

Commercial Lighting Control System IT Implementation Guide

Athena and myRoom XC

Revision L

27 March 2026



Table of Contents

Security Statement	4
Introduction	
Glossary and Abbreviations	5
Networking Overview	
System Startup and Commissioning	7
Network Architecture Overview	7
RF Considerations	8
Physical Medium	8
IP Addressing	8
Class D Addressing	8
Latency Requirements for Managed Networks	8
Communication Speed and Bandwidth	9
Other Protocols Supported	9
System Internet Connectivity	10
Internet/Cloud Services and Mobile App Connectivity	12
Single Sign On (SSO)	14
Firewall/Routing Requirements	15
Configuration Examples	
Athena System Deployment Utilizing Built-in Unmanaged Ethernet Switches	20
Athena System Deployment Utilizing Customer-Provided PoE Ethernet Switches	21
myRoom XC Guestroom System Deployment	22
Network Diagram	
Connected Mode	
Athena System During Startup/Maintenance	23
Athena System During Runtime	24
myRoom XC System During Startup/Maintenance	25
myRoom XC System During Runtime	26
Server Mode	
Athena System During Startup/Maintenance	27
Athena System During Runtime	28
myRoom XC System During Startup/Maintenance	29
myRoom XC System During Runtime	30
Networked	
Athena System During Startup/Maintenance	31
Athena System During Runtime	32

Table of Contents *(continued)*

Ethernet Cable Wiring Diagram

Connected Mode

Athena System During Startup without Building Network.33
Athena System During Startup/Maintenance with Building Network (Option 1).34
Athena System During Startup/Maintenance with Building Network (Option 2a)35
Athena System During Startup/Maintenance with Building Network (Option 2b: with QP5-2L-POE-EM)36
Athena System During Startup/Maintenance with Building Network (Option 3).37
Athena System During Startup/Maintenance with Building Network (Option 4).38

Server Mode

Athena System During Startup without Building Network.39
Athena System During Startup/Maintenance with Building Network (Option 1).40
Athena System During Startup/Maintenance with Building Network (Option 2a)41
Athena System During Startup/Maintenance with Building Network (Option 2b: with QP5-2L-POE-EM)42

Server Mode Setup Overview

Purpose of Server Installer43
Installer Files43

Pre-requisites for Server Installer

IT Checklist.44
Infrastructure and VM Preparation45
Network Ports45
Domain Name and Certificate Requirements46
Identity Provider (IDP)47
SMTP Server Configuration (Optional)47
Administrative Access48
Copy Installation File48
Finalize and Share Checklist with FSE48

Revision History49
-----------------------------------	-----

Customer Assistance49
--------------------------------------	-----

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 system-server or system-cloud communication with unique keys for every system.
2. A secure hardware element (“chip”) on all processors to guard the keys used for secure communication and authentication.
3. Enforcing industry-standard encrypted communication and techniques for our integration protocols to the highest extent possible. Any integrated third-party components or systems should be evaluated independently.
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. Lutron is committed to one year of security support from system start-up date.
See lutron.com/security for updated details on support periods. Internet-connected systems can be configured to update automatically.
6. Use of industry-standard techniques for identity-based 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.

SOC2 report available upon request.

Introduction

Cybersecurity is a dynamic field that is always evolving. If you have any questions about this document or need additional information, contact your local Lutron sales representative.

Glossary and Abbreviations

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. This controller is required to be on the same network as other Lutron processors.

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 required to be on the same network as other Lutron processors. 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 – Type X Gateway – 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 other Lutron processors. 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.

Introduction *(continued)*

Glossary and Abbreviations *(continued)*

Server Mode – This deployment option includes a customer-managed server that allows access to the Lutron dashboard. The dashboard is hosted on a customer-supplied server (on premise or VM), must run Windows/Ubuntu, and typically resides on the same network as other Lutron processors.

Connected Mode – This is a cloud-based service provided by Lutron to host and access the Lutron dashboard, providing the most up-to-date feature set and automatic updates.

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.¹ 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 edge 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 the **Commissioning Internet Connection** section for a transition to using Lutron dashboard connected mode or **Commissioning Server Mode Connection** section for transition to using Lutron dashboard server mode. 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 – Type X Gateways, 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.

¹In a scenario where only IPv4 is supported, static IP must be used.

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 – Type X Gateways 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 IPv6.¹ 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.

¹In a scenario where only IPv4 is supported, static IP must be used.

