Communication and Security

Technical Overview

Power System, Electrical, and Battery information from **Connect** (PC Service Application) and **Mobius** devices is communicated in binary format over port 80 (HTTP) back to our Enovate API residing on Enovate servers. All connections are initiated by the device (outbound), and an inbound connection cannot be initiated from Enovate's Cloud servers.

Enovate requires that the hospital's network allow connections to be made to Connect.MyEnovate.com, which currently resolves to 40.122.135.195.

No direct connections to the device can be initiated by Enovate. All remote management, updates, and diagnostic functions of Enovate devices are achieved through responses to the connection initiated by Mobius or Connect.

Mobius devices currently support the following Wireless security types:

- WEP
- WPA-Personal
- WPA-Enterprise*
- WPA2-Personal

*Including support for most networks using Radius authentication/authorization.

And the following encryption types (where applicable):

- TKIP
- AES

For networks that do not support or wish to use the above security protocols, **Connect** service for PC communicates back to Enovate using the wireless network the PC is connected to; no further configuration is required.

All information that is sent to Enovate that is used for diagnostic, reporting, and technical services is stored in a secure database that is not accessible to any third parties or applications besides Enovate. Customer device Information that is sent back to Enovate can be viewed in detail through Pulse Tech Web and Rhythm, Enovate's customer facing applications.

Please contact TechnicalServices@EnovateMedical.com for any further information.