Commercial Lighting Control System IT Implementation Guide

Athena and myRoom XC

Revision F   **26 July 2023**

LUTRON

Table of Contents

LUTRON

Lutron Security Statement

Lutron takes Cybersecurity very seriously. We vigorously monitor the threat landscape and take a proactive approach to security and privacy, continuously working to update and enhance our systems and processes.

At Lutron, we call our approach to cyber security "**Secure Lifecycle**," and we would like to present the following steps we take to protect your security and privacy:

- **Security by Design.** When building a new system, Lutron utilizes a dedicated security team to ensure best practices are implemented. Security is built in. It is not an afterthought or add-on.
- **Third-Party Validation.** Security is complicated. Lutron has a dedicated team of internal experts, we also leverage external experts to double- and triple-check our work and make security recommendations.
- **Continuous Monitoring and Improvements.** Security is a constantly moving target. Lutron uses a dedicated security team to continuously monitor the market for potential threats and, when needed, send out security patches to update installed systems.
- **Ongoing Support.** Lutron has the resources you need to answer questions about security when they arise.

We incorporate a variety of security features into our product designs. These features include recommendations from the National Institute of Standards and Technology (NIST) among others, and they are aimed at meeting our Secure Lifecycle protections. While we do not publish a comprehensive list of our security features, the following list is a small example of some of the techniques employed in our system design for Lutron Athena processors and associated services (such as mobile applications and cloud resources):

1. Secure and authenticated remote access with unique keys for every system's processor.
2. A secure hardware element ("chip") on every processor to guard the keys used for secure communication and authentication.
3. We are enforcing industry-standard encrypted communication and techniques for our integration protocols.
4. Secure commissioning – all communication between the system programming software tool/app and the processors is encrypted and authenticated. Programming a system requires permission to access that system.
5. Security updates pushed out automatically to the processors for urgent security patches.
6. Use of industry-standard techniques for integrations, such as OAuth2.0
7. Signed processor firmware to ensure a firmware update is authentically from Lutron.

If you have additional questions, feel free to reach out via our 24/7 Technical Support line at 1.844.LUTRON1 or email support@lutron.com.

Glossary and Abbreviations

DIN Rail System Panel – Pre-assembled and tested lighting control power panels that are configurable to control multiple load types. Panels are available in different sizes and panel types. System panels come with DPMs (DIN Power Modules) and a control equipment compartment that an Edge processor and power supply, and other low-voltage equipment can be installed into.

Edge Processor – This is the basic Lutron system controller supporting an embedded Linux operating system and will be the main system component connected to most networks. Each processor has two RJ45 female connectors – one for the LAN/VLAN connection and the other for serviceability. The two ports in the processor are connected internally via an unmanaged switch.

Lutron Wireless Processor – This is another processor option that supports communication between the Lutron system, 2.4 GHz Clear Connect – Type X devices such as Ketra wireless fixtures and lamps and 434 MHz Clear Connect – Type A devices such as Radio Powr Savr sensors. This controller is Ethernet connected and utilizes PoE (Power over Ethernet) for power. These processors may be powered by PoE switches included in the hub, by PoE injectors (provided by Lutron or customer-provided), or by customer-provided Ethernet PoE switches.

Clear Connect Gateway – Type X – This is an optional controller that supports communication between the Lutron system and 2.4 GHz Clear Connect - Type X devices such as Ketra wireless fixtures and lamps. This controller is required to be on the same network as the Lutron processor. This controller is Ethernet connected and utilizes PoE for power. These gateways may be powered by PoE switches included in the hub, by PoE injectors (provided by Lutron or customer-provided), or by customer-provided Ethernet PoE switches.

Hub – Metal enclosure containing one or more edge processors. Wall-mounted vertically and predominantly located in electrical closets. For example, the QP5 enclosure houses up to two Athena processors and a Lutron-provided 8-port unmanaged layer 2 network switch with PoE for connectivity. PoE is provided to power devices such as wireless processors and Lutron touchscreens.

Lutron Touchscreen – This is a wall-mounted digital control that manages system connected lights and shades through the Lutron processor. This device is required to be on the same network as the Lutron processor, but may be on a different subnet, if desired. It is Ethernet connected and utilizes PoE for power and communication. These touchscreens may be powered by PoE switches included in the hub, by PoE injectors (provided by Lutron or customer-provided), or by customer-provided Ethernet PoE switches.

Field Service Engineer (FSE) – Is a Lutron Services Company representative that is tasked with programming and commissioning a system.

Hospitality Technology Integrator (HTI) – Is a Lutron-certified company approved to program and commission a Lutron system.

