), plus bandwidth and uptime charts on the device.

Replaced hardware

When a site swaps an AP, switch or gateway, **Map → Replaced hardware** hands the existing SmartTile device to the new unit: same id, name, contacts, ticket rules and history. A person confirms every swap; each is logged.

Performance thresholds

WAN loss, WAN latency, overheating, port errors and half-duplex links can alert and ticket once sustained; Wi-Fi experience, channel utilisation, PoE headroom and end-of-life are advisories. **Off by default.**

How it goes live

1. **Create the key.** On the console: UniFi Network → **Settings** → **Control Plane** → **Integrations** → **Create API Key** (Network 9 or newer). Cloud route instead: **unifi.ui.com** → **your profile** → **API** → **Create API Key**.
2. **Add the connection.** DeviceAutomate → **UniFi Controllers** → Add: pick the auth mode, the controller URL (or console id for the cloud connector) and paste the key. A customer admin can use **Connect My Network** instead.
3. **Test.** A failure names the fix — key rejected, which SmartTile address to allow on HTTPS, or a wrong console id.
4. **Map → Sync → Import.** Map each site to a location, Sync, tick the devices and click *Import selected*.

CONNECTION	WHAT WORKS
Controller API key *(recommended)*	Status, reboots, CPU / memory, clients, uplink throughput, plus full console telemetry and thresholds through the same key.
Classic controller login	Everything the classic API gives, including controller report history for bandwidth and uptime charts.
Site Manager API key	Device list and status, reboots, firmware waiting, site client counts, console ISP metrics. No per-port or per-radio detail.
Cloud connector	The Integration API reached through api.ui.com with the Site Manager key — no VPN or port-forward.

When a UniFi device goes down

Confirmed before it tickets

A device must be offline for 3 consecutive checks (about 6 minutes) before a ticket opens. If half the fleet drops at once, that is a reporting gap — statuses update, tickets hold.

One ticket per location

Tickets go through the normal SmartTile path: the device's auto-ticket flag, the location's automation switch and per-location dedup — so every AP behind one dead uplink is one ticket with notes. Rev.io plus any other ITSM system connected for the company.

Honest uptime, closed on recovery

Every DOWN, UP and reboot is written to state history, so availability and reports count it. A Rev.io ticket is closed once every device on it is confirmed up for 10 minutes; a long outage stays open for the RFO.

Exactly what SmartTile asks UniFi

GET	`/proxy/network/integration/v1/sites`	sites (Integration API, API key)
GET	`…/sites/{id}/devices/{id}/statistics/latest`	uptime, CPU, memory, clients, uplink
GET	`/proxy/network/api/s/{site}/stat/health`	site WAN / WLAN / LAN / VPN health
POST	`/api/s/{site}/stat/report/{interval}.{scope}`	history charts — classic login only (a read)
GET	`api.ui.com /v1/isp-metrics/{type}`	console WAN latency and loss
GET	`…/integration/v1/sites/{id}/devices`	device list and online state
GET	`/proxy/network/api/s/{site}/stat/device`	full device detail: ports, radios, temperature
GET	`/api/s/{site}/stat/sta`	clients and top talkers
GET	`api.ui.com /v1/hosts · /v1/sites · /v1/devices`	Site Manager fleet list
GET	`api.ui.com /v1/connector/consoles/{id}/network/…`	cloud connector, no VPN

Security and control

Reads only

Every call above reads. SmartTile adopts, configures and upgrades nothing on the console.

Keys stay in the vault

API keys and passwords are encrypted at rest (AES-256-GCM) and never returned — the form only shows that one is set; leave it blank to keep it.

Your company only

A customer admin sees and maps only the controllers their company owns; another tenant's controller id answers *not found*.

Switches you control

The integration, uptime history, ticket confirmation, down and reboot detection, full telemetry and hardware replace each have their own setting. Every replace is in the transaction log.

Common objections

OBJECTION	ANSWER
“UniFi already alerts us.”	UniFi e-mails a person. SmartTile records the outage, counts reboots in availability and opens the ticket in your ITSM system — one per site, not one per AP.
“A controller hiccup will flood us with tickets.”	Three checks in a row before a ticket, a fleet-share hold, and a blind controller turns devices grey (UNKNOWN), not red.
“We swap APs all the time.”	Replaced hardware keeps the device's name, contacts, rules and history on the new unit — no re-import, no orphaned history.
“Does the key let you change our network?”	SmartTile issues no configuration writes to UniFi. Delete the key on the console and access ends.

The AP that rebooted at 2 a.m. is in the uptime report — and the site that went dark already has its ticket.