



Front Desk — Security overview

The one-pager to hand your security team

Secure remote operations for field devices — kiosks, cash machines, signage, controllers, and embedded boards

The model: devices call out. Nothing calls in.

Devices make outbound TLS connections to Front Desk and wait for work. No inbound firewall rules, no port forwarding, no public VNC/SSH/RDP, no site-to-site VPN, and no permanent route into the customer network. When no session is active, there is nothing to connect to — the device never becomes a server.

Zero-trust posture

- **Devices authenticate** with per-device certificates and tokens — presence on a network is never trusted by itself
- **Users authenticate** through the portal; access is identity-bound, never shared-credential
- **Sessions are scoped** to one device, one purpose, and end when the work is done
- **Approval gates** are available per account — a customer contact can approve or deny each session before it starts
- **Everything is recorded**: who asked, for which device, when, and what happened

Transport and authorization

Every stream is carried over TLS and relayed through Front Desk's purpose-built streaming system — designed for responsive interactive sessions, multiple simultaneous streams per device, and per-stream authorization. Certificates and tokens govern authentication and authorization end to end.

What the customer network must allow

Outbound HTTPS and WebSocket to approved Front Desk domains. That is the whole request — no inbound rules, no address planning, no VPN project, and no change when the site's ISP or router changes.

Audit, including AI session review

Access attempts and sessions are logged with identity and scope. Accounts can also turn on AI session auditing: captured screen frames are reviewed against a plain-language policy the account writes, producing a written account of what the operator did — kept with the session record.

Beyond the standard posture

If your security policy requires more — specific key handling, network constraints, review workflows, or bespoke controls — Front Desk staff build custom security as engineering work, not as an exception.

THE PATH, END TO END

