Wireless Security Protocol

- We support WPA2-PSK (AES) and 802.1X authentication. Thermostats can connect using EAP-TLS using PKI (Certificate) or PEAP-MSCHAPv2 (Username and Password).
- We support IP v4 and IP v6 protocol.
- We support DHCP and Static IP Assignment.
- Thermostats will connect to visible and hidden SSID.
- Thermostat allows for post-installation modifications of certificates, usernames, and passwords.
- We support 802.11 a/b/g/n at 2.4 and 5 GHz.
- Traffic communicates using standard HTTP protocol over TCP port 80.
- Connections are made outbound eliminating the need to open external ports on the firewall.
- WPA3 Upgradable.

Range of Wireless Thermostats

- Thermostats have a typical laptop range. A wireless access point (WAP) will be needed every 2-3 classrooms.

Data Usage

- Each data transmission uses different sized data packets; most are larger than 100 bytes but less than 1K.
- Communication occurs on the set interval (typically 5 minutes) or on data changes at the thermostat (set point, mode, temperature). Changes via the online software do not cause communication to occur, but may add additional data to the transaction.

The Most Secure Wireless Solution

Our Thermostats initiate all communication directly to our cloud over standard HTTP ports with a small JSON message, and receive updates via the HTTP Response. There is NO inbound connection to each stat, we only respond with data to requests. Also, our thermostats have NO persistent connection to the outside cloud, keeping our devices secure. Lastly, there is no OS Kernel on our devices, so traditional viruses cannot run on our thermostats.

Wireless Network Considerations for additional security

- Thermostats can be places on separate VLAN to isolate traffic.
- Thermostats can connect to a hidden SSID.
- Set content filter to only communicate out to our cloud, preventing thermostats from ever attempting to communicate to a different cloud server.
- Configure devices for a static IP address, so customers can lock a secure VLAN to only include our thermostats.
- Configure a unique username and password with WPA2 Enterprise level security, which provides the customer maximum flexibility in controlling access via their AD controller.

Locally Hosting the EMS

- A virtual server would be set up onsite where the EMS app would be installed.
  Additional set-up and maintenance costs apply for this option.

*If thermostats fall offline they act as a locked programmable thermostat and execute the last program they received.