synapse

NETWORK SECURITY
RESOURCES

Network Security

SimplySNAP can provide all its basic lighting control services without an internet connection. However, many customers will find that internet or LAN connectivity provides additional functionality and benefits.

When connecting SimplySNAP to the internet or a LAN, the following information may be important to you and your IT team.

System Information

Physical Access

Security of the SimplySNAP system begins with physical security. The SimplySNAP site controller provides a recovery mechanism for resetting the default password and factory defaulting the entire system, so physical access to these buttons should be limited to authorized personnel only.

Software Updates

New features and security enhancements are provided in SimplySNAP software updates multiple times a year. Synapse recommends upgrading your system regularly to maintain a secure device.

Network Encryption

SimplySNAP uses commercial-grade, industry-standard encryption for all its network communications. Specific details are provided in the table below.

Interface	Encryption
802.11 b/g/n Wi-Fi Access Point, 2.4 GHz	WPA2-PSK
UI (over Wi-Fi or LAN)	HTTPS/TLS
802.15.4 Mesh, 2.4 Ghz	AES-128

Local Services

SimplySNAP offers several local connections to deliver its lighting control services:

- The SimplySNAP UI is delivered via a web interface. The UI is always available over the Wi-Fi server interface and can also be available from the LAN over the Ethernet

or Wi-Fi client interface. To provide the UI, the system must be able to receive inbound connections on TCP port 443 (HTTPS). SimplySNAP also accepts connections on TCP port 80 (HTTP) but will then automatically redirect to port 443.
- The SimplySNAP system will respond to ICMP echo (PING) requests.
- The SimplySNAP system will accept inbound SSH connections on TCP port 22. This connection is for Synapse internal use only and is not available for use by SimplySNAP customers.

Remote Services

SimplySNAP offers several services for internet-enabled installations:

- *SimplySnap Cloud Pro* is an optional service that allows a system administrator to access the UI of the SimplySNAP system via the internet.
- *Remote Troubleshooting and Upgrades* - Customer Support may occasionally need to perform remote troubleshooting or remote upgrades of the SimplySNAP system. The SimplySNAP system must be able to establish outbound connections to tunnel.snap-lighting.com on TCP port 22 for Customer Support to contact the system. In SimplySNAP 4.0 and later, this remote connection is enabled by default but can be disabled by the system administrator.
- *NTP* - the SimplySNAP system will attempt to sync its local clock to a Network Time Protocol (NTP) server by connecting to UDP port 123 to ntp.ubuntu.com. The NTP Server can also be configured to connect to a customer's NTP server.

User Authentication & Access Control

SimplySnap implements role-based access control for both UI and API interactions. Each user is issued unique credentials and assigned a role that enforces least-privilege access. Supported roles include:

- o Admin – full configuration and user management
- o Manager – operational control of devices and scenes
- o All Control – full lighting control only
- o Scene Control – ability to execute predefined scenes only

All passwords are stored using secure hashing and salting techniques. Password complexity policies enforce a minimum length of 8 characters. A 15-character minimum requirement is planned before the end of 2025.

Authentication mechanisms include HTTP Basic Authentication and Session Cookie Authentication. All authentication and data-in-transit uses TLS 1.3 to prevent credential interception and replay attacks. Enterprise identity provider integration (e.g., OpenID Connect for AD-based SSO) is planned before the end of 2025.

Physical Security

Default administrator and Wi-Fi passwords are printed on the site controller label for initial deployment. The site controller also includes hardware buttons to reset credentials or perform a factory default of the system. Because the device's hardware interfaces can alter or bypass access-control mechanisms, physical security of the site controller is critical. Only authorized personnel should have physical access to the device enclosure and cabling.

LAN Connectivity

If the SimplySNAP system is connected to an active Ethernet network, by default the system will attempt to retrieve an IPv4 address assignment using DHCP. You can determine which IP address is assigned via DHCP to the device by connecting to the Wi-Fi interface and viewing the Config page(s).

