eGauge Proxy Server Security and Functionality

All metering data is stored locally on the meter hardware itself, the proxy server only acts as a relay between the internet and local meter interface to serve data remotely. The meter will have full functionality and no reduction in capacity if the meter is not connected to the eGauge proxy server or even the internet in general.

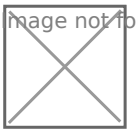
Accessing the meter via local network IP or hostname will show the same web interface as if visiting using the eGauge proxy server, for example https://eGaugeHQ.d.egauge.net or https://eGaugeHQ.egaug.es will show the same thing as if you were on the local network visiting the meter via IP address, such as https://192.168.1.102. For local IP or hostname access to work, you must be on the same local network as the meter.

egaug.es is an alias of d.egauge.net and may be used interchangeably.

Encrypted connections are supported on EG4xxx series meters. Legacy meters, such as the EG30xx and eGauge2 do not support an encrypted connection between the meter and proxy-server. However, if encryption is supported by the client browser, encrypted HTTPS may be used between the proxy-server URL and the client browser.

To disable the eGauge proxy server, navigate to Settings -> General Settings and set "Proxy-server hostname" to the number `0`. In this case, support services may be limited due to the meter not being available for remote troubleshooting and assistance.

Overview



The eGauge proxy server allows easy remote access to the eGauge webserver interface. Because the connection is established outbound from the device, usually no changes to the router or firewall are necessary.

The proxy server relays data stored on the eGauge meter to the client browser requesting it, and keeps the meter location and IP address anonymous. The client browser will see data coming from the eGauge proxy server, not the IP address of the eGauge device. All communication via the proxy is handled by the proxy, the client browser never directly communicates to the eGauge meter.

When an eGauge device is powered up, it connects to port 8082 (eGauge2/EG30xx, non-encrypted) and 8084 (EG4xxx, TLS 1.2 encrypted) of the server defined in the under **Settings -> General Settings -> Proxy-server hostname**. Normally, this is set to d.egauge.net but may be different for certain customers.

If the connection is successful, the device will be available remotely at http://**DEVNAME**.**PR0XY** (and https://**DEVNAME**.**PR0XY**/ if EG4xxx model or newer) where **DEVNAME** is the eGauge device name and **PR0XY** is the proxy-server hostname. For example, http://eGauge99999.d.egauge.net (or http://eGauge9999.egaug.es, as "egaug.es" is an alias for d.egauge.net).

If a device does not have a site-wide password enabled and is connected to d.egauge.net, it will become visible on the "Find my Device" page at egauge.net/eguard/find/. To be removed from this list, enable a site-wide password in the eGauge interface through **Settings -> Access Control -> Password-protect entire site**.

Disabling the proxy-server connection

If for any reason it is undesirable to maintain the proxy-server connection, “Proxy-server hostname” under **Settings -> General Settings** can be set to "0" (the number zero, without any quotes). Once this setting is saved and the device restarted, it will only be possible to connect to the eGauge device from the LAN or with port-forwarding configured on the router/firewall.

Security Considerations

If an eGauge device is available on the proxy server, anyone with the URL can attempt to access. If meter data is intended to be private, a site-wide password should be enabled as described in the previous section.

If remote administration is enabled on a user account ("Allowed to view all data and change settings from anywhere" access in **Settings -> Access Control**), the password must be secure enough to prevent brute-force attempts at cracking the password.

The proxy server uses a combination of hostname and private-public key authentication when meters connect. This ensures it is not possible for meters to be renamed and "overlap" with another, and ensures any connections to the proxy are authorized and commissioned by eGauge Systems.

HTTPS Access

> It is recommended to use up-to-date firmware as there are periodic releases with enhancements and bug fixes. Information on upgrading meter firmware can be found **here**.

The current line of meters (EG4xxx) support HTTPS access locally and via the proxy server.

Data transferred between EG4xxx meters and the proxy server are encrypted using TLS 1.2, and data between the web browser and proxy server is encrypted using TLS 1.3.

Local webserver access to EG4xxx provide TLS 1.2. EG4xxx meters can use a custom SSL certificate as well.

Local insecure HTTP access may be disabled via Settings -> Network Settings -> Disable unencrypted network services.

Legacy Model Meters

Legacy meters (eGauge2, EG30xx models) do not have encryption (HTTPS) available via the proxy server. Care should be taken when configuring passwords to ensure the local internet connection is not compromised. Credentials when used to save settings are not transmitted over plaintext or reversible as they use HTTP digest authentication.

Related Articles:

Network Connections