LUTRON

Networking Overview

System Startup and Commissioning

For new system startup, electricians will need to interconnect the various hubs, processors, and gateways to create a standalone network prior to startup and commissioning of the system by the Field Service Engineer or Hospitality Technology Integrator (FSE or HTI). These interconnections utilize unmanaged PoE Ethernet switches, such as those contained in QP5 hubs. In typical applications Lutron processors and hubs are placed on their own LAN/VLAN. FSEs / HTIs can work with the customer's IT group to configure DHCP-provided IP addresses on each processor. The network must be capable of supporting IPV6 traffic, although IPV6 addresses do not need to be allocated via DHCP. Information on IP address requirements can be obtained from the FSE / HTI. Some system features require the processors to have Internet access, such as mobile app control.

For customers who do not wish to have unmanaged Ethernet switches on their network, customer-provided managed Ethernet switches may be used. Each processor and gateway shall have a single connection from the processor to the Ethernet switch. For Clear Connect gateways, wireless processors, and Lutron touchscreens in a system, an Ethernet switch supporting IEEE 802.3af or 802.3at is required to power them.

In a QP5 hub there may be two processors enclosed. While the edge processor has two Ethernet ports, the second port may not be used for daisy chaining to other processors. Edge processors with a single Ethernet port may also be present depending on the specification of your system. The Ethernet port should be used to connect the processor to the network, and every processor must have a dedicated Ethernet cable home run back to the switch.

When the customer-provided network becomes available for use with the lighting system, a transition from the network used for commissioning to the customer network can be scheduled and carried out, see "Commissioning Internet Connection" below for details. Because of this anticipated network transition, IP addresses set via DHCP are recommended. Refer to the firewall and routing table in this document for information on ports required for communication between the Lutron processors and Cloud connectivity.

Network Architecture Overview

The typical system network architecture contains edge or wireless processors, optional Clear Connect Gateways – Type X, Lutron touchscreens, and client devices (e.g., PC, laptop, tablet, mobile device, etc.).

The network architecture does NOT include the lighting actuators, sensors, and load controllers. This includes keypads, wired and wireless daylight sensors, wired and wireless occupancy sensors, load controllers, dimmers, switches, lighting panels, fluorescent lamp ballasts, or LED drivers. These devices communicate on a Lutron proprietary wired or wireless communication network.

Networking Overview *(continued)*

RF Considerations

While Lutron's Radio Powr Savr RF occupancy sensors, daylight sensors and Pico controls operate on a frequency outside of Wi-Fi, Clear Connect – Type X devices (e.g., wireless processors, gateways, and Ketra fixtures) operate in the 2.4 GHz band. 2.4 GHz Wi-Fi networks deployed on standard channels (1-6-11), or that operate in the 5 GHz band, will not interfere with communication between Clear Connect – Type X devices. There are five Clear Connect – Type X channels that are preferred for Lutron system deployment because they avoid or minimize interference from standard Wi-Fi channels; these will be used by default unless other requirements are communicated to the FSE/HTI.

- Channel 25 (2475 MHz)
- Channel 11 (2405 MHz)
- Channel 24 (2470 MHz)
- Channel 20 (2450 MHz)
- Channel 26 (2480 MHz)

Clear Connect Gateways – Type X and Lutron wireless processors should be kept at least 5 ft (1.5 m) away from 2.4 GHz Wi-Fi access points, routers, hotspots, or other devices communicating via 2.4 GHz Wi-Fi. Other Clear Connect – Type X devices should be kept at least 3 ft (1.0 m) away from 2.4 GHz Wi-Fi access points, routers, hotspots, or other devices communicating via 2.4 GHz Wi-Fi. myLutron users can access Lutron App Note #745 (P/N 048745) at www.lutron.com for further details.

Physical Medium

IEEE 802.3 Ethernet – The physical medium standard for the network between Lutron processors.

CAT5e – The minimum network wire specification of the Lutron LAN/VLAN.

IP Addressing

IPv4/IPv6 – The system requires communications and IP addressing over IPv4 and IPv6. Either static IP or DHCP can be used. DHCP for IPV4 addresses is the enabled default setting, but hard-coded IP addresses may be used if desired. Link Local IP addresses are not permitted to be used as static IP addresses. If a DHCP server is not present on the network, the processors will self-assign link-local IP addresses.

