

Avi-on Security Overview

Avi-on is the most secure lighting control platform on the market today. The system is built to military-grade standards from the ground up. The platform has achieved the highest-level security rating ever granted by UL (1376 Diamond), across any system in any industry. The system is deployed in multiple military facilities, including buildings with classified areas. Below is a summary of the core elements of our security infrastructure.

AVI-ONBLUETOOTH MESH NETWORK

The mesh network was developed by Avi-on and uses fully encrypted communications on BLE advertising channels. Each building is commissioned with its own unique 128-bit AES security key for all communications. These communications cannot be read or generated by ordinary Bluetooth devices, applications, scanners, or even other Avi-on users without the proper credentials.

Access to tools and the network is secured by a cloud-managed email username and password, with SOC 2–compliant password complexity enforced. Admin and customer support personnel have stricter requirements, including higher security standards, timeouts, and password reset rules. All new user emails are validated before system access is granted.

The Bluetooth network stands alone and does not interface directly with any in-building networks. In addition, the mesh network cannot support or carry IP traffic. This means it cannot be hacked through, or used as a platform for hacking, any in-building Wi-Fi or Ethernet network.

While there have been reports of some Bluetooth security vulnerabilities, they do not apply to Avi-on's network because the software models required to exploit those vulnerabilities are not present on Avi-on devices.

Summary:

- All messages encrypted with AES 128–256
- Network keys never shared over the air (expiring token only)
- No IP traffic over the lighting system
- All BLE services that could support direct or remote attacks are removed
- No way to use standard BLE connection tools (e.g., phones, scanners) to communicate with devices
- Packet sniffing cannot reveal connection methods, message content, sender, or recipient
- Chipset configuration tools cannot update firmware
- Cloud passwords can be remotely reset at any time, instantly locking out users if needed
- Single Sign-On available, including existing integrations with Microsoft Azure military/government authentication systems

CLOUD SYSTEM AND REMOTE ACCESS

Avi-on supports optional remote access to provide enterprise visibility, data collection, remote commissioning, diagnostics, and remote control of the lighting system. The network can also operate fully offline with no internet or corporate Wi-Fi connection.

When remote access is enabled, the bridge connects over a Wi-Fi network to the Avi-on cloud REST API. It cannot serve as an access point to either the corporate network or the lighting system. Communications can also run over LTE cellular (with no corporate network connection), exclusively on the corporate LAN/WAN via Ethernet, or on the corporate network with built-in cellular backup.

- All access password-protected with secure email password reset
- All traffic encrypted via HTTPS; passwords use SHA-256 or stronger
- Bridge access passwords are unique and not available to users or the factory
- Only HTTPS ports are used (443, 53, 82, 83, 900, 5671, 5672); no other ports or libraries are enabled
- All communication occurs between encrypted APIs; no VPN required and compatible with standard corporate firewalls
- No external access possible to the bridge (e.g., no Telnet, SSH, or remote logins)
- Even with a password, local bridge access is restricted inside the network
- Single Sign-On available; system owners can control whether Avi-on personnel have access

WI-FI AND BLUETOOTH INTERFERENCE

Some users have asked about possible interference between Wi-Fi and Bluetooth Mesh communications. Avi-on systems have not experienced or caused interference due to the small size of messages and the use of BLE advertising channels, which do not overlap with Wi-Fi channels. This has been proven in real-world deployments, including:

- Avi-on replacing systems that experienced interference, resolving the issue
- Avi-on operating for 5 years on the CES show floor among tens of thousands of Wi-Fi and Bluetooth devices in high density without performance issues
- Avi-on systems running in buildings with more than 4,000 nodes in high density with no Wi-Fi interference

THIRD-PARTY TESTING AND COMPLIANCE

Avi-on routinely reviews and updates its security documentation, third-party certifications, and threat testing for every software release.

UL 1376

Avi-on selected UL for primary third-party certification because of the comprehensiveness of its evaluation. UL reviews not only passwords and general corporate security management, but also:

- Device security (hardware-level encryption)
- Network and inter-device security
- Secure data transmission over the internet
- Cloud infrastructure and security
- User roles and password management
- Security policy development, maintenance, escalation, and communication



This process is more comprehensive than SOC 2 and includes hands-on testing and intrusion attempts. UL awarded Avi-on its highest rating (Diamond)—a level no other system has achieved, nor come within two levels of.

NIST 800-171

This standard is the primary framework for evaluating security in U.S. military facilities. Like UL, it goes beyond basic corporate data security. Avi-on has passed full 800-171 security reviews by military agencies and is deployed inside facilities with classified areas, approved on corporate networks, and authorized for Avi-on mobile and web apps to be installed on controlled devices. A copy of Avi-on's NIST 800-171 filing is available under NDA.

Routine Third-Party Threat Testing

Avi-on uses multiple third-party vulnerability analysis providers appropriate to cloud, mobile, and device software. Threat analysis is triggered before every new release. The most recent reports are available under NDA and may be provided annually after installation to document compliance. Avi-on maintains documentation and resolution plans for any identified weaknesses, monitors security notices, and updates libraries with known vulnerabilities.

ALL PRODUCT, PRODUCT SPECIFICATIONS AND DATA ARE SUBJECT TO CHANGE WITHOUT NOTICE TO IMPROVE RELIABILITY, FUNCTION OR DESIGN OR OTHERWISE. The information contained herein is believed to be reliable. Avi-on makes no warranty, representation or guarantee regarding the information contained herein, the suitability of the products for any particular purpose, or the continuing production of any product. Avi-on assumes no responsibility or liability whatsoever for the use of the information contained herein. The information contained herein, or any use of such information does not grant, explicitly or implicitly, to any party any patent rights, licenses, or any other intellectual property rights, whether with regard to such information itself or anything described by such information.

