Networking and security guide

sensi

Sensi thermostats are designed for installation in spaces to control traditional 24VAC controlled heating and cooling equipment - with the addition of a wireless interface for remote management.

SENSI RADIO

Sensi utilizes a 802.11n 2.4ghz radio. As such, it is recommended to use WPA2 PSK security (Open, WEP, and WPA-PSK encryption suites are also supported). While some enterprise wireless networks may be configured for these wireless security standards, WPA2-Enterprise (requiring 802.1X authentication processes) is commonly implemented in these environments and not supported by current Sensi hardware platforms. Each Sensi device utilizes DHCP for obtaining an IP address on the network. Please ensure this addressing requirement has been taken into consideration before connecting to the network.

GUEST NETWORKS OR OPEN NETWORKS

For security reasons, we discourage connecting your Sensi device to a network you know nothing about, and using someone else's network without their permission.

ENTERPRISE 802.1X/RADIUS NETWORKS

Sensi does not support common enterprise Wi-Fi implementations utilizing 802.1X. For these users, we recommend that you set up a dedicated Wi-Fi connection with WPA-2 Pre-Shared Key (PSK) security for your Sensi thermostats so your business data and your HVAC related data is completely isolated and consolidates IP address usage by the thermostats.

Reference http://www.ciscopress.com/articles/article.asp?p=1750205 for an overview of options for connecting non-802.1X devices to enterprise networks.

SENSI FIREWALL REQUIREMENTS

Sensi devices initiate communications with Sensi cloud services. These communications are outbound only to port 8091 (TCP) to our service cloud or port 8092 (UDP) for updates. Newer radios use port 80 and 443 for some updates. It is recommended to allow both of these outbound ports to be available. Response traffic varies on port usage.

SENSI SECURITY

We take measures to safeguard your system and to protect data. In order to provide you with Sensi capabilities and services, information is collected in accordance with our terms, available at https://sensicomfort.com/legal.
The Sensi clients - including the mobile apps and the web portals-use industry standard security (i.e. SSL).

WHITELISTING

For accounts with existing firewalls, it will be necessary to whitelist the following URLs for Sensi to operate effectively:

- ICDA.sensiapi.io
- ICDA.sensicomfort.com
- ICDA.fl33t.ninja
- Manager.sensicomfort.com

Additionally, please ensure that outbound TCP traffic via port 8091 can navigate any network firewalls, proxies, or filter devices.

SIGNAL STRENGTH

Test the Wi-Fi signal strength at the location of the thermostat. *You can download a free Wi-Fi Analyzer app to your phone to see what channel broadcasts the strongest in the area where you're standing. As a rule of thumb, we recommend ensuring your signal strength is over -70 dbs.*

3RD PARTY VETTING

Sensi complies to Emerson's comprehensive vetting process prior to the usage of any 3rd party service. This process ensures that full risk assessment is performed prior to any compatibility approval.

VULNERABILITY SCANNING

Sensi is in compliance with Emerson's Information Security policy on timely remediation of security vulnerabilities identified.

THREAT INTELLIGENCE MONITORING

Sensi utilizes Emerson's dedicated team for threat intelligence and vulnerability management to enable the product team to evaluate and respond quickly to any potential security vulnerability.

The scope of the technical and application information included in this article is necessarily limited and is subject to updates, without notice, as technologies and capabilities change.

EMERSON