Class D addressing

Multicast addressing is used for two primary functions in a Lutron system: device discovery via mDNS and inter-processor communication utilizing multicast groups. Multicast traffic for mDNS discovery is always required. Multicast traffic for inter-processor communication may not be needed for newly-installed systems, but may have been utilized in previously-installed systems; check with the FSE/HTI for details. For systems that utilize multicast for inter-processor communications, this communication is required, and has the following properties:

- Each group of Lutron processors that need to share events will need a unique and common class D address. The class D multicast address can be field set by the FSE/HTI and specified by the customer.
- Any source multicast is used because any Lutron processor may be enacting the event.
- Multicast communication in the system is primarily event based (e.g., system trigger or change in state for monitoring). Polling is not a basis of communications in a Lutron system.

Latency Requirements for Managed Networks

Note that for managed networks, the maximum latency between any two processors should be less than 10 ms.

Communication Speed and Bandwidth

100 BaseT full duplex – Is the maximum link speed supported by the Lutron processor communications.

2 Mbps – Worst case bandwidth in a fully loaded system. Most systems include only 1 to 4 processors.

⁂LUTRON

Networking Overview *(continued)*

Other Protocols Supported

IGMP – Lutron systems support IGMP versions 1, 2, and 3 for multicast communication between the processors. Any possible flooding of multicast traffic can be constrained to a set of interested ports by using IGMP snooping.

mDNS – Multicast DNS is used by the Lutron design software, Lutron touchscreen and the Lutron mobile app to discover the processor and gateway devices. The processors and gateways will respond to any mDNS discovery requests sent by any compatible device. These responses are used to discover the IP address, version and other information required to allow the design software and mobile app to operate with the Lutron system. For proper system operation, mDNS must be routed through the entire subnet, both wired and wireless networks.

SSH/SCP – Secure Shell is used by both the Lutron design software and Lutron mobile app. The Lutron design software utilizes this protocol for database transfer and diagnostic log download from the processors and gateways. The mobile app utilizes this protocol for diagnostic log download only. Connections using this protocol can only be made by an authorized/paired device using the mobile app, or computer with the design software and current system configuration database.

TLS – Transport Layer Security is used specifically for external integration with the system. This is used by the Lutron mobile app to allow control of system devices. In addition, this is used by AV integration systems to make a connection to the processor/gateway device to allow control. Access to this is either certificate-based with approved vendors, or with custom username/passphrase logins. Custom logins may be configured by the FSE/HTI during system commissioning for approved integration partners. Lutron systems support TLS 1.2.

Telnet – a Lutron QSE-CI-NWK-E can be added to the system for Telnet AV integration. This device provides a RS232 or Telnet connection for system integration. For Telnet integration, the QSE-CI-NWK-E is not required to be connected to the same Network/VLAN as the Lutron processors. For limitations, see the QSE-CI-NWK-E specification submittal (P/N 369373) at www.lutron.com.

System Internet Connectivity

The Lutron system is enhanced when coupled with Internet connectivity. This connectivity provides the following enhancements:

1. Lutron App connectivity to the system for control, monitoring and reprogramming.
2. Automatic firmware updates of the processors.
3. Remote factory service options provided by Lutron.

A permanent network connection provided by the customer is recommended for Lutron systems to provide the processor with Internet connectivity.

If there is **no Internet connection provided** to the system, the following is true:

1. Local physical controls of the system will continue to operate as expected, and existing timeclock events will continue as scheduled.
2. The processor will not receive automatic firmware updates.
3. There will be no control or reprogramming of the system via the Lutron App.
4. Certain cloud based features such as DALI emergency testing and the Lutron dashboard will NOT be available.

Commissioning Internet Connection

During the startup of a Lutron system, an LTE modem may be provided by Lutron to facilitate ease of commissioning by Lutron Field Service Engineers or Hospitality Technology Integrators (FSE or HTI). This device may be installed by the electrical contractor as part of the system. The modem will not be used to connect any non-Lutron components to the Internet. This LTE modem will be removed or deactivated by the Lutron FSE or HTI within 30 days of the end of jobsite startup.

If the customer network is already up and running when a Lutron FSE or HTI is scheduled for startup, the temporary LTE modem will not be used.

Networking Overview *(continued)*
Internet/Cloud Services and Mobile App Connectivity

- DNS Resolution
  - The processor will use the IT-specified DNS server to resolve IP addresses to access Internet connected services. The DNS server's IP address can be set either manually by the Lutron FSE or HTI or via DHCP.

