ADVANCED
MECHATRONIC
SOLUTIONS

Access Control Gateway — On-site Checks (Wi-Fi & PoE)

Data/Date: 2025-10-21

Summary & Purpose

This guide helps diagnose gateway disconnects/power-offs on site. It includes quick checklists for Wi-Fi and PoE/Ethernet versions. Please follow these steps before opening a ticket.

Checks for Wi-Fi Gateway

- Stable power (PSU). Use UPS if available.
- 2.4 GHz signal RSSI ≥ −65 dBm; place gateway away from interference (microwave, BT).
- Fix channel to 1/6/11, 20 MHz width; avoid congested 'auto'.
- Dedicated IoT SSID (no captive portal); disable band steering/forced 5 GHz.
- WPA2-AES authentication (avoid TKIP/mixed).
- DHCP lease ≥ 24 h with IP reservation by MAC (prevents conflicts).
- DNS/NTP reachable; correct router time (TLS relies on clock).
- Firewall: allow only outbound TLS (TCP 443) and, if applicable, MQTTS (TCP 8883) 2999、4999、9999, should be concerned..
- No TLS inspection/SSL proxy on the IoT SSID.
- Update firmware on gateway and AP/router; factory reset and clean setup if needed.

Checks for PoE/Ethernet Gateway

- Tested Ethernet cable (Cat5e/6) and alternate switch port.
- Check PoE budget on the switch; try PoE injector or external PSU.
- Disable EEE/Green Ethernet on the device port.
- Link negotiation: use auto/auto; if unstable, force 100/Full or 1000/Full as supported.
- Switch port in access mode on the correct IoT VLAN (untagged).
- Enable PortFast/Edge; ensure STP is not blocking the port.
- Port-security/Sticky MAC: adjust limits; clear bindings when swapping gear.
- If 802.1X/NAC is present: exempt the port (MAC auth bypass) or apply an 'IoT Allowed' profile.
- DHCP Snooping/IP Source Guard/DAI: ensure proper bindings/reservations; avoid drops.
- Upstream Firewall/ACL: allow outbound TLS (TCP 443) and MQTTS (TCP 8883) 2999、4999、9999, should be concerned.; no TLS inspection.

Quick Checklist (60 seconds)

- Swap PSU/port/PoE and confirm stable LEDs.
- RSSI ≥ −65 dBm (Wi-Fi) OR 100/1000 Full link (PoE).
- DHCP reservation in place (no duplicate IPs).
- Outbound TLS 443 (and 8883 if applicable) allowed (no SSL proxy).
- DNS/NTP reachable; correct time.
- Firmware up to date; proper temperature.

Information to return to support

- Exact time/date of the incident.
- Gateway serial number and MAC/IP.
- AP/switch logs/screenshots (link flap, STP, port-security, DHCP).
- Confirmation of VLAN/SSID and applied policies.

i-tec®

one step forward

Global Visions

Web: GlobalVisionsInc.com
Email: sales@GlobalVisionsInc.com
Phone: 877-725-8869