Networking Overview *(continued)*

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.

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 to operate with the Lutron system. For proper system operation, mDNS must be routed through the entire subnet, both wired and wireless networks.

SFTP - Secure File Transfer Protocol is used by the Lutron design software for database transfer and diagnostic log download from the processors and gateways. Connections using this protocol can only be made by a 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 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

Networking Overview *(continued)*

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.
4. Monitoring and reporting via the Lutron dashboard.

A permanent network connection provided by the customer is recommended for Lutron systems to provide the processor with Internet connectivity. The Lutron system can support forwarding proxies if desired by the customer. The connection requires a mutual TLS connection between the processor and the cloud.

Full Internet Connection to Lutron Cloud (Connected mode)

When the processor has Internet access to the Lutron cloud, all cloud-connected features are available, including app connectivity, automatic firmware updates, remote factory service, and dashboard monitoring/reporting.

Local Server Connection Without Internet Access (Server mode)

If the system is connected to a customer-provided local server, the processor will not be able to reach the Lutron cloud. In this case:

1. Local physical controls of the system will continue to operate as expected, and existing timeclock events will continue as scheduled.
2. Communication with the local server may remain available, subject to the server and network configuration.
3. Firmware updates are performed manually and when available.
4. There will be no control or reprogramming of the system via the Lutron App.
5. Remote service options provided by Lutron will not be available.
6. Certain features will only be available with the Lutron dashboard connected mode and not server mode.

No Internet Connection nor Server Provided (Networked)

If there is no Internet connection nor any server 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. All cloud-based features and the Lutron dashboard will not be available.

Networking Overview *(continued)*

System Internet Connectivity *(continued)*

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.

Commissioning Server Mode Connection

During initial setup of a Lutron system, the customer-managed server may not yet be available. In this case, the Lutron FSE may proceed by commissioning the system in standalone mode (without a server connection nor LTE modem). Once the customer server and supporting network infrastructure are in place, the Lutron FSE can follow the procedure to connect the system to the server hosting the Lutron dashboard.

SOCKS5 Proxy

Lutron's embedded systems support outbound communication through a SOCKS5 proxy. DNS resolution will be handled directly through the provided DNS server, not through the SOCKS5 proxy.

The customer needs to provide the hostname (either ip or domain name) and port of the customer-provided SOCKS5 server so the Lutron FSE or HTI can manually set it. For example, my.socks5.proxy.com, port 8000.

SOCKS5 Proxy Requirements

1. Authentication between the Lutron processor and SOCKS5 proxy is not supported
2. No proxy-based DNS support
 - a. The Lutron processor does not support DNS resolution through the proxy
 - b. SOCKS5h, which performs remote DNS resolution via the proxy, is not supported
3. Terminating proxies are not supported
 - a. The Lutron processor does not support custom root certificate injection
 - b. Lutron uses end-to-end SSL encryption, performing intermediate SSL termination re-encryption will cause the Lutron cloud server to reject the traffic
4. HTTPS/HTTP proxies are not supported
 - a. HTTPS/MQTTs will all be routed through the SOCKS5 proxy
5. A Lutron system can only have one (1) SOCKS5 proxy configuration¹

¹ A system is defined in Athena System Specification Submittal (P/N 3691298) and myRoom XC System Specification Submittal (P/N 3691330) on www.lutron.com. If multiple SOCKS5 proxy servers are being hosted for redundancy or regional optimization, it is recommended to provide a domain name (e.g., proxy.example.com) for your SOCKS5 proxy configuration. Then, configure your local DNS infrastructure to resolve that domain name to the appropriate IP address based on your preferred routing logic. This allows for flexible proxy management while maintaining the single-proxy configuration requirement within the Lutron system.

