LEADING THE FUTURE OF
LIGHTING + TECHNOLOGY

Emergency Light Test (ELT) System–Quiet and Secure

Bluetooth® mesh version (2.4 GHz)

The Emergency Light Test System is an automated, wireless, retrofit solution designed to simplify the testing and maintenance of emergency lighting systems. The system leverages a Bluetooth mesh wireless architecture and is both quiet and secure.

*Note: A 900 MHz non-mesh version will also be available early 2022.

Quiet

Emergency lighting tests can be scheduled to run outside of a building's normally occupied hours to minimize wireless traffic as well as visual disruptions to occupants. These tests are typically a 30-second monthly test, and one 90-minute test annually.

When the system is not actively conducting a test, the only data being transmitted is a "heartbeat" from the gateway once per minute which contains the time (for synchronization), followed by a status reply from each node. These messages are extremely small at approximately 50-60 bytes each.

Secure

Bluetooth mesh networking was designed with security as its number one priority and from the ground up. **Security in Bluetooth mesh networking is mandatory.** Key security features include:

- All Bluetooth mesh messages are encrypted and authenticated
- Replay and Trashcan Attack prevention
- Security key separation and refresh capabilities

For more information about Bluetooth mesh security, please visit:

https://www.bluetooth.com/blog/bluetooth-mesh-security-overview/

Additional FAQs

Bluetooth® mesh version (2.4 GHz)

Q: Is the system always sending data?
A: When no tests are being run, the only data transmitted is the once-per-minute "heartbeat" (described above). Manual tests are initiated by a single command from the gateway into the mesh; automatic tests are initiated by each node's internal clock (therefore no "start" command is sent from the gateway). When each node completes its test, it transmits the results to the gateway through the mesh.

Q: What security exists on the gateway?
A: The gateway initiates all connections to the cloud using MQTT over Transport Level Security (TLS).

- Only TLS 1.2 is supported; TLS 1.1 and 1.0 are not supported.

Server and client certificates are used for authentication.

- The gateway uses Amazon Root CA certificate.
- Local Certificate Authorities (CA) are not supported.

The web portal is the only service accepting inbound connections.

- The web application on the gateway does not communicate with anything on the internet, it's a self-contained system that runs solely on the gateway.

Access to the web portal is password protected.

- User passwords are hashed using the pbkdf2 sha256.

Q: Is the system connected to the internet? If so, how?
A: Yes, optionally. When the customer ops-in for data sharing the gateway connects to the EMC cloud using MQTT over a TCP/IP connection with TLS 1.2.

Q:If the mesh were compromised, would that allow access to my local network?
A: There is no access to the internet or the local network through the mesh, it is completely isolated.

Q: What happens if someone tries to hack into the system Over-the-Air (OTA) with malicious firmware?
A: The image is signed and must be validated by the application before it is flashed.

Q: What ports are being used for communication with the cloud?
A: (Outbound only) TCP 8883, 8443, 443.

Q: What happens if the gateway is unplugged and not plugged back in for a while?
A: After the gateway is powered back up, it will begin to receive the results from all of the nodes on the network. The node will store the last 12 monthly tests 10 annual tests and 10 events. This will take a while depending on the size of the network and the amount of traffic in and around the network.