



# IT, NETWORKING & SECURITY QUESTIONS WHITE PAPER

- What is SimplySnap?
- How does the SimplySnap solution work?
- Is the SimplySnap solution secure?



# WHAT IS SIMPLYSNAP? HOW DOES THE SIMPLYSNAP SOLUTION WORK?

Synapse Wireless' sustainability focus encompasses strategic and targeted solutions to enable organizations meet their corporate ESG goals by delivering actionable insights through the deployment of a wireless mesh, distributed, interoperable and modern cloud architecture integrating existing facility equipment and resources across multiple facilities or domains.

Synapse Wireless SimplySnap solution delivers facility insights, energy management, lighting management, HVAC air quality management, machine state, and material flow which ultimately enable organizations optimize resource management.

## Does SimplySnap reside on my corporate network? Can SimplySnap access corporate information?

SimplySnap creates its wireless, and isolated wireless mesh network (WMN) separate from corporate infrastructure. No access to corporate infrastructure is necessary for the SimplySnap solution to operate. To facilitate advanced functions and external access to services, a

SimplySnap hardware gateway controller should have external outgoing internet connectivity.

## What does a corporate IT department need to do to allow the SimplySnap solution to operate as intended?

Below is a description of each outbound connection to the cloud servers used by a Synapse gateway.

SERVICE	PORT	URI	DESCRIPTION
SSH	TCP 22	tunnel.snap-lighting.com	Provides Synapse Support Team command-line access into customer gateway for remote commissioning and troubleshooting. Can be Enabled/ Disabled by the customer.
NTP	UDP 123	ntp.ubuntu.com	Used to synchronize local clock on gateways.
ConfigSync	TCP 443	couchdb.simplysnapcloud.com	Used to synchronize configuration between Synapse gateways and cloud service.
VPN	UDP 1196	Vpn.simplysnapcloud.com	OpenVPN is used to push configuration to the gateways from the cloud service. Also allows administrator access to the Ui of each SimplySnap gateway from a single web domain.
MQTT	TCP 8883	A25n2uts2ytmw2-ats.iot.us-east-1.amazonaws.com	Used to communicate power and sensor data for SimplySnap connected devices to SimplySnap cloud service.

## **Do any changes need to be made corporate firewall settings?**

Generally, no changes have to be made to existing corporate network infrastructure. All connections are initiated from the gateway via a secure outbound connection to the SimplySnap cloud service, therefore no external connections can be established inbound. This prevents unauthorized access to the gateway from the outside.

## **Is SimplySnap hosted in the cloud?**

SimplySnap is a combined integrated hardware and software solution. We utilize AWS services. We selected AWS services due to reliability, scalability and robustness centered around a well-documented solution offering. More information is available at:

[https://aws.amazon.com/security/?nc1=f\\_cc](https://aws.amazon.com/security/?nc1=f_cc)

## **Does the SimplySnap system interfere with other wireless corporate networks?**

Our wireless technology incorporates the latest advancements in a secure, wireless architecture that was created to provide high-availability (HA) mitigating typical wireless congestion. Based on the industry standard of the IEEE 802.15.4 wireless protocol, our SNAP network easily coexists among other deployed IEEE based wireless protocols. More detailed information is available within the following document: "Synapse Wireless Solution: Wireless Co-existence", available directly from Synapse.

## **Where can I find more information about the SimplySnap cloud solution?**

More information regarding our holistic solution approach can be found on our website at:

<https://www.synapsewireless.com/>

## **Does Synapse maintain any corporate solution IT networking, security, or ISMS certifications?**

Yes, we are ISO27001 certified.

## **How does SimplySnap protect the integrity of the network?**

The SimplySnap architecture itself protects the mesh network integrity and prevents attack vectors from cloud to node through threat compartmentalization in each network segment. This protocol transition prevents IP-based attacks from progressing from the cloud to the nodes and preventing attack vectors on enterprise or collateral networks. More information related to network best practices can be found on our website at:

<https://help.synapsewireless.com/resources/best-practices/network-security.html>

## **Is SimplySnap secure? What encryption method does SimplySnap use?**

Our mesh network uses industry standard AES-128 symmetric encryption over 802.15.4 for RF communication from node-to-node and gateway-to-node. Gateways using SimplySnap Things Services employ WPA-PSK for Wi-Fi based connections and TLS 1.2 over Ethernet. Synapse IoT devices are capable of live Over-the-Air (OTA) updates from the gateway down to the node. This allows Synapse developers to respond to the latest cyber threats to push patches and configuration hardening on-demand.

### **Is the SimplySnap solution security audited by third parties?**

Synapse has a robust vulnerability analysis and hardening program as part of our DevSecOps development lifecycle. Our products go through rigorous external penetration testing as well as targeted vulnerability analysis of specific threat vectors by certified third-party security tool

### **Are there best practices associated with allowing a Synapse gateway to access the internet through an outbound connection?**

First, all connections are initiated from the gateway via a secure outbound connection to the SimplySnap cloud service, therefore no external connections need to be established inbound. This prevents unauthorized access to the gateway from the outside. Next, networking best practices suggest that all networking equipment be isolated whenever possible. Establishing the Synapse gateway on a dedicated VLAN is suggested from a networking administration perspective. Additional best practices suggest adding the Synapse controller within a dedicated DMZ.

### **Where can I find more information related to Synapse Wireless security philosophy?**

More information related to our security philosophy, methodologies and current security information can be found on our website:

<https://www.synapsewireless.com>

# SYNAPSE

6723 Odyssey Drive

Huntsville, AL 35806

(877) 982-7888

[synapsewireless.com](http://synapsewireless.com)