ATS Digital Security

Revision B

With any type of connected device, security concerns must be addressed to ensure that it continues to work as expected, reports accurate data, and remains impervious to third-party malicious attacks. All Traffic Solutions takes digital security very seriously. Numerous steps have been taken to ensure the integrity of our system, starting with the architecture itself.

Security at the Device

- ATS devices do not accept incoming connection requests from any web server (including ATS's own cloud servers). ATS devices initiate all web communication to known servers.
- All sign communications are secured with device-unique credentials following industry standard best practices.
- Communication payloads are encoded to prevent data snooping
- SSL encryption is enabled where supported. (some low power devices do not support SSL)
- Support access via SSH utilizes personalized keys, never simple username/password authentication.

Server Security

- All of ATS' user-facing sites use https to secure communication.
- Where possible, communication between systems is encrypted.
- All Data stored on ATS infrastructure (Microsoft Azure or AWS) is encrypted at rest.
- Data and systems are backed up following industry standard best practices.