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.
 - Dynamic Public IP Resolution
 - The system relies on periodic DNS resolution to determine the current IP address of the public FQDNs. The firewall also has to manage dynamic IPs, otherwise outbound traffic to the Lutron cloud service may be blocked.
- Internet connectivity test (for connected mode only)
 - 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
- Time Sync
 - For connected mode: 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
 - Processors can be configured to use an alternate NTP server provided via DHCP.
 - For server mode: The processor sync time with Lutron Designer at database transfer.
 - For both modes: A customer-specified NTP server can be configured.
- Automatic Firmware Updates (for connected mode only)
 - Lutron systems support a **robust, secure, and automated firmware update process** for system processors and connected devices. This ensures timely delivery of **security patches, bug fixes, and feature enhancements** via an internet connection, with minimal disruption to system operation.
 - Mechanism: Establishes HTTPS connection to firmwareupdates.lutron.com which may resolve to one or more [Amazon S3 - Cloud Storage - AWS](#) addresses.
 - Key features
 - **Automated updates:** Firmware is delivered directly to systems over the internet without manual intervention. This can be disabled by the FSE or HTI during system commissioning.
 - **Secure delivery:** All firmware is **encrypted and cryptographically signed**, ensuring only authentic and validated Lutron firmware is installed.
 - **Minimal downtime:** Updates are applied using a dual-partition ("A/B") strategy, allowing systems to continue running while the new firmware is written and verified.
 - Testing and Qualification Process
 - **Automated and QA testing:** Includes scale testing, edge cases, and power-loss scenarios.
 - **Real-world runtime:** Firmware is deployed to internal and pilot sites before public release.
 - **Staged rollout phases:**
 - Pre-Alpha (2+ weeks), Alpha (2+ weeks), Beta (2+ weeks), Gamma (salt-in), designer software only developments via the web, "canary" groups via the cloud and monitoring for issues which would halt the deployment, full deployment.
 - Integrity and Resilience
 - **Dual-partition updates:** Firmware is written to an inactive partition and verified before switching. This allows rollback if corruption is detected.
 - **Checksums and syncing:** Image integrity is verified before activation. The active partition is also synchronized to ensure fallback capacity.

Networking Overview *(continued)*

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

- 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.
 - The mobile app requires a connection from the processors and gateways to Lutron's cloud services to control the system.
 - 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.

Networking Overview *(continued)*

Single Sign On (SSO)

- Athena and myRoom XC are built on the Lutron Connect platform, which supports SSO using industry-standard OIDC and SAML federation protocols.
- For connected mode:
 - SSO is an optional paid feature available as part of Lutron's premium cloud services, and it requires the system to be connected to the internet. If a customer stops maintaining premium cloud services, their SSO functionality will be disabled and all existing users will get a password reset email so they can configure their own standalone credentials.
 - Once SSO is setup for a company's domain, all users signing in using accounts with email addresses within that domain will be redirected to the company's SSO provider. This SSO functionality applies to most Lutron applications that utilize a myLutron sign-in, including the Lutron dashboard, Lutron App (Pro Installer Mode), Lutron Designer, and other web applications.¹
 - If SSO is desired, customers will need to provide a suitable contact person who will be responsible for implementing the SSO integration with Lutron and performing any necessary maintenance on the connection. The customer is responsible for ensuring this contact information stays up to date and notifying Lutron of any changes. It will be the customer's responsibility to rotate SAML certificates as prompted by our system or to provide Lutron with any updated OIDC keys/secrets two weeks prior to them expiring by emailing remotesvcs@lutron.com.
- For server mode:
 - The customer needs to follow the Identity Provider (IDP) subsection within the **Pre-requisites for Server Installer** section on page 44 to provide information for Lutron to configure SSO on a customer-managed server. The customer is solely responsible for maintaining the SSO.
- The customer is responsible for maintaining an accurate list of individuals who have access to Lutron's system.

¹ The following applications do not support SSO:

- Caséta mobile app (Personal Home Mode)
- RadioRA 2 Select mobile app
- HomeWorks QS (version 15.6 and below)
- RadioRA 2 (version 12.8 and below)
- myRoom plus (version 3.3.275 and below)
- myRoom prime (all versions)
- Q-Design version (3.4.321 and below)
- Quantum Vue (all versions)

