FTMaintenance Select SSL/TLS Certificate

SSL/TLS Certificate

Modern mobile operating systems like iOS and Android enforce strict HTTPS security policies. When your mobile app or browser attempts to connect to a secure site, it checks the server's SSL certificate against a list of trusted public Certificate Authorities (CAs).

To run the application reliably across all devices and browsers, you will need a valid SSL/TLS certificate issued by a trusted authority. Specifically, we recommend:

- A wildcard certificate covering your domain (e.g., *.yourcompany.com)
- Installation of this certificate on the workstation hosting the app, as well as on any devices that access it
- Optionally, using a free Let's Encrypt certificate for short-term or internal use

A trusted certificate ensures that:

- Your application works on both desktop and mobile
- Traffic is securely encrypted and trusted by the operating system
- You meet modern security standards and avoid browser or app warnings

A Note about Self-signed Certificates

A self-signed certificate is not issued by a trusted CA and is automatically rejected by mobile platforms. Unlike desktop browsers (such as Chrome or Edge), mobile systems do not allow users to bypass SSL warnings or proceed with untrusted connections, even if running behind the firewall, which causes secure connections from your mobile app or browser to fail.

On desktop systems, browsers allow you to manually trust a self-signed certificate, usually by clicking through an "Advanced" warning message. This flexibility is helpful for testing and production behind the firewall, but is not considered secure over the internet and is not permitted on mobile platforms. Mobile devices silently block untrusted connections for security reasons, with no override prompt available.

Please let us know if you'd like assistance purchasing or installing a valid certificate for your domain.