The recommended method for assigning an unchanging IP address to the system is to configure the DHCP server to always serve the same IP address to the system (for example, by using a DHCP host pool or address reservation in your router). For more information, please consult your router or DHCP server.

The Ethernet interface can also be configured with a static IP address, netmask, default gateway, and DNS server(s). A button is available on the side of the unit to factory default the entire system, including the Ethernet settings. For this reason, the physical security of the site controller is paramount.

When the SimplySNAP system is connected to a LAN, the user interface should be accessible to all devices on that LAN segment. The LAN can also be configured to isolate the SimplySNAP system on a separate LAN segment (typically referred to as a VLAN) that allows internet connectivity but limits access to/from other LAN segments. For information about how to configure the LAN in this manner, please consults your switch or router documentation. When the LAN is configured in this way, SimplySnap Cloud may be required to allow access to the UI of the system from devices on other segments of the LAN. The SimplySNAP system cannot accept tagged VLAN traffic and must receive traffic without 802.1q tags.

The Ethernet interface of the SimplySNAP system cannot be disabled. If a LAN connection is not desired, Synapse recommends not connecting an Ethernet cable to the system.

Wi-Fi Configuration

The 802.11 b/g/n 2.4 GHz Wi-Fi access point built into the SimplySNAP site controller provides a mechanism for delivering the UI without requiring wired Ethernet. If Ethernet is also connected, the SimplySNAP system will not allow traffic to be bridged in either direction between the Wi-Fi interface and the Ethernet interface.

The access point uses WPA2-PSK authentication. The Wi-Fi SSID and password are configurable. However, the SimplySNAP system does not support disabling SSID broadcast while leaving the Wi-Fi access point interface enabled. This Wi-Fi access point can be disabled. Synapse recommends disabling the Wi-Fi interface if Wi-Fi access is not required. However, disabling the Wi-Fi interface may make troubleshooting (ie, LAN connectivity) more difficult. The Wi-Fi interface can be configured in Client mode to connect to a local Wi-Fi network. When in client mode, users cannot connect to the Wi-Fi server.

Cellular Connectivity

The SimplySNAP system is available with an integrated Verizon LTE modem. The cellular interface provides IP connectivity in deployments where a wired LAN connection is unavailable or undesirable. When an active LAN connection is present on the Ethernet interface, the SimplySnap system prioritizes the LAN for communication and will not establish a cellular data session. The system does not bridge or route traffic between its LAN and cellular interfaces, keeping the two networks isolated. The cellular interface can be administratively disabled when not required. Cellular connectivity is included with the SimplySnap Cloud service; however, customers may choose to use LAN connectivity to the Cloud when that is preferred by their network policy.

SNAP Mesh Connectivity

The SimplySnap site controller communicates with wireless lighting controllers using SNAP, a self-forming and self-healing IEEE 802.15.4 mesh network operating in the 2.4 GHz ISM band. Transmit power varies based on radio hardware and selected channel and is restricted to CE-compliant levels within the EU. For a complete list of channels, see page 6.

The mesh network interface is required for proper lighting control system operation and cannot be disabled. By default, encryption is disabled on the mesh network to facilitate initial commissioning. After commissioning, all traffic on the SNAP mesh is encrypted with AES-128-CBC w/ CTS. Synapse strongly recommends enabling encryption on the mesh network once commissioning is complete.

Prevention of spoofing

For compatibility with existing/legacy controllers, SNAP does not include a message authentication code (MAC) to guard against spoofing.

Prevention of replay attacks

SimplySNAP uses an 8-bit sequence number in control messages to prevent replay and detect re-broadcasts. An upgrade to a 32-bit sequence number is planned for release before the end of 2025.

SNAP Channel Range

SNAP Channel	802.15.4 Channel	Frequency MHz
0	11	2405
1	12	2410
2	13	2415
3	14	2420
4	15	2425
5	16	2430
6	17	2435
7	14	2440
8	19	2445
9	20	2450
10	21	2455
11	22	2460
12	23	2465
13	24	2470
14*	25	2475

*SNAP transmit power is limited on channel 14