Firewall/Routing Requirements

Source ¹	Destination	Port	Transport and Network Layer Protocol	Application Layer Protocol	Startup / Maintenance ²	Runtime	Mode
Commissioning Device ³	1. All Edge and Wireless Processors, Clear Connect – Type X Gateways 2. Hotel Integration Appliance	22	TCP IPv4	SFTP	On-site startup / maintenance		- Connected - Server - Networked
		Description: For database transfer, processor and device firmware download, support file generation, and diagnostics					
Mobile Device on Local Processor Network	All Edge and Wireless Processors and Clear Connect – Type X Gateways	22	TCP IPv4	SFTP	Not required but may see traffic		None
		Description: For support file generation and diagnostics. This port and destination are not utilized during operations phase and can be closed. Lutron support may request these ports to be temporarily opened to support diagnostics and troubleshooting					
AV Integration System IP	IP Address of QSE-CI-NWK	23	TCP IPv4	Telnet	NWK Integration	NWK Integration	- Connected - Server - Networked
		Description: For integration systems which utilize Telnet, an NWK is the only means for Telnet integration to Athena					
1. All Edge and Wireless Processors, Clear Connect – Type X Gateways 2. Hotel Integration Appliance	Customer Specified DNS Server	53	UDP IPv4/IPv6	DNS	1. Required for cloud connectivity 2. Recommended otherwise	1. Required for cloud connectivity 2. Recommended otherwise	Connected
		Description: DNS resolution is required for cloud connectivity and NTP time sync					
1. All Edge and Wireless Processors, Clear Connect – Type X Gateways 2. Hotel Integration Appliance	google.com	80	TCP IPv4	HTTP	Not Required	Not Required	None
		Description: For processor internet connectivity check, not required and can be blocked					
1. All Edge and Wireless Processors, Clear Connect – Type X Gateways 2. Hotel Integration Appliance	time.iot.lutron.io (connected mode only) or customer specified NTP server (all modes)	123	UDP IPv4	NTP	Recommended	Recommended	- Connected - Server - Networked
		Description: NTP is used for automatic time sync which allows time based events to trigger accurately					
Commissioning Device ³	firmwareupdates.lutron.com	443	TCP IPv4	HTTPS	On-site startup / maintenance		Connected
		Description: For Lutron Designer to obtain the latest processor firmware and device firmware upgrade					
Commissioning Device ³	statestore.rollout.io conf.rollout.io x-api.rollout.io analytic.rollout.io	443	TCP IPv4	HTTPS	On-site startup / maintenance		Connected
		Description: For Lutron Designer to properly enable features					
Commissioning Device ³	designer-relay.lutron.com	443	TCP IPv4	HTTPS	On-site startup / maintenance		Connected
		Description: For Lutron Designer login, shade configuration validation in Canvas View					
Commissioning Device ³	<ul style="list-style-type: none"> • api.design.lutron.io • api.iot.lutron.io • connect.lutron.io • lutron-system-design-artifacts.s3.amazonaws.com • digital-twin-artifacts.s3.amazonaws.com 	443	TCP IPv4	HTTPS	On-site startup / maintenance		Connected
		Description: For Lutron Designer to connect to Places, which is essential for saving, retrieving the updated project files and managing access to project files					
Commissioning Device ³	designer-installers.iot.lutron.io designer-services.lutron.com	443	TCP IPv4	HTTPS	On-site startup / maintenance		Connected
		Description: For auto-updater, release notes, and internet detection for any features requiring cloud connectivity					

Table continues onto next page...

