SMARTTILE · DEVICEAUTOMATE™ · SITE-TO-SITE VPN (IPSEC / IKEV2)

# Your private network, watched through one IPsec tunnel

One IKEv2 tunnel from your firewall to SmartTile lets us monitor the switches, access points, phones and cameras that live on private addresses — with no port opened to the internet — and VPNAutomate watches the tunnel itself, opening and closing the ticket when it drops.

**SMARTTILE INTEGRATES WITH**

Any firewall or router that speaks standards-based **IPsec IKEv2 with a pre-shared key**, tunnelled to the **strongSwan** VPN server inside SmartTile.

**HOW SMARTTILE AUTOMATES IT**

SmartTile writes and loads its side of the tunnel from the Location record, polls and pings the private devices *through* the tunnel, and VPNAutomate reads the tunnel's live state every 60 s — down past 3 minutes opens a ticket in your ITSM system, noted and closed when it is back.

**CATEGORY**

**Device**
DeviceAutomate™

Most of a site's network has no public address: the switch stack, the access points, the phones, the camera recorder. Monitoring them from the cloud means either exposing them — no — or building a private path. A site-to-site IPsec tunnel is that path. SmartChoice builds SmartTile's end from the site's Location record; your firewall builds the other end with the same settings. From then on SmartTile reaches every device in the subnets you name, and the tunnel is a monitored thing in its own right.

## What the tunnel turns on

### Private devices, monitored

Ping, SNMP and SSH to addresses inside the tunnel's subnets are sent from SmartTile's own tunnel address, so they ride the tunnel instead of leaking to the internet — and the devices report up, down, vendor, model and serial like any other.

### SmartTile's side, written for you

Saving the Location writes the strongSwan connection ( `tunnel-<location>` ) and its key, then reloads IPsec **without dropping the other tunnels** on the server. The result — provisioned, or exactly why not — shows on the Location.

### Live tunnel state on the Locations list

Each site shows **VPN UP** with its uptime, **VPN DOWN** or **VPN ERROR**, read live from the VPN server — not from the saved setting.

### VPNAutomate: the tunnel is watched

Every IPsec tunnel on the server appears on DeviceAutomate → VPNAutomate. Switch **Watch** on and it is polled every 60 s from `ipsec statusall` : established = up, configured but no security association = down.

### Down → a ticket; back → closed

Down for 3 minutes (per tunnel, 0–1440) opens a ticket in the ITSM system your company connected and e-mails the contacts you pick. On restore: a note, then auto-close per your Ticket Policy. Drops again first? A note, and the close is cancelled.

### Re-establishes by itself

Tunnels are written `auto=route` with dead-peer detection set to restart, so a cleanly closed tunnel comes back on the next monitoring packet instead of waiting for a person.

## What it takes on your firewall — the change request

1. **SmartChoice sets up SmartTile's side.** Locations → edit the site → *VPN Configuration*: your firewall's public IP (Peer IP), the private subnets to monitor (VPN Subnets), the pre-shared key, encryption, DH group, PFS and lifetime. The same panel shows **Our IP** and **Subnet** — SmartTile's end.
2. **Build the matching tunnel on your firewall.** A route-based or policy-based IKEv2 site-to-site VPN to *Our IP*: local networks = the subnets you gave us, remote network = SmartTile's subnet, same PSK and proposals.
3. **Allow monitoring in.** Permit ICMP (and SNMP / SSH if you want those) from SmartTile's subnet to the devices, and point each device's SNMP allow-list at it.
4. **Check the pill.** The Location shows VPN UP with its uptime. Then switch Watch on for the tunnel in VPNAutomate.

No inbound port to your LAN from the internet, no agent, nothing changed on production traffic. Delete the tunnel on your side and access ends.

| SETTING | SMARTTILE'S SIDE |
|---|---|
| **Key exchange** | IKEv2, pre-shared key |
| **Proposal** | `aes256-sha256` (default), `aes256-sha1` or `aes128-sha1` |
| **DH group** | 14 (default), 2, 5, 19 or 20 |
| **PFS** | On by default |
| **Lifetime** | 28,800 s IKE and child (default) |
| **NAT** | UDP encapsulation forced; fragmentation on |
| **Dead peer** | 30 s detection, restart |
| **Scope** | Only the subnets you list for the site |

## When a tunnel drops

**VPN tunnel down: Head Office ↔ SmartTile (IPsec tunnel to SmartTile)** — OPENED · AUTOMATED

Down for 4 min — configured but no security association.

Site: Head Office · Peer: 203.0.113.10 · Watched by VPNAutomate

**Next steps:** confirm both sites have WAN service (a circuit outage is a carrier ticket, not a VPN one); if they do, check the peer-side tunnel config and escalate.

Link back to the tunnel in SmartTile VPNAutomate.

> SmartTile VPNAutomate: Head Office ↔ SmartTile is back up after 22 min (IKE SA established). This ticket closes automatically if the tunnel stays up. 09:36

> Stayed up since 09:36 — closing per the platform Ticket Policy. 09:46

**Where the ticket goes** is worked out per company from what that company has actually connected: its own IT Service Management (ITSM) system under ServiceAutomate — Kaseya (Autotask, BMS), Freshservice, ServiceNow, Jira Service Management, HaloPSA, ConnectWise PSA, Zendesk, NinjaOne, ManageEngine, Ivanti or Freshdesk — and Rev.io only for companies SmartChoice manages there. The page shows the same answer before anything fires; nothing connected means no ticket, and it says so. The Ticket Policy open delay is honoured.

## Security and control

### Nothing exposed

Monitoring reaches private addresses only through the encrypted tunnel, and only the subnets named for that site. Your devices never need a public address.

### Never overrides a human

SmartTile owns exactly one include file. It refuses to write a tunnel that collides with a manually-built one, and refuses to reload keys if the secrets file has wildcard or conflicting entries — the reason is shown on the Location.

### Your tenant only

VPNAutomate shows each company only its own tunnels (reseller: its companies). Watch, alert window, contacts and ticket/e-mail are per tunnel; a new tunnel is never watched by surprise.

### Switches and evidence

Engine, ticketing and e-mail switches; a global kill switch for tunnel provisioning; every state change recorded and downloadable as CSV.

## Common objections

| OBJECTION | ANSWER |
|---|---|
| **“We will not expose our LAN.”** | You don't. The tunnel is encrypted IPsec between your firewall and SmartTile; devices keep private addresses and only the subnets you name are reachable. |
| **“Which firewalls?”** | Anything that does IKEv2 with a pre-shared key — the settings are standard strongSwan proposals, listed on page 1. |
| **“One hub failure will page us fifty times.”** | Each tunnel alerts once, after its window. For hub-and-spoke designs, Smart Alerting can hold the downstream devices as a visible *VPN Hub Outage - Automated Snooze* behind one hub ticket — off by default, switched on by SmartChoice per server once the hub layout is checked. |
| **“A re-key will open a ticket.”** | No — the 3-minute window (per tunnel, adjustable) filters a re-key; tunnels are not watched until someone switches Watch on. |

**One tunnel, and the private half of your network is on the pane with the rest of it.**