LSI Industries
AirLink Network Security

01/31/18

Best Practices

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

System Information

Physical Access

Security of the AirLink system begins with physical security. The AirLink 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 AirLink software updates multiple times a year. LSI recommends upgrading your system regularly to maintain a secure device.

Network Encryption

AirLink uses commercial-grade, industry-standard encryption for all of its network communication. In addition to this summary, further details are provided in the sections 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

AirLink™
enabled by Synapse®

Local Services

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

- The AirLink UI is delivered via a web interface. The UI is always available over the Wi-Fi interface, and can also be available from the LAN over the Ethernet interface (when connected). To provide the UI, the system must be able to receive inbound connections on TCP port 443 (HTTPS). AirLink also accepts connections on TCP port 80 (HTTP), but will then automatically redirect to port 443.
- The AirLink system will respond to ICMP echo (ping) requests.
- The AirLink system will accept inbound SSH connections on TCP port 22. This connection is for LSI internal use only and is not available for use by AirLink customers.
- The AirLink system will respond to DHCP requests on the Wi-Fi interface using UDP port 67.
- In AirLink 3.1 and later, the AirLink system will respond to DNS requests on the Wi-Fi interface using UDP port 53.
- The AirLink system is listening on TCP port 9999 but will only accept inbound connections from the ALRA server.
- In AirLink 4.0 and later, the AirLink system can accept connections from other AirLink site controllers on TCP ports 48625 and 48626.

Remote Services

AirLink offers several services for internet-enabled installations:

- AirLink Remote Access (ALRA) - ALRA is an optional service which allows a system administrator to access the UI of the AirLink system via the internet. The AirLink system must be able to establish outbound connections to vpn.AirLink.snaplighting.com on UDP port 1196 to connect to the remote access server.
- Email Notifications - AirLink can send notifications (also known as alarms or alerts) via email. The AirLink system must be able to establish outbound connections to TCP port 443 to connect to the email server.
- Remote Troubleshooting and Upgrades - LSI Wireless Customer Support may occasionally need to perform remote troubleshooting or remote upgrades of the AirLink system. The AirLink system must be able to establish outbound connections to tunnel.snap-lighting.com on TCP port 22 for LSI Wireless Customer Support to contact the system. In AirLink 4.0 and later, this remote connection is enabled by default but can be disabled by the system administrator.
- NTP - the AirLink system will attempt to sync its local clock to a Network Time Protocol (NTP) server by connecting to UDP port 123 on either ntp.ubuntu.com or time.nist.gov.

AirLink™
enabled by Synapse®

Passwords

- A "secure password" is long (at least 12 characters) and not easily guessed. (For example, don't use information like your name or birthday or anniversary.) A combination of letters, numbers, and symbols is recommended.
- AirLink versions prior to 3.3 have a single username and password. LSI recommends changing these values from the defaults to more secure values at the time of commissioning.
- In AirLink 3.3 and later, the system supports multiple users, each with their own password. LSI recommends changing the administrator password from the default to a more secure value at the time of commissioning. LSI also recommends creating secure passwords when each new user is created. AirLink 3.3 and later will enforce password complexity requirements.
- A button is available on the side of the unit to reset the administrator password. For more details on this operation, please consult the AirLink User Guide available at help.LSI-wireless.com/Lighting/. For this reason, physical security of the site controller is paramount.
- For site controllers manufactured with AirLink 4.0 and later, the default administrator password is printed on a label on the side of the unit. For site controllers manufactured prior to AirLink 4.0, the default administrator password is given in the AirLink User Guide.
- In AirLink 3.3 and later, the Wi-Fi SSID and password are configurable. LSI recommends changing the Wi-Fi password from the default to a new, secure value at the time of commissioning.
- For ALRA, LSI recommends changing the Wi-Fi password from the default to a new, secure value when you log in the first time.
- A button is available on the side of the unit to factory default the entire system, including the Wi-Fi password. For more details on this operation, please consult the AirLink User Guide. For this reason, physical security of the site controller is paramount.
- For site controllers manufactured with AirLink 4.0 and later, the default Wi-Fi password is printed on a label on the side of the unit. For site controllers manufactured prior to AirLink 4.0, the default Wi-Fi password is given in the AirLink User Guide.

LAN Connectivity

If the AirLink 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 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.

In AirLink 4.0 and later, 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 more details on this operation, please consult the AirLink User Guide. For this reason, physical security of the site controller is paramount.

When the AirLink 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 AirLink 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, ALRA may be required to allow access to the UI of the system from devices on other segments of the LAN. The AirLink system cannot accept tagged VLAN traffic and must receive traffic without 802.1q tags.

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

Wi-Fi Configuration

The 802.15.4 b/g/n 2.4 GHz Wi-Fi access point built into the AirLink site controller provides a mechanism for delivering the UI without requiring a LAN. If the LAN is also connected, the AirLink system will not allow traffic to be bridged in either direction between the Wi-Fi interface and the LAN interface.

The access point uses WPA2-PSK authentication. In AirLink 3.3 and later, the Wi-Fi SSID and password are configurable. However, the AirLink system does not support disabling SSID broadcast while leaving the Wi-Fi access point interface enabled. In AirLink 3.3 and later, this Wi-Fi access point can be disabled. LSI 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 AirLink system does not support using Wi-Fi in client mode to connect to an existing WLAN.

