SMARTTILE · DEVICEAUTOMATE™ · FORTINET FORTIGATE

FortiGate, unlocked through the API

One read-only API user on the firewall turns a ping-only FortiGate into a fully observed one — identity, health, VPN tunnels, the policy rule base, configuration backups and firmware advisories — next to the rest of the network, with tickets in the IT Service Management (ITSM) system your team already uses.

SMARTTILE INTEGRATES WITH

Fortinet FortiGate firewalls (FortiOS) — directly, through the FortiOS REST API (`/api/v2/monitor` and `/api/v2/cmdb`) on the HTTPS admin port, with an API token or an admin login.

HOW SMARTTILE AUTOMATES IT

Polls every FortiGate with credentials every 5 minutes (identity, interface counters) and hourly (rule base → change ledger); backs up the config on change; turns new FortiGuard builds into firmware tickets that are scheduled, verified and closed.

CATEGORY

Device
DeviceAutomate™

A FortiGate watched by ping alone says up or down and nothing else. FortiOS has a REST API that answers what a NOC actually asks, and SmartTile only ever **reads** it: every monitoring call is a GET, and the one write SmartTile can make — starting a firmware upgrade — is switched off platform-wide by default. Up/down stays with SmartTile's ping check; the API adds everything behind it.

What the API turns on

Identity that fills itself

Serial, model, hostname, FortiOS version and MAC are written to the device record every 5 minutes, each marked "FortiGate API" with the time. A value typed by a person is never overwritten.

Health at a glance

CPU, memory and session count with the FortiGate's own recent history, interface link state and uptime — in the device's **Analytics** view and in Device Health.

VPN tunnels

Every IPsec tunnel: up or down, phase-2 selectors, local and remote subnets, bytes in and out — plus the count of active SSL-VPN sessions. Read live when the VPN view is opened.

Policy inventory + change ledger

Every rule and the addresses, groups, services and VIPs it references, with per-rule hit counters. Re-read hourly; every rule added, removed or modified is logged field by field (90-day view).

Configuration backups

The full configuration pulled over HTTPS on the device's backup schedule. Saved only when it changes, with a diff of what changed; a change can raise a ticket. Needs super_admin — see the table.

Firmware advisories

FortiGuard builds compared with what is running. Target = newest patch on the same branch (7.4.4 → 7.4.8); a branch jump is flagged as a planned migration. Ticketed with a 14-day SLA, scheduled, verified, closed.

Honest uptime

The Uptime view uses the FortiGate's boot counter and the outages SmartTile recorded — a recorded DOWN always counts, and the view never guesses 100% from silence.

Test REST API explains itself

Tests what is typed, before saving. A timeout becomes a sentence: wrong port (and which one answers), HTTPS admin closed on the WAN, or token rejected.

What it takes on the firewall — the change request

1. **Create the API user.** System → Admin Profiles and API Users → new API user with a read-only profile. Generate the key (FortiOS shows it once) and paste it in SmartTile: DeviceAutomate → Fortinet FortiGate → **FortiGate Setup**. Or: a dedicated admin (System → Administrators) with username + password.
2. **HTTPS admin access.** Enabled on a reachable interface; port from System → Settings → Administration Settings (SmartTile assumes `10443` if left blank).
3. **Trusted hosts.** If enforced on that user, allow SmartTile's two monitoring addresses: `157.245.117.9` and `159.203.150.140` .
4. **Test REST API.** Green shows the hostname and FortiOS version it reached; anything else is explained in plain words.

No agent, no SNMP required, no inbound rule to the LAN, no change to production policies. Delete the API user and access ends.

ACCESS LEVEL	WHAT WORKS
Read-only API user or admin	Identity, health, VPN tunnels, policy inventory and change ledger, firmware advisories (detect, ticket, schedule, verify).
super_admin profile	Everything above, plus configuration backups over the API — FortiOS refuses the backup call to anyone less. Still reads only.
Firmware execution · off by default	SmartTile starts the scheduled upgrade itself. Needs the platform switch "Execute upgrades" on and stored credentials; the FortiGate reboots to finish. Otherwise a technician upgrades in the window and SmartTile verifies.

Security posture, for the change board

Read-only by design

Every monitoring, policy, backup and firmware-check call is a GET. SmartTile never writes a rule. The only write — the firmware upgrade — is off platform-wide by default.

The token is never shown

Sent only in the Authorization header. The API returns “token set”, never the value; the field always reads blank; the audit log redacts it by field-name pattern.

Two addresses, one port

With Trusted Hosts, only `157.245.117.9` and `159.203.150.140` can use that user on the admin port. Revoke the user and access ends.

Multi-tenant and audited

Every FortiGate view is tenant-checked — your company’s users and SmartChoice super admins only. Each Test REST API run is written to the activity log with the result.

Exactly what SmartTile asks the firmware

GET	`/api/v2/monitor/system/status`	identity, FortiOS version, uptime; the Test call
GET	`/api/v2/monitor/system/interface`	interfaces, link state, MAC
GET	`/api/v2/cmdb/firewall/policy`	the rule base (inventory, ledger)
GET	`/api/v2/cmdb/firewall/address · addrgrp · vip`	objects the rules reference (+ services)
GET	`/api/v2/monitor/system/firmware`	running and available builds; verify
GET	`/api/v2/monitor/system/resource/usage`	CPU, memory, sessions
GET	`/api/v2/monitor/vpn/ipsec · /vpn/ssl`	IPsec tunnels · SSL-VPN sessions
GET	`/api/v2/monitor/firewall/policy`	per-rule hit counters
GET	`/api/v2/monitor/system/config/backup`	configuration backup (super_admin)
POST	`/api/v2/monitor/system/firmware/upgrade`	only with “Execute upgrades” switched on

Firmware, ticketed where your team works

New build → a ticket

One advisory per FortiGate with running and target versions, the same-branch or branch-jump note and the SLA date — opened in Rev.io and in each system the company has enabled for firmware, Jira Service Management and Asana included.

Window → verify → close

Schedule the window; the ticket gets a note when it opens. SmartTile re-reads the running version for up to 4 hours afterwards and closes the ticket when it matches.

Switches you control

FirmwareAutomate is on for Automate-tier companies, with a per-device off switch. Auto-ticketing and contact e-mails each have their own switch; execution is off until you turn it on.

Change summary

CHANGE	RISK	ROLLBACK
Read-only API user and its token	Low — the profile cannot change configuration; SmartTile only reads.	Delete the API user.
Trusted-host entries for two SmartTile addresses	Low — narrows who may use the new user to two hosts.	Remove the entries.
Optional: super_admin profile for config backups	Medium — a full read of the configuration; still no writes.	Downgrade the profile; backups stop, the rest continues.
Optional: firmware execution by SmartTile	A planned change per window, with a reboot.	Leave “Execute upgrades” off — the default.

Common objections

OBJECTION	ANSWER
“You would have write access to our firewall.”	No. The profile is read-only and the calls are reads. Firmware execution is the only write, and it stays off unless it is switched on.
“Is the token safe with you?”	Never shown back, never logged, sent only as a header, usable only from the two addresses you allow.
“We already have FortiManager.”	Different job. SmartTile puts the FortiGate next to your circuits, switches and access points, with tickets in your ITSM system — it does not manage configuration.

Ten minutes on the firewall, read-only — and your FortiGate joins the pane your NOC already watches.