- Internet connectivity test
  - The processor will ping public DNS servers to verify Internet connectivity:
    - 8.8.4.4, 8.8.8.8, 208.67.220.220, 208.67.222.222, 209.244.0.3, 209.244.0.4
  - The processor will also attempt to make an HTTP connection to www.google.com

- Time Sync
  - The processor will reach out to the below list of Internet time servers. NTP is used to allow accurate execution of automatic timeclock and other scheduled events. In the event that a time server is not available, the clock on the processor is set during system programming and is retained during power outages. When Internet connectivity is available, the processors will reach out to time.iot.lutron.io, which may resolve to one or more of the following NTP servers:
    - 0.pool.ntp.org, 1.pool.ntp.org, 2.pool.ntp.org 3.pool.ntp.org, 0.north-america.pool.ntp.org

- Automatic Firmware Updates
  - The processor will attempt automatic firmware upgrades by establishing an HTTPS connection to firmwareupdates.lutron.com which may resolve to one or more s3.amazonaws.com addresses.
  - This feature is enabled by default but can be disabled by the FSE or HTI during system commissioning.

- Cloud Connectivity
  - The optional Lutron mobile app is available on iOS and Android mobile devices. This app is typically used by facility managers and lighting designers to allow control of lighting loads including Ketra color selection and window shade position. The app will also allow creation and editing of timeclock events, scene editing and renaming of areas. In the mobile app, Floors and Rooms are presented to users in a tree format, allowing access to control all of the lighting and shade zones in each area.
  - Use of the mobile app requires that a myLutron cloud-based account be created, which is then paired to the processors. If more than one user will need to access the system via the app, each user will need to create a myLutron cloud-based account, and the original account holder will need to share access with the new users. Shared access can be set for a limited time or indefinitely, or revoked at any time.
  - Initial setup of the app requires the mobile device to be on the same subnet as the processors so that discovery and secure authentication can be performed. Following initial setup of the mobile app, the mobile device will no longer be required to be on the same network.
  - The mobile app requires a connection to Lutron's cloud services to control the system. The app-to-processor communication connects to Lutron's cloud services as defined in the "Mobile App, Internet, and Cloud Connectivity Features" section in this document.
  - Device-login.lutron.com & *.iot.*.amazonaws.com are used for cloud connectivity.
  - All cloud connectivity functions utilize outbound connections only. Both the processor hardware and the mobile app originate connections to the cloud servers to exchange messages. No inbound connections are made from the cloud server to the processor.

LUTRON

Firewall/Routing Requirements

Required for System Startup and Programming

These ports are used for system startup and database transfer to processors and gateways. After the system has been started up these ports may be closed if desired. If changes to the system need to be made, these ports will need to be re-opened to allow upload of programming changes to the system.

Source	Destination	Port	Protocol	Description
Commissioning Device [1]	224.0.0.251	5353	UDP IPv4 Multicast	mDNS is utilized for processor discovery and initial configuration
All Edge and Wireless Processors and Clear Connect Gateways – Type X	224.0.0.251	5353	UDP IPv4 Multicast	This is the mDNS discovery response sent from the processor/gateway back to the Lutron configuration software
Commissioning Device [1]	All Edge and Wireless Processors and Clear Connect Gateways – Type X	8083 8081	TCP IPv4/IPv6	These ports are used to configure processors and enable integration with third-party equipment through the Lutron API (LEAP)
Commissioning Device [1]	All Edge and Wireless Processors and Clear Connect Gateways – Type X	22	TCP IPv4	Used for database transfer, support file generation and diagnostics
Commissioning Device [1]	Sqltofb.lutron.com Firmwareupdates.lutron.com	443	TCP IPv4/IPv6	Allows Lutron software to obtain the latest processor firmware
Commissioning Device [1]	All Edge and Wireless Processors and Clear Connect Gateways – Type X	51023	TCP IPv4/IPv6	Unicast communication between design software and processors
Commissioning Device [1]	Lutron Touchscreens	8080	TCP IPv4	Touchscreen diagnostics

Required for System Runtime

These ports are required for system runtime, and must remain open for system functionality.

Source	Destination	Port	Protocol	Description
All Edge and Wireless Processors and Clear Connect Gateways – Type X	Multicast Address of the system (239.0.38.1 – 239.0.38.xx) [2]	2056-3055	UDP IPv4 Multicast	Used to share events and status of lights between the processors and gateways. Only needed if system is configured for inter-processor communication via multicast.
All Edge and Wireless Processors and Clear Connect Gateways – Type X	All Edge and Wireless Processors and Clear Connect Gateways – Type X	443	TCP IPv4/IPv6	Used to share events and status of lights between the processors and gateways.
Lutron Touchscreen	224.0.0.251	5353	UDP IPV4 Multicast	mDNS is utilized for edge processor discovery by the Athena touchscreen
Lutron Touchscreen, Lutron Mobile App, and API Integrations	All Edge and Wireless Processors and Clear Connect Gateways – Type X	8083 8081	TCP IPv4	These ports are used to communicate between the processors and Lutron touchscreens, Lutron mobile app, and/or API integrations

1 The commissioning device is the IP address of the computer used to commission the Lutron system. This is typically a laptop operated by the Lutron FSE/HTI during system startup.
2 Multicast addresses by the system will be configured by the FSE/HTI during system startup.

