Encryption Support

> EG4xxx meters have full TLS 1.2 support.

Proxy-server HTTPS support

Legacy meters do not support encryption between the meter and proxy server. However, encryption may be supported between the proxy server and the client requesting data.

HTTPS Support and certificate validation

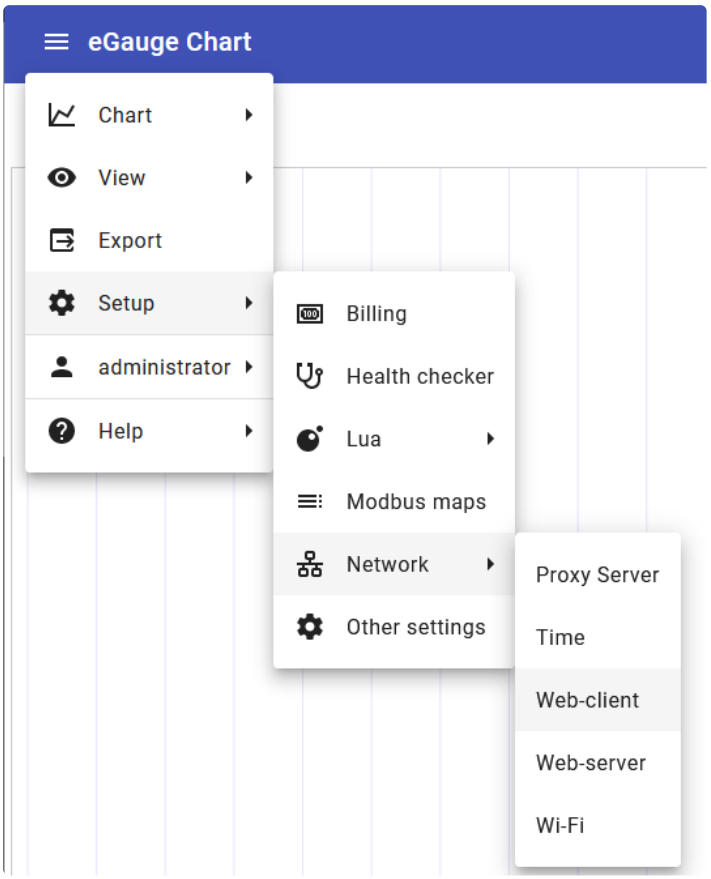
eGauge2 and EG30xx meters have limited TLS 1.1 encryption support. By default, on modern firmware, client-side (meter) initated HTTPS requests (such as Data Sharing or Alert Service to an HTTPS URL) will attempt to validate the HTTPS certificate before sending data. Due to the older SSL library used on legacy meters, some certificates may fail to validate even if they support TLS 1.1. This may include the eGuard Alert Service.

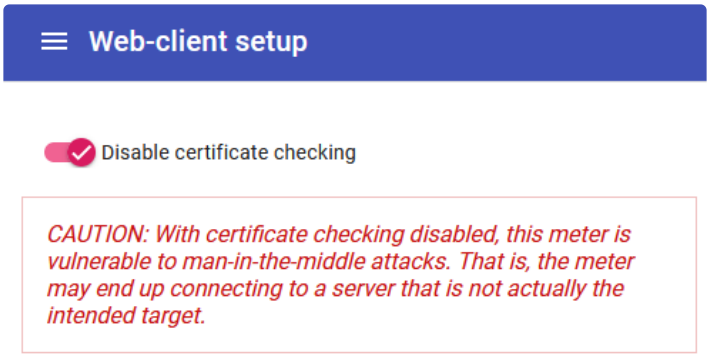
Disabling certificate validation

> Certificate validation must not be disabled if the information being sent is sensitive. Disabling certificate validation can allow for man-in-the-middle (MITM) attack if, for example, the local network the meter is using is compromised. The data will still be encrypted, but the meter will not be able to verify the destination's identity.

Beginning in firmware v4.5.5, The Modern Interface may be used to disable this certificate validation which can allow the meter to push data via HTTPS to certain services that support TLS 1.1 but which the meter cannot validate the certificate. To disable certificate validation, navigate to:

Setup → Network → Web-client, and toggle the "Disable certificate checking" option.





In addition, the WebAPI may be utilized to configure the certificate validation via the `/config/net/http/client/insecure` endpoint

---

Please visit kb.egauge.net for the most up-to-date documentation.