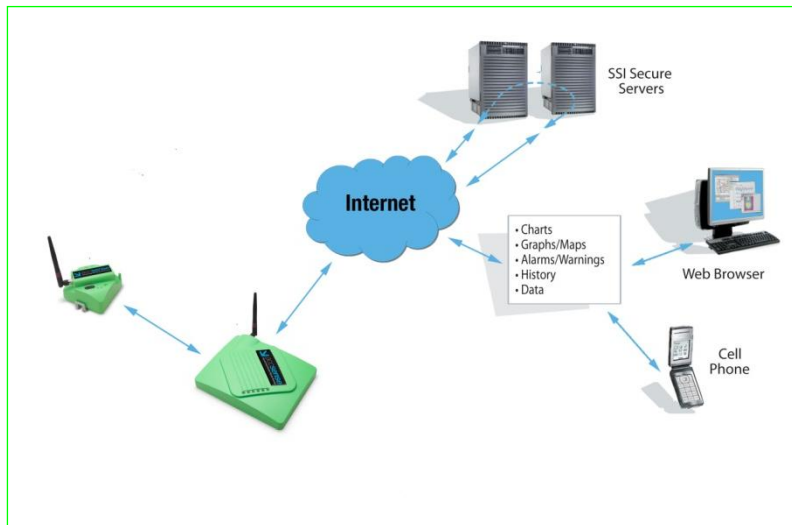


# Accsense Security Document

With the Accsense Monitoring Systems your data is always secure and the network is always protected. Accsense systems are designed with customer's data privacy, integrity, and network security as top priorities. This document explains how security has been implemented at every level of the Accsense system, including:

- 1) wireless communications
- 2) link between wireless and wired networks
- 3) internet communications



## 1. Wireless Communications

Accsense utilizes the IEEE 802.15.4 standard coupled with a proprietary protocol for wireless communication. The transmissions are 2.4 GHz, but transparent to, and will not interfere with, 802.11b/g (WiFi) networks. For additional information on wireless coexistence consult the Accsense Wireless Coexistence document.

When a system is first configured, each Sensor Pod is “bound” to a single gateway through a simple association procedure. During this process, the gateway and pod store each other’s serial numbers to memory, and then only communicate with each other. This is a similar concept to MAC address filtering in WiFi networks. In addition to the hardware address-based filtering, a Pod also acquires a unique network (PAN) ID and radio frequency channel (from the gateway) during the association process. The gateway will not accept data from another PAN ID or radio channel, resulting in a redundant binding between pod and gateway.

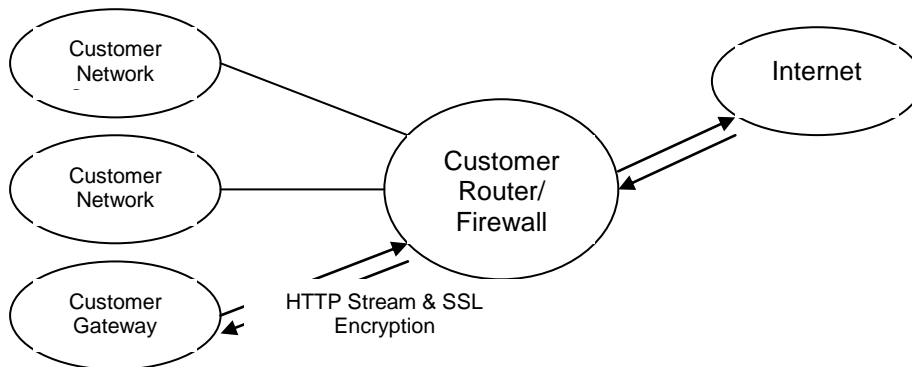
With the methods outlined above, mischievous exploits are nearly impossible. For example, for any faulty or fake data to be sent to the gateway, the attacker would have to ascertain obscure hardware, know the PAN ID, determine the channel, and know the serial number of the Pod— extremely difficult, if not impossible to accomplish. In addition, the attacker would have to synchronize transmissions perfectly with wireless communications which is asleep more than 99.9% of the time in order to conserve battery.



## 2. The link between the wireless and wired networks

A major point of concern for IT professionals is whether or not an attacker could leverage the Accsense wireless network to gain access to a wired network. The resounding answer is, "no." Within the gateway, the link between the wireless and wired networks is a single low bandwidth RS232 connection that is well controlled and secured. The serial connection links the two main processors of the gateway: One communicates with and controls the wireless network, referred to as the gateway Radio Control Module (GRCM), and the other receives/transmits data over the internet to the Accsense servers referred to as the gateway Host Processor (GHP). On the host processor side, this port is not configured to operate as a unix/linux console (no pseudo terminal access) and is controlled by a proprietary application written and maintained by Accsense. This proprietary application controls the GRCM using a proprietary console based protocol. This proprietary console based protocol would reject any malicious or unexpected code sent over the wireless and not allow it to pass onto the Ethernet.

## 3. Internet Communications



Communication from the Gateway to the Accsense secure servers utilizes the HTTPS protocol and only relies on an outbound connection over port 443. Because the communication between the gateway and servers is initiated from the gateway there is no need to open inbound ports on customer firewall. HTTPS over port 443 is a standard communications for secure Web traffic (e.g. credit card transactions).

Data sent over the Internet utilizes two forms of encryption:

- 1) SSL Encryption, the same "padlock" feature that many Web sites use to ensure Web purchases are secure.
- 2) Certificate Encryption, each gateway is issued a unique, digitally signed certificate that is associated with its serial number.

This ensures the highest level of security, as only devices with certificates containing this digital signature are permitted to connect to the Accsense servers. If a certificate is ever compromised, its unique signature can be revoked, making this virtually un-exploitable to system crackers. These two forms of encryption prevent security problems such as Denial of Service attacks. Secondly, they make it is virtually impossible to maliciously insert or spoof data - ensuring accurate data, every time

