All Traffic Solutions
Sign Security

In any remote environment, security concerns must be addressed to ensure that devices are working as expected, reporting accurate data, and are impervious to third-party attempts to hijack them for malicious use. All Traffic Solutions takes remote security very seriously. A number steps have been taken to ensure our devices stay secure, starting with the very architecture itself.

Security at the communication level:

- ATS devices do not accept communication from any server (including the ATS server). ATS devices are "send only", meaning they initialize all communications.
- All communications from devices are authenticated with device-specific credentials. These credentials conform to the industry standard complexity best practices.
- All communications from devices are encoded to prevent "data snooping".
- Where devices can support it, communication is encrypted with SSL (some lower-power 8-bit devices do not have this capability).
- Any communication for support purposes is done exclusively by using personalized SSH keys with access and never with 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.