Cellular Connectivity

The AirLink system is available with an optional integrated Verizon cellular modem. This cell modem can provide the system an internet connection for situations where a LAN connection is not available or not desired. Although you can connect the system to a LAN via the Ethernet port, the system will not use the LAN unless a cellular connection cannot be established. If the LAN is also connected, the AirLink system will not allow traffic to be bridged in either direction between the cellular interface and the LAN interface; in addition, the system will prefer routing IP traffic to the cell network over the LAN network. If present, the cellular connection cannot be disabled on the AirLink system; however, the cellular interface will not be functional unless the device is activated on a Verizon data plan.

Mesh Connectivity

The AirLink site controller uses an 802.15.4 mesh network operating at 2.4 GHz to interact with the wireless lighting controllers in the system. The mesh network interface is required for proper lighting control system operation and cannot be disabled. For more details on selecting the proper mesh radio channel, please consult the AirLink User Guide. The mesh network is capable of using AES-128 for encrypting the mesh network. By default, encryption is disabled on the mesh network to facilitate initial commissioning. LSI strongly recommends enabling encryption on the mesh network once commissioning is complete.

AirLink™ enabled by Synapse®

Applications & Recommendations

Below you will find several sets of recommended network security best practices, depending on how the AirLink system is being used.

No internet connectivity desired

For a site without Internet access and where the benefits of cellular access do not outweigh the cost, AirLink can function stand-alone. At this type of site, all system management will be done locally via the system's Wi-Fi interface.

For this type of installation, LSI makes the following recommendations:

1. Install the device in a secure location that limits physical access to authorized personnel only. This location must also be suitable for the Wi-Fi network and the mesh network to operate.
2. Change the default administrator password at commissioning.
3. Change the default Wi-Fi password at commissioning.
4. Enable mesh encryption after commissioning.

Shared internet connection available

For sites with an internet-connected LAN where segmenting the LAN may be beyond the capability of the IT equipment or staff, AirLink can share the internet connection with other devices.

For this type of installation, LSI makes the following recommendations:

1. Install the device in a secure location that limits physical access to authorized personnel only. This location must also be suitable for the Wi-Fi network and the mesh network to operate.
2. Change the default administrator password at commissioning.
3. Change the default Wi-Fi password at commissioning (or disable Wi-Fi altogether).
4. If possible, configure the router or DHCP server to always assign the same IPv4 address to the AirLink system.
5. Subscribe to the desired internet-enabled services.
6. Enable mesh encryption after commissioning.
7. Disable remote troubleshooting connection after commissioning.

AirLink™
enabled by Synapse®

Internet access desired, limited LAN access required

Some sites may have an IT or network policy that does not allow devices to be installed onto existing LAN segments.

For this type of installation, LSI makes the following recommendations:

1. Install the device in a secure location that limits physical access to authorized personnel only. This location must also be suitable for the Wi-Fi network and the mesh network to operate.
2. Change the default administrator password at commissioning.
3. Change the default Wi-Fi password at commissioning (or disable Wi-Fi altogether).
4. Provision the LAN to create a separate segment (VLAN) for AirLink that allows outbound internet traffic only.
5. If possible, configure the router or DHCP server to always assign the same IPv4 address to the AirLink system.
6. If possible, configure the traffic filters between the existing LAN segment(s) and the new LAN segment to allow access to port 443 on the AirLink system.
7. Subscribe to the desired internet-enabled services.
8. Enable mesh encryption after commissioning.
9. Disable remote troubleshooting connection after commissioning.

Local access desired, internet access prohibited

Some sites may have an IT or network policy that does not allow devices on the LAN to connect to the internet.

For this type of installation, LSI makes the following recommendations:

1. Install the device in a secure location that limits physical access to authorized personnel only. This location must also be suitable for the Wi-Fi network and the mesh network to operate.
2. Change the default administrator password at commissioning.
3. Change the default Wi-Fi password at commissioning (or disable Wi-Fi altogether).
4. If desired or required, provision the LAN to create a separate segment (VLAN) for AirLink that allows outbound internet traffic only.
5. Then, if possible, configure the traffic filters between the existing LAN segment(s) and the new LAN segment to allow access to port 443 on the AirLink system.
6. If possible, configure the router or DHCP server to always assign the same IPv4 address to the AirLink system.
7. If required, configure the LAN to block all outbound connections from the AirLink system.
8. Enable mesh encryption after commissioning.

AirLink™
enabled by Synapse®

Internet access desired, LAN access prohibited

Some sites may have an IT or network policy that does not allow devices to be connected to the LAN in any way. Other sites may not have a LAN at all.

For this type of installation, LSI makes the following recommendations:

1. Purchase a AirLink site controller with an integrated Verizon cellular modem.
2. Activate the system's cell modem on your Verizon data plan.
3. Install the device in a secure location that limits physical access to authorized personnel only. This location must also be suitable for the Wi-Fi network and the mesh network to operate.
4. Change the default administrator password at commissioning.
5. Change the default Wi-Fi password at commissioning (or disable Wi-Fi altogether).
6. Enable mesh encryption after commissioning.
7. Disable remote troubleshooting connection after commissioning.

Other types of applications

For recommendations regarding other types of applications and installations, please contact LSI Wireless Customer Support.