Firewall/Routing Requirements (continued)

Optional Features and Functions

These are optional feature ports used for integration and are outbound from the Lutron processor only.

Source	Destination	Port	Protocol	Description
AV Integration System IP	IP Address of QSE-CI-NWK	23	TCP IPv4	For integration systems which utilize Telnet, an NWK is the only means for Telnet integration to Athena
API Integration Device	IP Address of the Lutron Processor	8083 8081	TCP IPv4/IPv6	For third-party external integration with a processor via TLS

Mobile App, Internet and Cloud Connectivity Features

These ports are used for various cloud, app, and Internet connectivity functions.

Source	Destination	Port	Protocol	Description
Mobile Device on Local Processor Network	224.0.0.251	5353	UDP IPv4 Multicast	mDNS is utilized for processor discovery during setup and system pairing
Mobile Device on Local Processor Network	All Edge and Wireless Processors and Clear Connect Gateways – Type X	8083 8081	TCP IPv4/IPv6	Lutron mobile app authentication and configuration
Mobile Device on Local Processor Network	All Edge and Wireless Processors and Clear Connect Gateways – Type X	22	TCP IPv4	SSH is used for support file generation and diagnostics
All Edge and Wireless Processors and Clear Connect Gateways – Type X	*.iot.*.amazonaws.com	8883	TCP IPv4/IPv6	Lutron Cloud connectivity for mobile app runtime on network other than processor network. The destination address can be dynamic based on region. For example, it could look like: a32jcyk7azp7b5-ats.iot.us-east-1.amazonaws.com
All Edge and Wireless Processors and Clear Connect Gateways – Type X	firmwareupdates.lutron.com	443	TCP IPv4/IPv6	Used for automatic firmware upgrades, may resolve to one or more s3.amazonaws.com addresses
All Edge and Wireless Processors and Clear Connect Gateways – Type X	Device-login.lutron.com	443	TCP IPv4/IPv6	Device Registration and secure processor remote access
All Edge and Wireless Processors and Clear Connect Gateways – Type X	8.8.4.4 208.67.220.220 209.244.0.3 209.244.0.4 8.8.8.8 208.67.222.222	ICMP	ICMP	Processor Internet connectivity check
All Edge and Wireless Processors and Clear Connect Gateways – Type X	google.com	80	TCP IPv4/IPv6	Processor Internet connectivity check
All Edge and Wireless Processors and Clear Connect Gateways – Type X	Customer Specified DNS Server	53	UDP IPv4/IPv6	DNS resolution is required for cloud connectivity and NTP time sync
All Edge and Wireless Processors and Clear Connect Gateways – Type X	0.pool.ntp.org 1.pool.ntp.org 2.pool.ntp.org 3.pool.ntp.org 0.north-america.pool.ntp.org time.iot.lutron.io	123	UDP IPv4	NTP is used for automatic time sync which allows time based events to trigger accurately
All Edge and Wireless Processors and Clear Connect Gateways – Type X	.iot.lutron.io	443	TCP IPv4/IPv6	Connectivity for Cloud based functionality

⁂LUTRON

Firewall/Routing Requirements (continued)

Guestroom Integrations with CELS, PMS and SMS[1]

Source	Destination	Port[2]	Protocol	Description
Guestroom Processor (Static IP)	Hotel Integration Appliance (Static IP)	5001-5003	TCP	These ports are used to communicate events from the guestroom processor to hotel integration appliance
Hotel Integration Appliance (Static IP)	PMS Server	9002	TCP	Events sent between the PMS server and the Lutron system
Hotel Integration Appliance (Static IP)	CELS Server	7000	TCP	Events sent between the CELS server and the Lutron system
Hotel Integration Appliance (Static IP)	SMS Cloud Service	442	HTTPS	Events sent between the SMS cloud service server and the Lutron system

Key:

PMS: Property managment system
SMS: Service management system
CELS: Central electronic locking system

