AleoBlue security framework

Setting the standard for secure wireless control

aleoblue™

Commercial-grade lighting control demands more than just reliability — it requires uncompromising security to protect essential building infrastructure and sensitive applications. From office spaces to schools, hospitals, and industrial facilities, ensuring the security and integrity of wireless systems is critical to maintaining trust and operational continuity.

By leveraging global standards and government-grade measures, AleoBlue provides the trusted security framework demanded by today's connected lighting solutions. Built on transparency and proven technologies, it enables partners and users to adopt wireless control with confidence and peace of mind.

Bluetooth® NLC: the standard for wireless security

At the core of our wireless solution lies Bluetooth NLC, a globally recognized open standard with a transparent, proven, and rigorously tested security architecture. Developed collaboratively by leading technology companies within the Bluetooth SIG, the standard employs state-of-the-art security measures to protect devices and communication across lighting control networks.

Security by design

Bluetooth NLC embeds security into every layer of the system from the ground up, defining it as a core necessity. This approach safeguards the entire networking framework, from device provisioning to data transmission, against unauthorized access and interference.

Mandatory security features

In Bluetooth NLC, security is non-negotiable. Devices cannot achieve qualification without implementing the standard's full suite of security features, making trust and reliability a baseline for all compliant solutions. Insecure Bluetooth NLC networks simply cannot be set up.

Full transparency

Unlike proprietary systems, which commonly operate as black boxes with unclear security mechanisms, Bluetooth NLC offers a fully transparent and auditable security framework. Specifications are publicly available and can be reviewed by anyone. This allows third-party validation, ensuring trust and reliability while minimizing risks.

No known vulnerabilities

Introduced in 2017 as part of Bluetooth Mesh specifications, the Bluetooth NLC security framework has been extensively scrutinized by independent researchers. As of now, no known vulnerabilities exist, reflecting its robust design and long-term security focus.

Why transparency is key to security

With the transparency of open standards, any potential vulnerabilities can be identified and addressed before they are exploited. In the case of proprietary technologies, it is not impossible to determine whether a particular solution is really secure. At best, it can be stated that it has not been compromised so far. But only open standards receive the scrutiny and attention that is necessary for true security.

Bluetooth NLC security fundamentals

Below are the most important security mechanisms that safeguard wireless communication in Bluetooth NLC lighting control systems:

- **Encryption and authentication**
  All communications within a Bluetooth NLC network are encrypted and authenticated, preventing unauthorized access and eavesdropping.
- **Separation of concerns**
  The architecture separates roles and functions, assigning specific security keys for different purposes, such as provisioning, network operations, and application data. This limits the scope of potential attacks and ensures better security management.
- **Area isolation**
  Networks can be divided into subnets, each operating with its own security keys. Such isolation prevents potential vulnerabilities in one area from compromising the entire system.
- **Key refresh**
  Encryption keys are automatically updated to minimize the risk of long-term exposure.
- **Message obfuscation**
  Bluetooth NLC hides the source and destination of messages to protect their details. This prevents attackers from tracking devices and users while also preventing attacks based on network traffic analysis.
- **Replay attack protection**
  Message sequence counters (*Sequence Number* and *IV Index*) are used to detect and block replay attacks, ensuring that malicious actors cannot retransmit valid packets to disrupt the network.
- **Trashcan attack protection**
  Devices removed from a network do not receive refreshed security keys, preventing them from reconnecting without proper reauthorization. This mitigates risks associated with stolen or discarded devices.
- **Secure device provisioning**
  Devices are added to the network through a secure provisioning process, during which unique keys are assigned to each device without being transmitted over the air. This prevents rogue devices from infiltrating the network.

Data protection

From sensitive building details to extensive monitoring data, we manage a diverse range of critical resources that drive connected lighting systems. While secure wireless communication is critical to prevent network vulnerabilities, a comprehensive approach to data protection is equally vital for safeguarding the entire solution. In systems connected to the cloud via a gateway, data flows through multiple touchpoints, each requiring strict security protocols to ensure its integrity and confidentiality.

Encryption

All communication within the AleoBlue system (between the mobile app, devices, gateways, and the cloud interface) is fully encrypted. The minimum encryption level used for communication within a mesh network is 128-bit AES. For the highest level of encryption, our services use TLS 1.3. All TCP/IP communication is encrypted using the latest version of the TLS protocol, with a minimum encryption level of 128-bit AES.

The myth of secure wired controls

Contrary to common assumptions, wired lighting control systems often lack even the most basic security measures. Unlike Bluetooth NLC networks, where comprehensive encryption, authentication, and key management procedures are in place, wired systems frequently rely on physical access as their sole line of defense. Without encryption or access control, data transmitted over wired connections can be intercepted, manipulated, or disrupted. Once a physical breach occurs, such as tapping into a cable, the entire network can be compromised. In contrast, Bluetooth NLC systems implement multi-layered security protocols designed to protect against both physical and digital threats, making them not just comparable but often superior in terms of security.

Cloud infrastructure

All user and project data are stored in Amazon Web Services (AWS) infrastructure with the following security measures implemented:

- **Security Groups and Network Access Control Lists (NACLs)**
  Virtual firewalls and subnet-level filters control traffic to and from the cloud, providing intrusion prevention and stateless filtering.

