SMARTTILE · DEVICEAUTOMATE™ · CISCO SECURE FIREWALL MANAGEMENT CENTER

Every Firepower firewall, watched through one FMC login

Connect the Management Center once and SmartTile sees every Threat Defense firewall behind it — inventory, health, confirmed outages with a ticket, daily log exports, versioned configuration snapshots, admin-login alerts and Cisco advisories — with the firewalls themselves left untouched.

SMARTTILE INTEGRATES WITH

Cisco Secure Firewall Management Center (FMC 7.x) and the Threat Defense (FTD) firewalls it manages — the FMC REST API (`fmc_platform/v1` + `fmc_config/v1`), plus a syslog receiver the firewalls send to.

HOW SMARTTILE AUTOMATES IT

Polls the FMC every 60 s: imports each FTD with model, serial and version; turns health RED (or an FTD the FMC stops listing) into a confirmed DOWN with a Rev.io ticket; saves daily log exports and change-only config snapshots to Documents; alerts on admin logins outside your allow-list.

CATEGORY

Device
DeviceAutomate™

An FTD watched by ping answers one question. The Management Center already knows every firewall's model, software version, HA role, health and pending deployments, and who logged in to change what. SmartTile signs in to the FMC with a dedicated API user — **Read Only is enough for monitoring** — and turns what it knows into devices, tickets and documents on the same pane as the rest of the network.

What the FMC connection turns on

Choose-before-import inventory

Every managed FTD listed as new, linked, imported or offline. Tick the ones you want; one already pinged by IP is **linked, never duplicated**. Model, serial and version are written to the device and kept fresh each poll.

Down from the FMC's own health

With *Monitor via FMC health*, RED for 3 polls (~15 min) = DOWN; an FTD the FMC stops listing = DOWN after 3. Each change lands in state history and a new DOWN opens a **Rev.io ticket**. All three counts are tunable.

Blind is grey, not green

If SmartTile cannot reach the FMC for 3 polls, its firewalls turn UNKNOWN and the NOC gets one e-mail — a dead FMC or expired password never shows an estate as healthy.

Configuration snapshots

Devices, interfaces, static routes, HA pairs, access and NAT policies and rules, objects and security zones — one JSON bundle daily, **stored only when it changed**, with a section-by-section compare.

Logs into Documents

Daily at the hour you pick: audit records, health alerts, health metrics (CPU, memory, disk), inventory, pending deployments and the FMC's backup-file list — each as CSV plus raw JSON.

AccessAutomate on admin logins

FMC audit logins, logouts, failed logins and changes, by user and source IP. A login not on the allow-list, or repeated failures, opens a ticket and e-mails the contacts you choose.

Advisories and upgrades

Cisco PSIRT advisories flagged against your running FMC and FTD versions. FirmwareAutomate spots an upgrade package on the FMC newer than an FTD's version, and tickets, schedules and verifies it.

Firewall syslog

FTDs and the FMC can send syslog (UDP/TCP 514) to SmartTile — connection, intrusion, file and audit events the REST API does not carry. Only known firewall addresses are accepted.

What it takes on the FMC — the change request

1. **Create the API user.** FMC: System → Users → Users → Create User, e.g. `smarttile`, long random password, role **Read Only**. Add an **Administrator** user later only for native backups or changes.
2. **Confirm the REST API is on.** System → Configuration → REST API Preferences → Enable REST API (on by default).
3. **Allow HTTPS (TCP 443) from SmartTile.** The wizard shows the address: SmartTile's public IP, or the site VPN tunnel address for a private FMC. System → Configuration → Access List → Add Rules, and on any edge firewall in front.
4. **Connect and test.** DeviceAutomate → Cisco Secure Firewall (FMC): URL, user, password. SmartTile tests the sign-in, then probes every endpoint and reports read-only or read-write.

Tokens last 30 minutes and renew themselves — the `smarttile` user signing in every half hour in the FMC audit log is expected.

FMC USER	WHAT WORKS
Read Only	Inventory and import, health and DOWN detection, config snapshots, log exports, backup-file list, advisories, firmware detect → ticket → verify.
+ Administrator (optional second user)	Adds native FMC/FTD backups and reads a Read Only user is refused (e.g. pending deployments on 7.6). **Still no writes** unless *Allow write actions* is switched on.
Allow write actions · off by default	Deploy pending changes; create, edit, delete host / network / port objects; start an FTD upgrade from FirmwareAutomate (also needs the platform switch, off by default).

Exactly what SmartTile calls on the FMC

POST	`/api/fmc_platform/v1/auth/generatetoken`	sign in (Basic); refreshtoken renews it
GET	`…/devices/devicerecords`	every FTD: model, serial, version, health
GET	`…/health/alerts · /health/metrics`	health alerts; CPU, memory, disk
GET	`…/deployment/deployabledevices`	pending deployments
GET	`…/object/networks · hosts · ports`	objects and security zones
POST	`…/backup/operational/devicebackup`	native FTD backup — Administrator only
GET	`/api/fmc_platform/v1/info/serverversion`	FMC version, VDB, SRU
GET	`…/devicehapairs/ftddevicehapairs`	HA role (primary / secondary)
GET	`…/audit/auditrecords`	who signed in and changed what
GET	`…/policy/accesspolicies · ftdnatpolicies`	rules for the config snapshot
GET	`…/updates/upgradepackages`	upgrade packages + applicable devices
POST	`…/deployment/deploymentrequests`	deploy — only with write actions on

SmartTile checks write permission with an empty-body request the FMC rejects before creating anything (403 = read-only). Calls are serialised with a pause to stay under the FMC's 120 requests a minute. The FMC API has **no restore call** — SmartTile keeps the snapshots, the backup-file list and a restore runbook; the restore itself runs on the FMC.

Security and control

Passwords stay in the vault

Both FMC passwords and the PSIRT client secret are encrypted at rest. The API returns only *has password* flags — the field reads blank on edit — and tokens are never logged.

Read-only unless you say otherwise

Every change sits behind a second Administrator user **and** *Allow write actions*, off by default. Each attempt is written to a change ledger with the request, the FMC's answer and who.

Your company only

Admins see and manage only their own company's FMC connections. Every create, edit, backup, export and change is written to the transaction log with user, time and source IP.

Switchable

One switch turns the whole integration off without a redeploy, plus a server kill switch; the syslog receiver has its own. Down counts, export hour and snapshot hour are set per FMC.

Common objections

OBJECTION	ANSWER
“You would have write access to our firewalls.”	Not with a Read Only user — the FMC itself refuses. Writes need a second Administrator user and a switch that is off by default, and each one is ledgered.
“We don't expose the FMC to the internet.”	Allow HTTPS from one SmartTile address, or reach a private FMC over the site VPN tunnel. Event logs come the other way, by syslog from the firewalls.
“A policy deploy turns health red for a minute.”	One RED poll changes nothing. DOWN needs 3 consecutive polls by default, and you can set it anywhere from 1 to 30.
“We already have FMC dashboards.”	SmartTile puts the FTDs beside your circuits, switches and access points, opens the ticket, and keeps the logs and snapshots in Documents for the audit.

One Read Only user on the Management Center — and every firewall behind it joins the pane your NOC already watches.