# nLight® AIR Security Architecture

## nLight® AIR Security Architecture

The nLight AIR wireless lighting control platform is designed for use in both retrofit and new construction and for small to large indoor to outdoor applications. nLight AIR lighting controls can scale from controlling one room to an entire floor, from one floor to an entire building, and from one building to an entire campus.

The comprehensive integrated security architecture of nLight AIR provides security controls at all product levels from connected luminaires, system controller and physical/virtual infrastructure to cloud and mobile applications. The solution uses the following communications devices:

- Bluetooth® Low Energy (BLE) radio for connectivity with mobile devices
- 900 MHz radio to communicate with other nLight AIR devices
- nLight ECLYPSE™ System Controller uses IP (over WiFi and Ethernet), BLE and 900MHz for communication

### Overview

nLight AIR uses a 5-tiered security architecture. This architecture reflects comprehensive security specifications that integrate leading best practices to protect the entire solution, representing one of the lighting control industry's most comprehensive security architectures.

### Data Encryption

All data is encrypted before messages are transmitted. Additionally, nLight AIR uses multiple data encryption techniques to prevent unauthorized individuals from reading or modifying communicated messages.

1. The CL***AIR***ITY™ Pro mobile app uses the Elliptic-curve Diffie-Hellman protocol, an industry standard key agreement algorithm, to establish a secure channel with the nLight AIR enabled luminaires and devices.

## nLight® AIR 5-Tiered Security

1. **DATA ENCRYPTION**
   We protect not only the device, but the user data by leveraging standard algorithms.
2. **FIRMWARE PROTECTION**
   We verify the integrity of the software on the device.
3. **TAMPER-PROOF HARDWARE**
   We design our hardware to thwart extraction of data from the device by unauthorized users.
4. **AUTHENTICATED USER ACCESS**
   We make sure all users are authenticated within the relevant access levels.
5. **MUTUAL DEVICE AUTHENTICATION**
   We make sure only authenticated devices are part of the solution.

One Lithonia Way, Conyers, GA 30012 | Phone: 770.922.9000 | www.acuitybrands.com

2. The nLight AIR enabled luminaires and devices use AES encryption to secure communications over the 900MHz radio frequency. The encryption keys are unique for each site deployment, are programmed at the time of device commissioning and are protected within the secure hardware storage.

3. The nLight ECLYPSE™ system controller and CL***AIR***ITY™ Pro mobile app use Transport Layer Security (TLS) for all communications with the Acuity Brands® cloud resources. TLS provides state of the art encryption channels for devices to exchange information.

This multi-faceted approach to data encryption helps secure communication of all messages in the solution.

## Firmware Protection

nLight AIR enabled luminaires and devices utilize secure firmware which prevents the devices from loading programs introduced or modified by a threatening or malicious entity. Only authenticated, secured firmware authorized by Acuity Brands can be installed on these connected luminaires and devices. Additionally, the encrypted firmware protects against unauthorized access or removal of data, including configuration data, passwords and encryption keys help to maintain a stable, operational system.

## Tamper-Resistant Hardware Storage

Tamper-Resistant Hardware Storage protects the information stored within nLight AIR enabled luminaires and devices from access by unauthorized individuals. nLight AIR enabled luminaires and devices have secure hardware storage that protects information stored within it. Any attempts to bypass this feature will completely erase all data stored on the device.

## Authenticated User Access

This step verifies that all requests are from authorized users (either through the portal or mobile app) before allowing access to data stored on nLight AIR enabled luminaires and devices.

**Mobile Authentication:** Applications and datastores running in the nLight Air cloud support the mobile app to provide identity management, user permission and multi-device synchronization services.

**Cloud Authentication:** The nLight AIR solution utilizes a cloud infrastructure for managing site configuration and firmware updates using the CL***AIR***ITY Pro mobile app to verify authorized users. The cloud-connected CL***AIR***ITY Pro app's secured token authentication enables the communication of modifications in settings and operation with the luminaires and other devices installed at each specific site.

**System Controller Authentication:** The nLight ECLYPSE System controller supports RADIUS servers for authentication, allowing for the end-user's system administrator to centrally manage accounts and ensure compliance with password policies such as periodic password changes. Other measures to safeguard accounts include a requirement to change default credentials during the initial setup of the system controller. In addition, administrators can specify user roles (admin, user, viewer, etc.) to simplify access and account management.

The nLight ECLYPSE system controller complies with the requirements of FIPS (Federal Information Processing Standard) 140-2 Level 1, an encryption mode recommended by the U.S. Federal Government for enabling computer security. Therefore, it is strongly recommended to enable FIPS 140-2 mode, if required, before configuring the controllers on the project.

## nLight AIR Connected Architecture

| | Digital Lighting Network | System Controller | Cloud |
|---|---|---|---|
| **Encryption** | • Encrypted Firmware<br>• BLE & 900MHz Encryption<br>• CL***AIR***ITY Pro App Uses TLS 1.2 API Calls to Cloud | • Enables with FIPS 140-2 encryption mode before controller configuration<br>• Validated for Use by Federal Agencies | • TLS 1.2 API Mobile Calls<br>• AES & TLS Encrypted WebApps |
| **Authentication** | • Authenticated API calls<br>• Signed Firmware | • Authenticated Portal Access<br>• Signed Firmware | • Authenticated Portal Access<br>• Delegated Portal and Mobile App Access |
| **Access Controls*** | • Replay Attack Protection<br>• Hardware-Level Firmware Protection | • Supports Radius<br>• Role-Based Access<br>• Password-Policy Enforcement | • Ability to Revoke User Access<br>• Role-Based Access |
| **Multi-Tenancy** | • Not Applicable | • Not Applicable | • Full Multi-Tenancy<br>• Data Segmentation |

* Most access controls are configured and maintained by end customers. The overall security posture of a site will vary based on the implementation of those controls.

Figure 1

## Mutual Device Authentication

Mutual Device Authentication ensures that devices within the nLight AIR architecture have valid permission to interact with other network devices before exchanging any data. A device must receive a valid authentication token before it can communicate with the CL***AIR***ITY Pro App in the commissioning or device managing procedures. A valid key is required before any messages are processed by other connected luminaires or devices. nLight AIR enabled luminaires and devices exchange information securely which prevents common attackssuch as message replay and session hijacking.

## Pulling it All Together

Acuity Brands is fully committed to developing and maintaining secure products and has a robust Product Security Program in place. Through the security governance mode, we incorporate core security principles and best practices (see Figure 1 above) early into the product development lifecycle.

Our security governance policies include standards-derived policies, industry best practices and guidelines.

For more information, contact the Acuity Brands cybersecurity team.

www.AcuityBrands.com/PSIRT