Security Requirements

This article provides a summary of the security requirements necessary when using any of the Fire Station+ products (such as the Department Hub).

Domains and IP Addresses

The following domains used by Fire Station+

- hub.firestationsoftware.com
- id.firestationsoftware.com
- apparatus-checks.platform.firestationsoftware.com
- field-reports.firestationsoftware.com

The following IP addresses are used by Fire Station+

- 159.89.244.89
- 45.55.64.197
- 45.55.69.140
- 45.55.66.17
- 159.203.150.119
- 159.65.33.78

> This list is subject to change.

Certificate Trust

Fire Station+ uses HTTPS to encrypt data sent over the internet. The SSL certificate used to establish a trusted connection is distributed by Let's Encrypt. Your computer must include the ISRG Root X1 certificate as a trusted root CA certificate. This should be included automatically, under most circumstances.

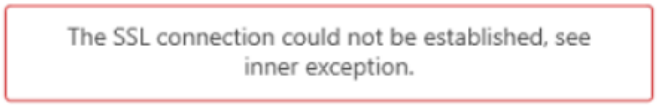
If you need to install this certificate, it can be downloaded using the following link:

https://letsencrypt.org/certs/isrgrootx1.pem

The SHA-1 fingerprint of this certificate is:

```
CA:BD:2A:79:A1:07:6A:31:F2:1D:25:36:35:CB:03:9D:43:29:A5:E8
```

If this certificate is not trusted you may see an error stating that "The SSL Connection could not be established".



TLS/HTTPS Requirements

Fire Station+ is compatible with TLS 1.2 or TLS 1.3 and supports the following ciphers.

- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-CHACHA20-POLY1305
- ECDHE-RSA-CHACHA20-POLY1305
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA384

Revision #1
Created 28 August 2024 18:45:22 by Wesley Naslund
Updated 29 August 2024 07:21:50 by Wesley Naslund