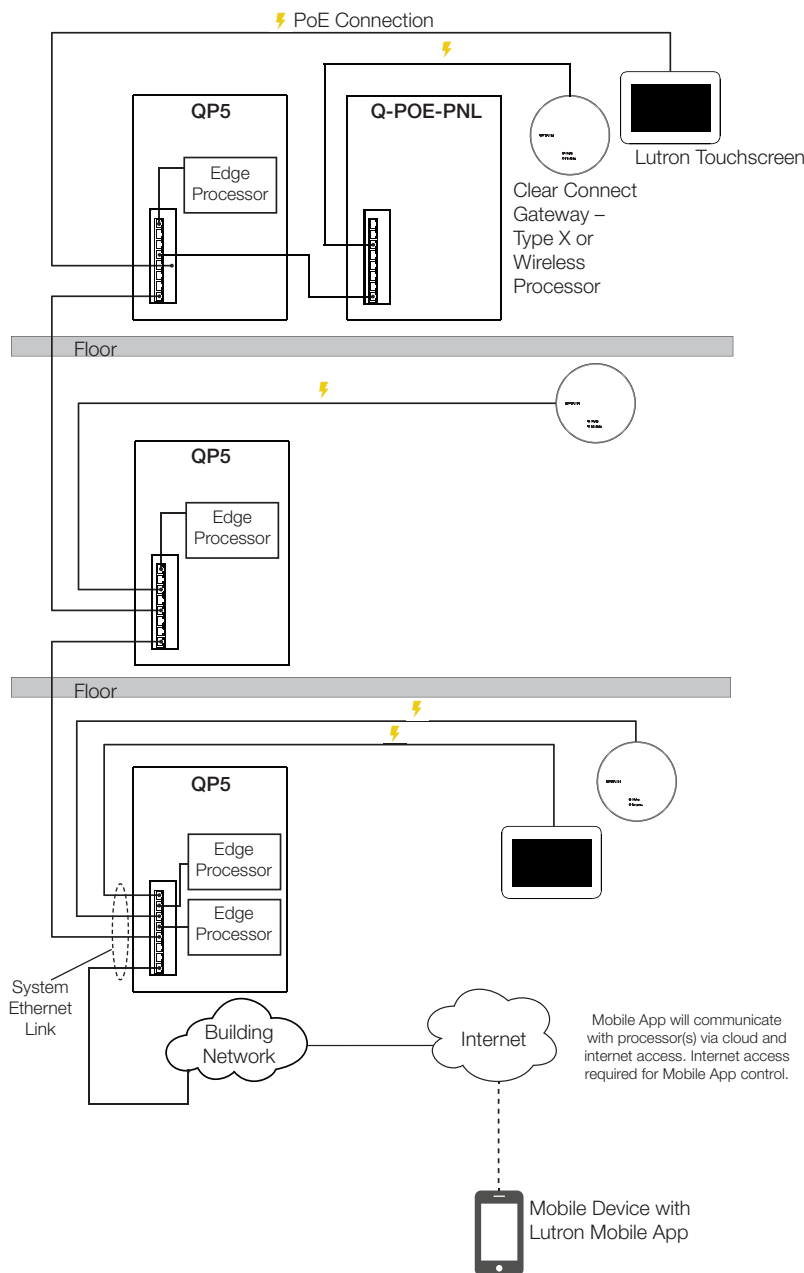1 This section only applies to the myRoom XC guestroom systems.
2 These port numbers are the defaults but may be set to other values during system configuration on-site. If configured differently, those ports will be provided by the commissioning agent and are required to be open between endpoints.

Configuration Examples

The following diagrams depict some of the various configurations of a Lutron system.

