synapse

SIMPLYSNAP CLOUD

Connectivity Guide

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

WHAT IS SIMPLYSNAP CLOUD

SimplySnap Cloud is a remote management service for the SimplySnap platform. It enables authorized users to monitor, manage, and support one or more SimplySnap site controllers from a centralized web interface.

The SimplySnap platform continues to operate locally even if internet connectivity is unavailable. Schedules, occupancy control, daylight harvesting, scenes, and other lighting control functions are executed locally by the site controller and connected devices.

When connected to the internet, SimplySnap Cloud provides additional capabilities including:

- Remote system access
- Multi-site management
- Cloud-based backups
- Energy and power reporting
- Email notifications and alarms
- Remote commissioning and support
- Centralized user management

This document describes the network connectivity requirements, communication methods, and outbound services used by SimplySnap Cloud.

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. Can also be configured for local NTP.
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 443	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

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/

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 found on our website at: https://help.synapsewireless.com/resources/best-practices/network-security.html

Is SimplySnap secure? What encryption method does SimplySnap use?

SimplySnap uses industry-standard security technologies to protect communications across its wireless, local, and cloud-connected interfaces.

The SNAP wireless mesh network uses AES-128 encryption over IEEE 802.15.4 communications between the site controller and connected devices. Wi-Fi connections are secured using WPA2-PSK, while all web-based user interface and API communications are protected using TLS encryption over HTTPS.

SimplySnap implements role-based access control (RBAC), secure password storage, and supports LDAPS (LDAP over SSL) integration for enterprise authentication. Regular software updates and over-the-air (OTA) firmware updates help ensure systems remain secure and up to date.

Is the SimplySnap solution security audited by third parties?

Synapse has a robust vulnerability analysis and hardening program as part 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 Wireless
351 Electronics Blvd SW Suite D
Huntsville, Alabama 35824
synapsewireless.com