Overcoming Network and Device Security Challenges in Government Facilities

Support mission-critical applications with custom connectivity solutions

USE CASE

Securing government facilities requires structural designs to prohibit unauthorized access to data, equipment, and documents. With that security come challenges in providing reliable wireless network coverage. The devices employees and contractors use in these sprawling facilities need to remain securely connected across thousands of square feet of warehouses, data centers, and offices—and be engineered to withstand harsh environments and resist tampering or malicious use.

CHALLENGE

With security as a prime directive for government agencies of all sizes, the facilities and buildings in which they operate have specific material requirements to thwart unauthorized access to the premises, both physically and virtually. This means many structures are designed with the use of complex corridor floor plans and reinforced concrete walls, resulting in the potential for radio frequency propagation issues on mobile networks and the need for costly broadband enterprise mesh Wi-Fi network management.

Additionally, the protection of sensitive data is paramount in these facilities, meaning the devices authorized for use by government employees and contractors must adhere to strict guidelines to ensure secure connectivity on its broadband and mobile networks. This includes proper tracking to restrict their use to specific mission-critical settings and controlling their operation at the hardware and firmware level to reduce risk of nefarious actors and to remove unwanted programs and applications.

SOLUTION

Governments are turning to Private LTE network deployment to better manage network connectivity when operating in challenging environments, such as large secure facilities and testing sites. As more departments implement this technology across their ecosystem, they require custom-built devices with SIM card or eSIM technology, authorized to operate on their network to keep their on-site employees and contractors informed and responsive. These security requirements often extend to devices, which need to be tamper-proof and programmed to prioritize authorized applications while simultaneously restricting access to others.

JACS Solutions Private LTE customizable tablets are purpose-built for use in environments where delivering secure wireless connectivity is challenging. The 4G LTE tablets are available in 8” or 10” display sizes and include features such as tamper-proof and transparent device casing, RFID and biometrics scanners and readers, and lock-down firmware to restrict application access.

809 Pinnacle Drive, Suite R
Linthicum Heights, MD 21090

443.718.4333
www.jacs-solutions.com