Athena System Deployment Utilizing Built-in Unmanaged Ethernet Switches

This diagram shows the system Ethernet link interconnections between hubs using built-in unmanaged Ethernet switches, which may be included in QP5 enclosures. The interconnected panels are then connected to the building's IT network, allowing the edge and wireless processors, Clear Connect Gateways – Type X and Lutron touchscreens to communicate to the Internet and the Lutron mobile app. Each edge processor may contain two RJ45 Ethernet jacks, which should not be used for daisy chaining (the second port is used for FSE/HTI diagnostics).
Each processor shall have a single connection to an Ethernet switch.
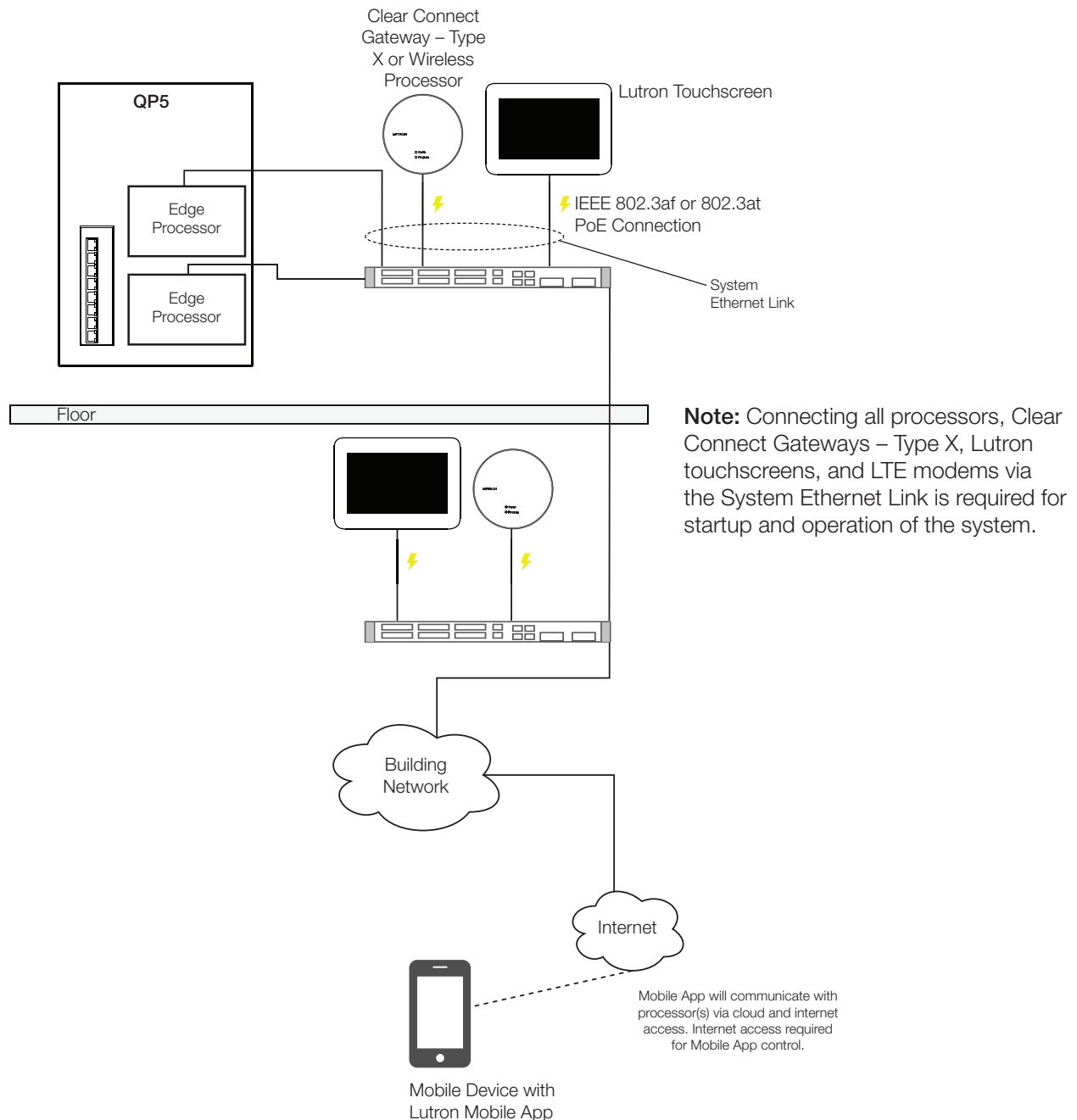

Note: Connecting all processors, Clear Connect Gateways – Type X, Lutron touchscreens, and LTE modems via the system Ethernet link is required for startup and operation of the system.

Configuration Examples (continued)

