Enlighted Security

The Enlighted system incorporates hardware devices, secure communications, user roles, and active monitoring and auditing.

Physical Security

The key information stored in a sensor cannot be retrieved by direct inspection of the persistent storage in the sensor or by tracing the execution logic. The on premise Enlighted Energy Manager is typically installed in a physically secure location, and the Enlighted wireless communication network is physically isolated from IT networks.

Onsite Network Security

All wired communication in the Enlighted system utilizes strong encryption techniques. The communication between the Energy Manager and Gateway utilizes SSL (TLS) encryption with 2048-bit certificates and SHA 256 Ciphers. HTTPS communication protocol is used between the Energy Manager and web clients.

Wireless Security

To prevent intrusion from external networks and being used as an intrusion point, the Enlighted Wireless network is isolated from all IT-managed networks. The Enlighted Energy Manager maintains a strict separation between the wireless network and any external, IT-managed networks. Enlighted wireless network traffic is never routed to the IT networks, and a host on the IT network can never communicate with sensors on the Enlighted wireless network.

In addition to isolation from IT networks, the Enlighted wireless network provides security against tampering through the wireless network. All Enlighted wireless network traffic is AES128 encrypted to prevent snooping and tampering. The commissioning process of the wireless network assigns a Network Key and Network ID. The value of both the Network Key and Network ID (as well as the wireless 802.15.4 channel) must be known to be able to communicate with commissioned devices in an Enlighted wireless network. Thus, it is not possible to take a commissioned sensor from one Enlighted wireless network where the Network ID and key are known and use it in another Enlighted wireless network where the Network ID and Key are not known. Additionally, the likelihood of tampering with the Enlighted wireless network is low due to the lack of availability of 802.15.4 interfaces for laptops and hand-held devices.

Multi-site Security

Enlighted supports large campuses consisting of multiple buildings and Energy Managers. These can be viewed and administered seamlessly at the campus level viewed via the Energy Manager. All communication between nodes uses SSL (TLS) or Secure Shell encryption. Communication between the Energy Manager and web clients is HTTPS. Further, on premise Energy Managers have the capability to connect the Enlighted system to the BMS for monitoring and advisory HVAC Control.