Firewall/Routing Requirements *(continued)*

Source ¹	Destination	Port	Transport and Network Layer Protocol	Application Layer Protocol	Startup / Maintenance ²	Runtime	Mode
Commissioning Device ³	<ul style="list-style-type: none"> aaz-fad-prod-messaging.azurewebsites.net 	443	TCP IPv4	HTTPS	On-site startup / maintenance		Connected
Description: For notifications in Lutron Designer							
Commissioning Device ³	<ul style="list-style-type: none"> api.data.lutron.io puekakk076.execute-api.us-east-1.amazonaws.com 	443	TCP IPv4	HTTPS	Optional for on-site startup / maintenance		Connected
Description: For anonymized analytics to help Lutron enhance user experience with Lutron Designer							
Commissioning Device ³	<ul style="list-style-type: none"> cdnjs.cloudflare.com login.microsoftonline.com lutron-prod.rpxnow.com lutron.us.janraincapture.com ssl-static.janraincapture.com sso.login.lutron.com umslogin.lutron.com widget-cdn.janraincapture.com workos-sso.login.lutron.com 	443	TCP IPv4	HTTPS	On-site startup / maintenance		Connected
Description: Necessary to log in to Lutron Designer							
Commissioning Device ³	Customer Managed Server	443	TCP IPv4	HTTPS	Required		Server
Description: Configuration of Customer Managed Server.							
All Edge and Wireless Processors and Clear Connect – Type X Gateways	All Edge and Wireless Processors and Clear Connect – Type X Gateways	443	TCP IPv4/IPv6	WSS	Multi-processor system	Multi-processor system	- Connected - Server - Networked
Description: For sharing events and status of lights between the processors and gateways							
1. All Edge and Wireless Processors, Clear Connect – Type X Gateways 2. Hotel Integration Appliance	<ul style="list-style-type: none"> firmwareupdates.lutron.com <p>IP Range About - Azure IP Ranges</p>	443	TCP IPv4	HTTPS	Automatic firmware upgrade	Automatic firmware upgrade	Connected
Description: For automatic firmware upgrades and may resolve to one or more s3.amazonaws.com addresses							
<ul style="list-style-type: none"> Firmware updates can be applied via a locally connected Commissioning Device if internet is not available 							
1. All Edge and Wireless Processors, Clear Connect – Type X Gateways 2. Hotel Integration Appliance	<ul style="list-style-type: none"> *.s3.amazonaws.com lutron-system-design-artifacts.s3.amazonaws.com https://digital-twin-artifacts.s3.amazonaws.com/ https://lutron-system-config.s3.us-east-1.amazonaws.com https://lutron-system-logs.s3.us-east-1.amazonaws.com https://lutron-system-runtime-data-logs.s3.us-east-1.amazonaws.com *.s3.dualstack.us-east-1.amazonaws.com <p>IP Range AWS IP address ranges - Amazon Virtual Private Cloud</p>	443	TCP IPv4	HTTPS	Remote Diagnostics	Remote Diagnostics	Connected
Description: For support file generation							
<ul style="list-style-type: none"> Diagnostics can be performed locally through the connected Commissioning Device if internet is not available. This includes support file generation 							
1. All Edge and Wireless Processors, Clear Connect – Type X Gateways 2. Hotel Integration Appliance	<ul style="list-style-type: none"> kinesis.us-east-1.amazonaws.com <p>IP Range AWS IP address ranges - Amazon Virtual Private Cloud</p>	443	TCP IPv4	HTTPS	1. Dashboard 2. Diagnostics	1. Dashboard 2. Diagnostics	Connected
Description: For energy usage and space occupancy features in dashboard, and anonymized analytics for processor issue diagnostics							

Table continues onto next page...

Firewall/Routing Requirements *(continued)*

Source ¹	Destination	Port	Transport and Network Layer Protocol	Application Layer Protocol	Startup / Maintenance ²	Runtime	Mode
1. All Edge and Wireless Processors, Clear Connect – Type X Gateways 2. Hotel Integration Appliance	<ul style="list-style-type: none"> c1fp46crw8ud8d.credentials.iot.us-east-1.amazonaws.com lutron-system-config.s3.us-east-1.amazonaws.com https://lutron-system-config.s3.dualstack.us-east-1.amazonaws.com IP Range AWS IP address ranges - Amazon Virtual Private Cloud	443	TCP IPv4	HTTPS	1. Remote startup / maintenance 2. Dashboard	Dashboard	Connected
		Description: For Athena dashboard and remote database transfer					
1. All Edge and Wireless Processors, Clear Connect – Type X Gateways 2. Hotel Integration Appliance 3. Mobile Device on Building Network	<ul style="list-style-type: none"> a32jcyk7azp7b5-ats.iot.us-east-1.amazonaws.com *.iot.lutron.io - https://data-ingestion.iot.lutron.io/ - https://feature.iot.lutron.io/ - https://api.iot.lutron.io - https://provision.iot.lutron.io - https://device.iot.lutron.io IP Range AWS IP address ranges - Amazon Virtual Private Cloud	443	TCP IPv4/IPv6*	HTTPS	1. Remote startup / maintenance 2. Mobile App 3. Dashboard	1. Mobile App 2. Dashboard	Connected
		Description: For connectivity for Cloud based functionality, including dashboard, mobile app remote access and remote service capability * IPv6 is supported for mobile app remote access and a subset of functionality in dashboard					
1. All Edge and Wireless Processors, Clear Connect – Type X Gateways 2. Hotel Integration Appliance	Device-login.lutron.com IP Range AWS IP address ranges - Amazon Virtual Private Cloud	443	TCP IPv4	HTTPS	Remote startup / maintenance	Dashboard	Connected
		Description: For device registration and secure processor remote access					
1. All Edge and Wireless Processors, Clear Connect – Type X Gateways 2. Hotel Integration Appliance	Customer Managed Server	443	TCP IPv4	HTTPS	Required	Required	Server
		Description: Connectivity for dashboard functionality.					
Web Browser Computer	Customer Managed Server	443	TCP IPv4	HTTPS	Required	Required	Server
		Description: Monitoring and reporting via the Lutron dashboard.					
Customer Managed Server	Customer defined Identity Provider	443	TCP IPv4	HTTPS	Required	Required	Server
		Description: Used for single sign on (SSO)					
Customer Managed Server	SMTP Server	587 by default ⁴	TCP IPv4	SMTPS	Dashboard alert emails	Dashboard alert emails	Server
		Description: Used to communicate to optional SMTP server for dashboard alert emails					
Hotel Integration Appliance (Static IP)	SMS Cloud Service	443 by default ⁴	TCP IPv4	HTTPS	Required for myRoom XC only	Required for myRoom XC only	Connected
		Description: For events sent between the SMS cloud service server and the Lutron system. This port is configurable through a web application hosted by the hotel integration appliance.					
All Edge and Wireless Processors and Clear Connect Gateways – Type X	Multicast Address of the system (239.0.38.1 – 239.0.38.xx) ⁵	2056-3055	UDP IPv4 Multicast	Proprietary	Only required for pre-2023 processor firmware	Only required for pre-2023 processor firmware	- Connected - Networked
		Description: For sharing events and status of lights between the processors and gateways. Only needed if system is configured for inter-processor communication via multicast. Not applicable for systems installed in 2023 or later.					
Commissioning Device ³	Hotel Integration Appliance (Static IP)	2607	TCP IPv4	HTTPS	Required for myRoom XC only		- Connected - Server - Networked
		Description: For connecting to the web-based user interface to configure the hotel integration appliance					