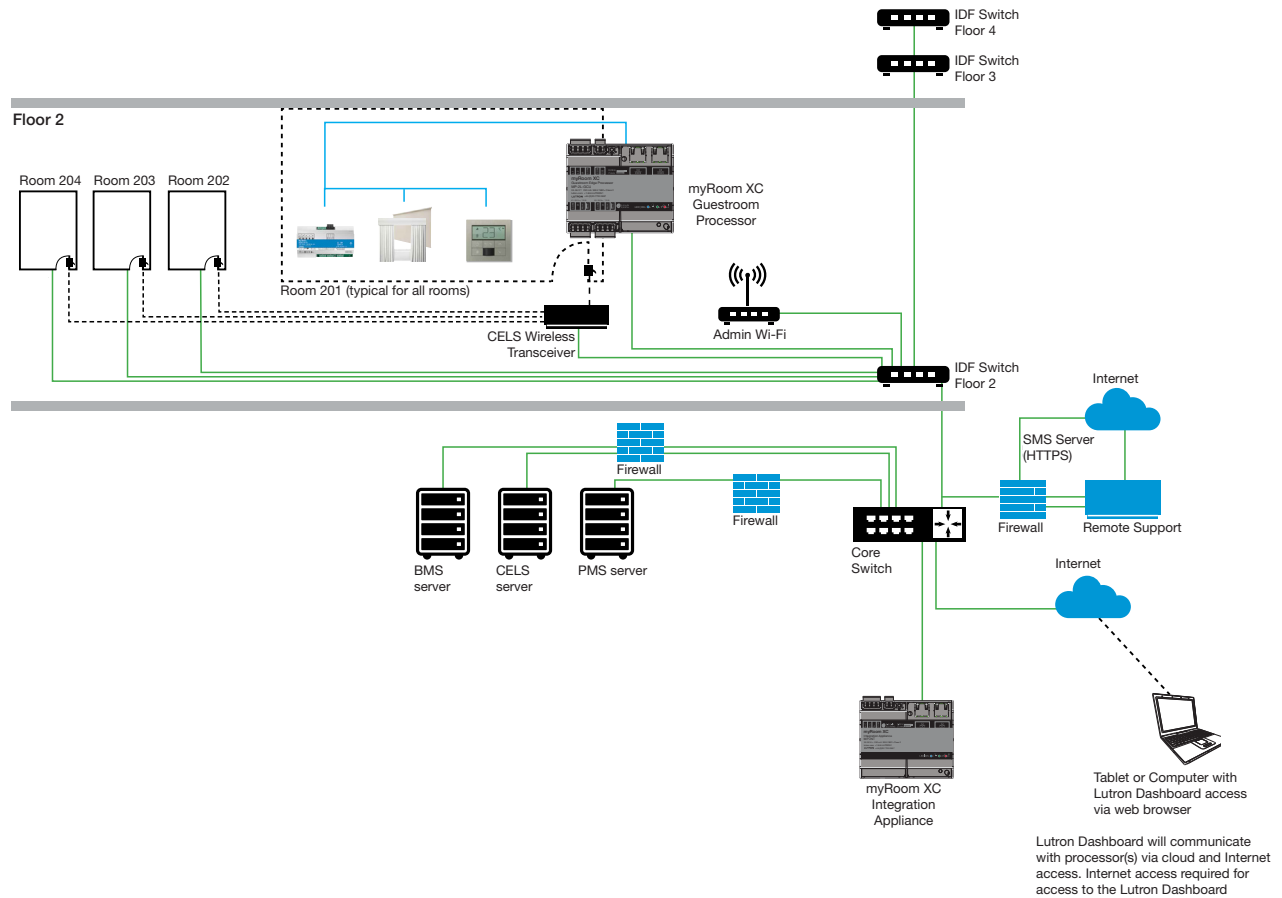## Athena System Deployment Utilizing Customer-Provided PoE Ethernet Switches

This digram shows the use of customer-provided Ethernet switches to connect processors to the building network infrastructure for the system Ethernet link. In this example the wireless processors, Clear Connect Gateways–Type X and Lutron touchscreens are powered from the customer-provided PoE switch. Each edge processor may contain two RJ45 Ethernet jacks, which should not be used for daisy-chaining (the second port is used for FSE / HTI diagnostics). Each processor shall have a single connection to an Ethernet switch.

Note: Connecting all processors, Clear Connect Gateways – Type X, Lutron touchscreens, and LTE modems via the System Ethernet Link is required for startup and operation of the system.

Mobile App will communicate with processor(s) via cloud and internet access. Internet access required for Mobile App control.

Configuration Examples (continued)

myRoom XC Guestroom System Deployment

This digram shows the use of customer-provided Ethernet switches to connect processors to the building network infrastructure for the system Ethernet link. Each edge processor may contain two RJ45 Ethernet jacks, which should not be used for daisy chaining (the second port is used for FSE/HTI diagnostics). Each processor shall have a single connection to an Ethernet switch.

Key

Wiring

- - - - Wireless doorlock link
——— Network link (Ethernet)
——— QS wired link

PMS: Property managment system
SMS: Service management system
CELS: Central electronic locking system

LUTRON

Customer Assistance

If you have questions concerning the installation or operation of this product, call the Lutron Customer Assistance.

Please provide the exact model number when calling.
Model number can be found on the product packaging.
Example: PJ2-2B-GWH-L01

U.S.A., Canada, and the Caribbean: 1.844.LUTRON1
Other countries call: +1.610.282.3800
Fax: +1.610.282.1243

Visit us on the web at www.lutron.com

☀ **LUTRON**

Lutron Electronics Co., Inc.
7200 Suter Road
Coopersburg, PA 18036 USA