SMARTTILE · DEVICEAUTOMATE™ · CISCO MERAKI

Every Meraki organisation, watched every 30 seconds

One Dashboard API key puts your MX appliances, MS switches, MR access points and the rest of the Meraki estate on the same pane as your circuits — status, WAN loss and latency, licences, VPN tunnels and firmware — with outages ticketed in the IT Service Management (ITSM) system your team already works in.

SMARTTILE INTEGRATES WITH

Cisco Meraki Dashboard — every organisation, network and device (MX, MS, MR, MG, MV, MT) the key can see — through the **Meraki Dashboard API v1** with one API key per company.

HOW SMARTTILE AUTOMATES IT

Reads device status every 30 s and syncs networks, licences, VPN, firmware and uplinks every 5 min. A device offline 14 min (you set it) is e-mailed and ticketed; a watched VPN tunnel down 3 min is ticketed by VPNAutomate; licences are alerted from 90 days out.

CATEGORY

Device
DeviceAutomate™

The Meraki Dashboard knows the moment an access point drops, a WAN uplink loses packets or a licence is about to lapse — but only if someone is looking at it. SmartTile looks for you. Paste one API key and SmartTile discovers every organisation, network and device behind it, imports the ones you pick onto your sites, and from then on turns what Meraki reports into **DOWN, UP, history and tickets** — the same way it treats every other device you monitor.

What the Meraki connection turns on

Discovery and import

Organisations, networks and devices found automatically. A preview shows every serial before import; each lands on a site matched from its network name, with model, serial, MAC and firmware filled in.

Status from the truth

Meraki's own online / offline / alerting / dormant reading every 30 s, plus a direct ping of the LAN address where SmartTile can reach it. Every change is written to the device's state history.

Outage → ticket

Offline for 28 polls (14 min, adjustable per organisation): e-mail to your recipients and a ticket in your ITSM system at the device's location. Back up: a restored e-mail.

WAN loss and latency

Every point of Meraki's uplink loss / latency series kept for 35 days, per-uplink bandwidth, and threshold tickets on loss, latency, temperature and bandwidth.

Ports, radios, sensors

Every switch port (link, speed, PoE, errors, LLDP/CDP neighbour), wireless channel utilisation, cellular signal, MX security events and MT readings — refreshed every 10 min.

Licence countdown

Licences and subscriptions checked every minute; e-mails at 90, 60, 30, 15, 5 and 1 days and on expiry, with co-term date shifts detected.

VPN tunnels

AutoVPN pairs and third-party IPsec peers polled every 60 s by VPNAutomate. A watched tunnel down 3 min opens one ticket; restored, it is noted and closed per your policy.

Firmware and changes

Running and available firmware per network into FirmwareAutomate advisories. Every dashboard configuration change, with the admin's name, lands in AccessAutomate.

How it goes live

1. **Enable API access (Meraki).** Organization → Settings → Dashboard API access → tick *Enable access to the Cisco Meraki Dashboard API*.
2. **Generate the key (Meraki).** Profile icon → My profile → API access → *Generate new API key*. Copy it — Meraki shows it once.
3. **Paste it (SmartTile).** Meraki Manager → Settings → Add API Key → *Save & Discover*. Discovery starts at once; *Test* lists the organisations the key can see.
4. **Pick and import.** Devices tab → select → preview → import. Set alert recipients and the down threshold under Settings → Alert Configuration.

No agent, no appliance, no inbound firewall rule — SmartTile calls the Meraki cloud, never your network.

MERAKI KEY BELONGS TO	WHAT WORKS
Read-only organisation admin	Discovery, status, outage tickets, loss/latency, ports, licences, VPN monitoring, firmware advisories, change history, config backups.
Full organisation admin	Everything above, plus the buttons that change a device: reboot, blink LEDs, cycle a switch port.
Optional · off by default	Arming a Meraki firmware window from SmartTile, and VPN auto-heal for third-party tunnels. Each needs its own switch turned on.

When something goes wrong

THE MOMENT	TODAY	WITH SMARTTILE
An AP drops off	Someone notices in the Dashboard — or a user calls.	Meraki reports *offline*; after your threshold the device goes DOWN, the NOC is e-mailed and a ticket opens at that site.
The API goes quiet	Everything stays green because nothing says otherwise.	Three failed status reads in a row turn the organisation's devices UNKNOWN, never green, and the NOC is told monitoring is blind.
A device leaves its network	It shows the last good status for weeks.	Flagged *not in any network*, with who removed it and when, and a warning before anyone re-adds it.
A licence is expiring	Discovered the day it stops passing traffic.	A countdown of e-mails from 90 days out.

Exactly what SmartTile asks the Meraki Dashboard API

GET `/organizations/{id}/devices/statuses`
status every 30 s

GET `/organizations/{id}/devices/availabilities`
DOWN / UP and state history

GET `/organizations/{id}/devices/uplinksLossAndLatency`
WAN loss and latency

GET `/organizations/{id}/networks · /devices · /inventory/devices`
discovery, network membership

GET `/organizations/{id}/licenses · subscriptions`
licence countdown

GET `/organizations/{id}/appliance/vpn/statuses`
AutoVPN reachability

GET `/networks/{id}/events (non_meraki_vpn)`
third-party tunnel truth

GET `/networks/{id}/firmwareUpgrades`
running and available firmware

GET `/organizations/{id}/switch/ports/bySwitch`
port telemetry (plus radios, sensors, security)

GET `/organizations/{id}/configurationChanges`
who changed what

POST `/devices/{serial}/reboot · blinkLeds · switch/ports/cycle`
only when a permitted user clicks

PUT `/networks/{id}/firmwareUpgrades · appliance/vpn/siteToSiteVpn`
only with firmware execution / auto-heal on

Security and control

Key encrypted at rest

Encrypted (AES-256-GCM) before it is stored and decrypted only to make a call. It is never sent back to the browser.

Your company only

Each company adds its own key. Every Meraki screen and action is checked against the companies you belong to.

Roles on every button

Viewers read; operators can ping, blink and cycle a port; only admins reboot. Every action, allowed or refused, is logged with user and time.

Polite to Meraki

8 calls a second per organisation, backs off on 429, and pauses a key after 50 failures in a row instead of hammering it.

Common objections

OBJECTION	ANSWER
“The Meraki Dashboard already alerts.”	It e-mails. SmartTile records the outage, opens the ticket at the right site in your ITSM system, and keeps history next to your circuits and other vendors.
“Will you change our config?”	Monitoring only reads. The buttons that change a device need a full-admin key and a permitted user; firmware windows and VPN auto-heal stay off until you turn them on.
“Our key sees many organisations.”	Hide the ones you don't want, and import only the devices you pick.

One API key, and the Meraki estate you already own reports DOWN and opens its own ticket.