

## Secure Device Management For Mission-Critical Access Control

XPressEntry Secure Device Management (SDM) gives security teams complete authority over their access control devices from the moment they are powered on. Designed for regulated, offline, and high-risk environments, SDM ensures every reader is trusted, locked down, and fully controlled without relying on cloud services, user accounts, or public certificate authorities.



## Benefits of Secure Device Management

### Secure QR-Based Provisioning

Enroll devices in minutes using QR codes that apply Wi-Fi, certificates, and apps automatically.

### Offline and On-Prem

Operates in isolated, firewalled, or disconnected environments without reliance on cloud services.

### Site-Controlled Device Trust

Only approved devices can join your system, with time-limited registration sessions and administrator approval.

### Remote Control and Recovery

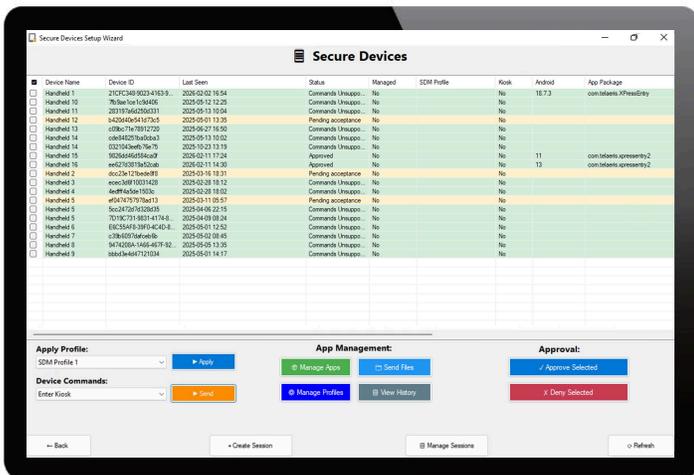
Reboot, wipe, reset, or reconfigure compatible devices instantly.

### Hardware Lockdown

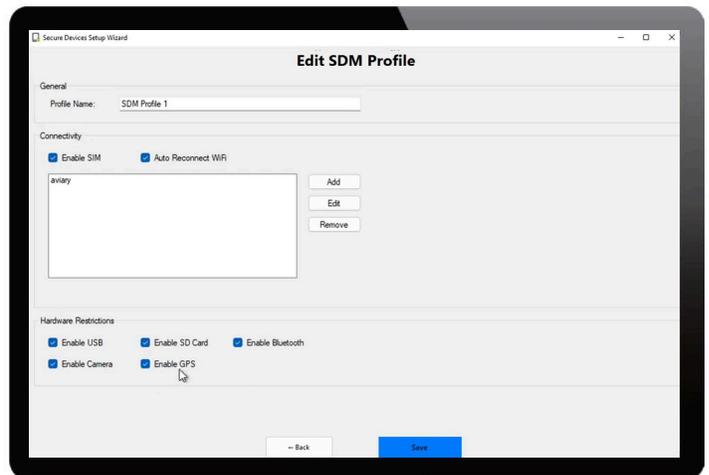
Lock devices into XPressEntry and disable USB, SIM, SD card, camera, and settings at the OS level.

### Purpose-Built for Physical Security

Designed for shared XPressEntry handhelds and critical infrastructure.



Manage apps, send commands, and view command history for multiple devices at once



Pre-configure device hardware and networking settings with SDM Profiles