

Sentinel: what you are approving

A one-page summary for whoever signs off the network change. Every line is a statement of fact about the software, not a marketing claim.

THE CHANGE, IN ONE SENTENCE

- One machine on your network makes an outbound HTTPS connection to Sentinel. Nothing is opened inbound. That is the whole change.

NETWORK

- Outbound: TCP 443 to a single Sentinel host, which you are given at install time.
- Inbound: none. No port forwarding, no VPN, no NAT rule, no inbound firewall change.
- Local: the machine reaches your cameras on their RTSP port (554 by default) on the same network. RTSP is forced over TCP.

THE MACHINE

- An always-on Windows or Linux box on the same LAN as the cameras. A CPU is enough; an NVIDIA GPU is faster and is picked up automatically.
- Runs as a Windows service or a systemd unit. Its state directory (C:\ProgramData\Sentinel\agent, or /var/lib/sentinel) is locked to SYSTEM and Administrators by SID.
- Logs to that directory, rotating at 5 MB x 5. Start, stop and fatal errors also go to the Windows event log.

WHAT LEAVES THE SITE

- A heartbeat every 45 seconds. Events. One snapshot per event, downscaled to 640px wide at the site and refused above 2 MB. A short clip, 8 seconds before the event and 4 after. Camera and agent status. One thumbnail per discovered camera, capped at 150 KB.
- Not sent: continuous video, audio, or anything at all from a camera nobody selected in the panel.
- If the link drops, events queue on local disk and replay when it returns. They are deleted only once the control plane has acknowledged them.

CREDENTIALS

- Enrollment uses a single-use token that expires in 24 hours. It is traded for a long-lived agent key stored owner-only on the machine and never printed.
- Camera credentials given to the agent stay on that machine. A stream URL that embeds a credential is encrypted at rest in the control plane and decrypted in exactly one place.

ACCESS AND AUDIT

- Roles are admin, site manager and viewer, and can be scoped to particular sites and to individual cameras.
- Every configuration change is written to an audit log. So is every view of footage.