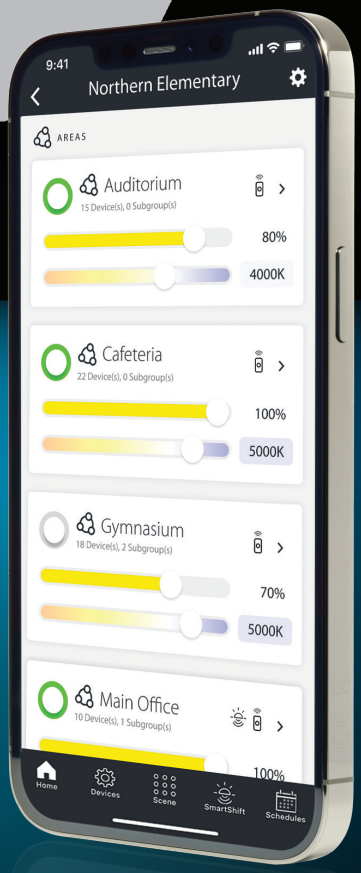
RAB

Lightcloud®



Lightcloud Blue | Security

Industrial-grade security in the palm of your hand.

Isolation

- Isolated from other networks
- Not affected by compromises to computer networks or dependent on utilizing existing IT infrastructure
- Only LCB devices are supported by the LC network – isolating it from interference and manipulation

Encryption

- End-to-end encryption (E2EE); If data were to be accessed, it would not be readable.
- That encryption remains whether it's between devices, cellular, or accessed via the web. Your data is always secure.

Restriction

- Every network uses its own keys, so a compromise would be isolated to a single location.
- Password best practices and two-factor authentication ensure individual users' passwords are secure and used only by the intended user.

Prevention

- Updates go through a rigorous evaluation period in an isolated environment before being released to devices.
- Evaluations include internal and external audits, keeping Lightcloud Blue security constantly ahead of any would-be intruders.

Protection Against…

Replay Attack - Attackers will try to "record" the activity within the network (e.g. *turn off* command), then "replay" the command by sending recorded messages to control the system. Lightcloud Blue uses a sequence number mechanism, so devices will ignore the duplicated messages (or message with lower sequence number) from the same original source.

Trashcan Attack - Attackers often collect the devices people throw away and extract its credential data. With Lightcloud Blue, when a device is deleted from the network, all credential data is erased. Additionally, each device has a unique "device key". Only with that key can a user/provisioner change the device's settings.

Tracking - Attackers will use trackers to gain access to a user's personal information (IP address, location, etc). Lightcloud Blue uses *obfuscation* technology, which means there is no plain text for source and destination addresses. The attacker cannot identify a node, even if it were using a network "sniffer".