Table continues onto next page...

Firewall/Routing Requirements *(continued)*

Source ¹	Destination	Port	Transport and Network Layer Protocol	Application Layer Protocol	Startup / Maintenance ²	Runtime	Mode
Guestroom Processor (Static IP)	Hotel Integration Appliance (Static IP)	5001 - 5003 by default ⁴	TCP IPv4	mTLS	Required for myRoom XC only	Required for myRoom XC only	- Connected - Server - Networked
		Description: These ports are used to communicate events from the guestroom processor to the hotel integration appliance. This port is configurable through a web application hosted by the hotel integration appliance.					
Commissioning Device ³	224.0.0.251	5353	UDP IPv4 Multicast	mDNS	Required		- Connected - Server - Networked
		Description: mDNS is utilized for processor discovery and initial configuration					
All Edge and Wireless Processors and Clear Connect – Type X Gateways	224.0.0.251	5353	UDP IPv4 Multicast	mDNS	Required		- Connected - Server - Networked
		Description: This is the mDNS discovery response sent from the processor/gateway back to the Lutron configuration software					
1. Lutron Touchscreen 2. API Integrations	224.0.0.251	5353	UDP IPv4 Multicast	mDNS	1. Touchscreen 2. Third-party Integration		- Connected - Server - Networked
		Description: mDNS is utilized for edge processor discovery by the Athena touchscreen and third-party devices integrating via API					
Mobile Device on Local Processor Network	224.0.0.251	5353	UDP IPv4 Multicast	mDNS	Not required but may see traffic		None
		Description: mDNS is utilized for processor discovery during setup and system pairing. This port and destination are not utilized during operations phase and can be closed. Lutron support may request these ports to be temporarily opened to support diagnostics and troubleshooting.					
CELS Server	Hotel Integration Appliance (Static IP)	7000 by default ⁴	TCP IPv4	HTTPS	Required for myRoom XC only	Required for myRoom XC only	- Connected - Server - Networked
		Description: For events sent between the CELS server and the Lutron system. This port is configurable through a web application hosted by the hotel integration appliance.					
Commissioning Device ³	Lutron Touchscreens	8080	TCP IPv4	HTTP	Touchscreen diagnostics		- Connected - Server - Networked
		Description: For touchscreen diagnostics					
Commissioning Device ³	1. All Edge and Wireless Processors, Clear Connect – Type X Gateways 2. Hotel Integration Appliance	8081 8083	TCP IPv4	mTLS	Required		- Connected - Server - Networked
		Description: For configuring processors and enabling integration with third-party equipment through the Lutron API (LEAP)					
1. Lutron Touchscreen 2. API Integrations	All Edge and Wireless Processors and Clear Connect – Type X Gateways	8081 8083	TCP IPv4/IPv6 *	mTLS	1. Touchscreen 2. Third-party Integration	1. Touchscreen 2. Third-party Integration	- Connected - Server - Networked
		Description: For communicating between the processors and Lutron touchscreens, and between processors and API integrations. One connection per system. * IPv6 is not supported for Lutron Touchscreen					
Mobile Device on Local Processor Network	All Edge and Wireless Processors and Clear Connect – Type X Gateways	8081 8083	TCP IPv4	mTLS	Not required but may see traffic	Not required but may see traffic	None
		Description: For Lutron mobile app authentication and configuration. This port and destination may not be utilized during operations phase and can be closed. Lutron support may request these ports to be temporarily opened to support diagnostics and troubleshooting. Traffic may appear on this port if left open as the Mobile App and Processor App try to optimize dataflow via local network. Processor connection to the Internet required for Lutron App and SSO services.					