- **VPC Flow Logs**
  Capturing and analyzing traffic patterns enables us to detect and mitigate potential security threats. We use Datadog to monitor and audit these logs in real time.

- **AWS Shield**
  A managed DDoS protection service safeguards applications running on AWS against flooding the server with superfluous requests in an attempt to overload the system.

- **Identity and Access Management (IAM)**
  Fine-grained access control ensures that only authorized users and processes can interact with AWS resources.

Data storage and server location

The physical location of the data center hosting all user and project data is Frankfurt, Germany. Data access requires proper authentication and occurs exclusively via encrypted communication channels. By adhering to strict data storage protocols and leveraging a trusted, EU-based server location, we ensure compliance with global data protection standards while maintaining secure and reliable access for authorized users.

Adherence to data privacy regulations

AleoBlue complies with the European Union's General Data Protection Regulation (GDPR), ensuring our solutions meet globally recognized standards for data privacy and user control. This includes offering users full transparency and control over their data, with secure procedures for account disabling and the ability to request the removal of personal and project data under the GDPR's *right to be forgotten*.

Access control

Ensuring that only authorized users can access systems, devices, and tools is a cornerstone of AleoBlue's security framework. Through effective authentication methods, reliable protection mechanisms, and clear access controls, we safeguard every interaction within our ecosystem. This layered approach ensures that access is granted only to verified users while preventing unauthorized attempts at every level.

User authentication

AleoBlue ensures secure user authentication through Auth0, a trusted and reliable identity management platform provided by Okta. Auth0 is GDPR-compliant, CSA STAR certified, and undergoes annual ISO 27001/27018 audits, ensuring the highest quality of provided services. Key protection mechanisms provided by Auth0 include:

- **Bot detection:** Monitors IP reputation by analyzing traffic quality to identify and block malicious bots.
- **Suspicious IP throttling:** Limits login attempts from suspicious IPs to prevent unauthorized access.
- **Brute-force protection:** Detects and blocks multiple login attempts from a single IP targeting specific accounts.
- **Breached password detection:** Identifies and prevents the use of passwords found in known data breaches.

AleoBlue does not use default users, roles, or permissions, ensuring that all access is securely configured throughout every interaction with the platform.

Secure network and application keys

AleoBlue protects mesh network and application keys by storing them securely within the platform. Such keys are accessible only to logged-in users, with strict controls ensuring that users with permissions for one project cannot access keys from other projects. API access is similarly segmented to maintain clear boundaries across projects and brands. As far as the mesh network is concerned, devices exchange network keys secured with individual device keys. The device keys are generated using the Diffie–Hellman key exchange protocol and are never transmitted over the air.

Role-based access control

AleoBlue employs role-based access control, assigning users specific roles with defined permission levels within each project. This ensures that sensitive actions are limited to authorized personnel only. Aligning permissions with user roles enhances security and operational efficiency, minimizing risks of accidental changes or unauthorized access.

Secure firmware distribution

AleoBlue ensures the secure delivery of firmware directly from our servers to partners' lighting components. The process is managed by our MaTE device, which guarantees that our firmware remains untampered, unmodifiable, and fully protected. We do not route firmware packages through external or third-party servers, ensuring maximum security and integrity of the distributed firmware.

AleoBlue security certificates and qualifications

Recognized for excellence in IoT security, the **ioXt certificate** validates our commitment to meeting the highest industry standards for device protection and secure communication.

Awarded for implementing best practices in platform security, **PSA L1 certification** demonstrates meeting rigorous requirements for securing connected systems.

DLC NLC5.1 qualification acknowledges our compliance with the stringent standards of the DesignLights Consortium, ensuring transparency, interoperability, and performance consistency across our solutions.

Security as a process

In today's connected world, security is not a one-time task but an ongoing commitment. Threat landscapes evolve, technologies advance, and user needs change — requiring a dynamic approach to maintaining and enhancing security. At AleoBlue, we view security as a continuous process, integrating proactive measures, regular updates, and a culture of vigilance to stay ahead of potential vulnerabilities. By treating security as a n evolving journey, we ensure our solutions remain resilient and reliable in the face of ever-changing challenges.

Real-time security monitoring

AleoBlue employs advanced analytical tools to continuously monitor servers, data sets, and network traffic. This proactive approach helps identify irregularities and detect suspicious activities in real time, ensuring immediate responses to potential threats.

Vulnerability Reporting Policy

Our Vulnerability Reporting Policy ensures quick and responsible handling of bugs and issues reported by partners, end users, or independent researchers. Once an issue is reported, we assess its severity, determine affected products, and work closely with the reporter to resolve it.

Internal security policies

Multiple internal policies are also in place to govern key aspects of security, including employee access to sensitive information, processing of personal data, internal password management, data backups, internal data encryption, or secure employee offboarding. This way, we protect ourselves against both internal and external risks that could potentially affect our systems, data, or devices.

Balance between security and ease-of-use

On our mission to deliver the best wireless lighting control experience in the industry, we constantly seek the perfect balance between ease of use and uncompromising security. While we take pride in the intuitive design of our commissioning tools, in the development process we always make sure that this convenience doesn't come at the expense of security. Through rigorous testing and thoughtful design, we strive to maintain this delicate equilibrium, providing tools that are both secure and easy to use.

If you have any questions regarding the security framework of AleoBlue, reach out to us at **support@aleolighting.com**.