SMARTTILE · DEVICEAUTOMATE™ · CLOUDAUTOMATE · AMAZON WEB SERVICES

Your AWS servers, on the same pane as the network

One read-only IAM access key turns every EC2 instance, RDS database and Amazon WorkSpace into an ordinary SmartTile device — status checks, CloudWatch metrics, uptime history, spend and security findings — alerting and ticketing in the IT Service Management (ITSM) system your team already uses.

SMARTTILE INTEGRATES WITH

Amazon Web Services — EC2, RDS and Amazon WorkSpaces, through the AWS APIs (EC2, CloudWatch, RDS, WorkSpaces, Cost Explorer, GuardDuty, Security Hub, IAM, Support) with one IAM access key per account.

HOW SMARTTILE AUTOMATES IT

Imports each resource one-to-one as a device under an "AWS <region>" location, polls its state every 60 s so a stopped or failed instance goes DOWN and tickets like any device, stores CloudWatch metrics every 5 min for health thresholds, and syncs spend and findings hourly.

CATEGORY

Device
DeviceAutomate™

A cloud server usually sits outside the NOC's view: it is not on a switch port, often does not answer ping, and its health lives in the AWS console. SmartTile CloudAutomate reads the account with a least-privilege IAM user and makes each instance a device like any other — **the state AWS reports this poll is the truth**, so a stopped instance, a failed status check or an expired key shows up instead of staying green.

What the AWS connection turns on

Servers as devices

EC2 instances, RDS databases and Amazon WorkSpaces imported one-to-one under an "AWS us-east-1"-style location. You pick what imports; a re-import updates in place, never duplicates.

Up/down from AWS itself

Instance state plus both EC2 status checks (system and instance), RDS status and WorkSpace state, every 60 s. DOWN after 2 bad polls, UP at once; every change lands in state history.

CloudWatch metrics

CPU, network in/out, EBS read/write ops and **CPU credit balance** every 5 min; memory and disk too when the CloudWatch agent runs. RDS: CPU, storage used, IOPS.

Honest when blind

If AWS stops answering for a key, its servers turn UNKNOWN after ~6 minutes and the NOC gets one e-mail — never a silent green. A launch time is never shown as uptime.

Spend

Cost Explorer daily and monthly spend, by service and by region, with the month's forecast — cached hourly on the Spend tab.

Security findings

GuardDuty (severity 4+) and Security Hub (high / critical), plus SmartTile's own checks: ports 22/3389/3306/1433/5432/27017/6379 open to 0.0.0.0/0, unencrypted EBS, access keys > 90 days.

Right-sizing hints

The Utilization tab flags idle, oversized and hot servers from 24 h, 7 d or 30 d of samples.

AWS Support cases

With a Business or Enterprise support plan: open a real AWS Support case from the device, or arm a device to open one on a confirmed outage. Both switches **off by default**.

How it goes live — about five minutes

1. In SmartTile: **DeviceAutomate** → **CloudAutomate** → **AWS**. Tick the scopes: Monitoring (always), Inventory, Spend, Security, Support. SmartTile generates the policy for exactly those.
2. AWS Console → **IAM** → **Policies** → **Create policy** → **JSON**. Paste the generated policy; name it `SmartTileCloudAutomate`.
3. **IAM** → **Users** → **Create user** `smarttile-cloudautomate`, no console access, attach the policy directly.
4. User → **Security credentials** → **Create access key** → "Application running outside AWS". Copy the key ID (`AKIA…`) and the secret — shown once.
5. Paste both, optionally regions and a name or tag filter, then **Save & Test**. Pick servers from the import table and import.

SCOPE	WHAT THE POLICY ALLOWS
Monitoring	`ec2:Describe` *instances/status/regions,* `cloudwatch:GetMetricStatistics` , `rds:DescribeDBInstances` , `workspaces:Describe` — read only
Spend	`ce:GetCostAndUsage` , `ce:GetCostForecast`
Security	GuardDuty / Security Hub findings, security groups, volumes, IAM users and key ages — read only
Support	`support:CreateCase` and case reads — the only write, and only if ticked

Save & Test calls each API once and records which scopes actually work — a missing permission shows as a locked tab, not a broken page. Blank regions = every region enabled on the account.

Exactly what SmartTile calls on AWS

READ	`sts:GetCallerIdentity`	Save & Test: proves the key and names the account
READ	`ec2:DescribeInstances`	Daily discovery (02:30) of instances, IPs, type, tags
READ	`rds:DescribeDBInstances`	RDS discovery and status
READ	`cloudwatch:GetMetricStatistics`	AWS/EC2, AWS/RDS, AWS/WorkSpaces, CWAgent metrics
READ	`guardduty / securityhub GetFindings`	Hourly threat and posture findings
POST	`support:CreateCase`	Only when a case is opened — switches off by default
READ	`ec2:DescribeRegions`	Which regions to scan when the field is blank
READ	`ec2:DescribeInstanceStatus`	Every poll: state + system/instance status checks
READ	`workspaces:DescribeWorkspaces`	WorkSpace inventory, state and connection state
READ	`ce:GetCostAndUsage / GetCostForecast`	Hourly spend by day, service, region + forecast
READ	`ec2:DescribeSecurityGroups, iam:ListAccessKeys`	SmartTile's own exposure and key-age checks

EC2 web-01 (us-east-1) — failed instance status check

DEVICE DOWN

Device: web-01 · t3.medium (2 vCPU / 4 GB) · Location "AWS us-east-1"

Seen by SmartTile: state *running*, instance status check *impaired* on two polls in a row → DOWN

Then: the normal ticket path for the company — Rev.io or the connected ITSM system — with state history and the Uptime chart showing the outage

- Status check failed — DOWN confirmed poll 2
- Outage ticket opened in the ITSM system per company rules
- If armed: AWS Support case opened, and noted into the outage ticket off by default
- Status checks pass — UP, ticket follows its auto-close rule next poll

Security and control

Least privilege, generated

The policy is built from the scopes you tick. Without Support ticked nothing in it can create, change, stop or delete anything.

Secret encrypted, never shown

The secret access key is encrypted at rest the moment it is saved and never returned by the API — only whether one is stored.

Walled per company

Each company connects its own AWS account; every CloudAutomate call is fenced to the caller's organization, and adding or testing keys needs an admin.

You choose what enters

Region, name and tag filters apply before discovery; the import table shows exactly what will be created or updated.

Every switch visible

Engine, status sync, health metrics, spend, security, WorkSpaces, auto-region and support cases each have their own Engine Safety switch, plus a global kill switch.

Audited

Key created, tested, updated or deleted, every import and every support case is written to the activity log, and every sync to the Connections tab log.

Common questions

QUESTION	ANSWER
Can SmartTile change our AWS account?	No — every scope except Support is read-only, and Support is opt-in. The only write is `support:CreateCase`.
Why no memory or disk?	AWS only publishes them through the CloudWatch agent (`CWAgent`). Install it and they appear; CPU, network and status checks work without it.
Does a stopped server alert?	Yes — anything not running or pending is DOWN. Keep a deliberately-stopped server out with the import filter or its own alert switches.

The server you would have found in the AWS console is already on the pane — with the ticket on its way.