Corporate Network Security & ecobee WiFi Internet Connection

This document applies to both the ecobee Smart Thermostat and ecobee Energy Management System Thermostat. These devices operate the same way with regards to WiFi internet access and their connection to the ecobee web servers.

The ecobee corporate website and servers are located at Q9 Networks in Toronto, Canada. Q9 is the most secure data center in Canada and counts as its customers the leading Financial Institutions and Insurance Companies. Q9 has many security safeguards to ensure only authorized personal are permitted into the server area, such as bullet proof glass and finger print identification. Q9 has UPS and diesel generators to ensure no downtime during a power outage. All ecobee servers are protected in a locked cabinet only accessibleby a limited number of authorized ecobee employees. Only a small number of authorized ecobee employees can access the servers.

The ecobee thermostat supports WEP, WPA and WPA2 security for connecting to the WiFi network. Once the ecobee thermostat has joined the WiFi network, it initiates an SSL encrypted connection to the ecobee web servers. The SSL connection is protected using both certificate authentication and data encryption to ensure 'Man in the middle' attacks are not possible. SSL is the underlying protocol used to protect browser based HTTPS connections. Because the SSL connection is initiated by the ecobee thermostat, there are no open TCP or UDP ports on the unit. The only exception is the UDP echo port, which enables external devices to "ping" the ecobee thermostat, all other connection attempts are blocked.

The secure SSL connection does not use the standard TCP port 443, but instead uses TCP port 8089, this is to enable specific firewall rules to be created. Since the connection is being initiated by the ecobee thermostat the local firewall/router settings of the corporate network do not typically require any changes to support the product, because in most networks the port range of 8000-9000 is not blocked. However, in very secure environments, it maybe desirable for the corporate WiFi router and corporate firewall to be configured with policies that block all other traffic in or out of the WiFi router. The ecobee server connection is identified by a destination address/port of: ecobee.com TCP port 8089.

If corporate policy limits or restricts the use of WiFi networks, then it is also possible to add the WiFi router to its own network outside the internal corporate network, and either:

- use a separate internet service dedicated to ecobee or;
- place the WiFi router on the DMZ (demilitarized zone) side of the corporate firewall and create specific policies to permit the ecobee to create a connection to the ecobee web servers