Table continues onto next page...

Firewall/Routing Requirements *(continued)*

Source ¹	Destination	Port	Transport and Network Layer Protocol	Application Layer Protocol	Startup / Maintenance ²	Runtime	Mode
1. All Edge and Wireless Processors, Clear Connect – Type X Gateways 2. Hotel Integration Appliance 3. Mobile Device on Building Network	<ul style="list-style-type: none"> • a32jcyk7azp7b5-ats.iot.us-east-1.amazonaws.com • *.iot.lutron.io - https://data-ingestion.iot.lutron.io/ - https://feature.iot.lutron.io/ - https://api.iot.lutron.io - https://provision.iot.lutron.io - https://device.iot.lutron.io IP Range AWS IP address ranges - Amazon Virtual Private Cloud	8883	TCP IPv4/IPv6 *	MQTT	1. Remote startup / maintenance 2. Mobile App 3. Dashboard	1. Mobile App 2. Dashboard	Connected
		Description: For connectivity for Cloud based functionality, including dashboard, mobile app remote access and remote service capability * IPv6 is supported for mobile app remote access and a subset of functionality in dashboard					
1. All Edge and Wireless Processors, Clear Connect – Type X Gateways 2. Hotel Integration Appliance	Customer Managed Server	8883	TCP IPv4	MQTT	Required	Required	Server
		Description: Connectivity for dashboard functionality.					
Commissioning Device ³	1. All Edge and Wireless Processors, Clear Connect – Type X Gateways 2. Hotel Integration Appliance	8902	TCP IPv4	mTLS	On-site startup / maintenance		- Connected - Server - Networked
Description: Local unicast communication between design software and processors, available in August 2025 and onwards							
Hotel Integration Appliance (Static IP)	PMS Server	9002 by default ⁴	TCP IPv4	Vendor specific	Required for myRoom XC only	Required for myRoom XC only	- Connected - Server - Networked
		Description: Events sent between the PMS server and the Lutron system. This port is configurable through a web application hosted by the hotel integration appliance.					
BACnet Integration Device	IP Address of the Lutron Processor	47808 by default ⁴	UDP IPv4	BACnet	BACnet	BACnet	- Connected - Server - Networked
		Description: For third-party external integration with a system that supports BACnet (e.g., BMS or HVAC system). One connection per processor. This port is configurable in Lutron Designer.					
Commissioning Device ³	1. All Edge and Wireless Processors, Clear Connect – Type X Gateways 2. Hotel Integration Appliance	51023	TCP IPv4	Proprietary	On-site startup / maintenance		- Connected - Server - Networked
		Description: Local unicast communication between design software and processors, to be deprecated for Lutron Designer software released after August 2025					
1. All Edge and Wireless Processors, Clear Connect – Type X Gateways 2. Hotel Integration Appliance	8.8.4.4 8.8.8.8 208.67.220.220 208.67.222.222 209.244.0.3 209.244.0.4	Not Applicable	ICMP	Not Applicable	Recommended for cloud connectivity	Recommended for cloud connectivity	Connected
		Description: Processor Internet connectivity check					

¹ For connection-oriented protocol, source address initiates the connection.

² If the facility manager or hotel operator's daily operation involves using the Lutron Designer software, that is considered part of the maintenance phase.

³ 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.

⁴ These port numbers are the common defaults, but may be set to other values during system commissioning, depending on the third-party system being used for integration. If configured differently, the connection information will be provided by the commissioning agent, and are required to be opened between endpoints for proper system operation. When configuring ports, make sure they don't conflict with ports used by other applications of the same processor, gateway, or hotel integration appliance.

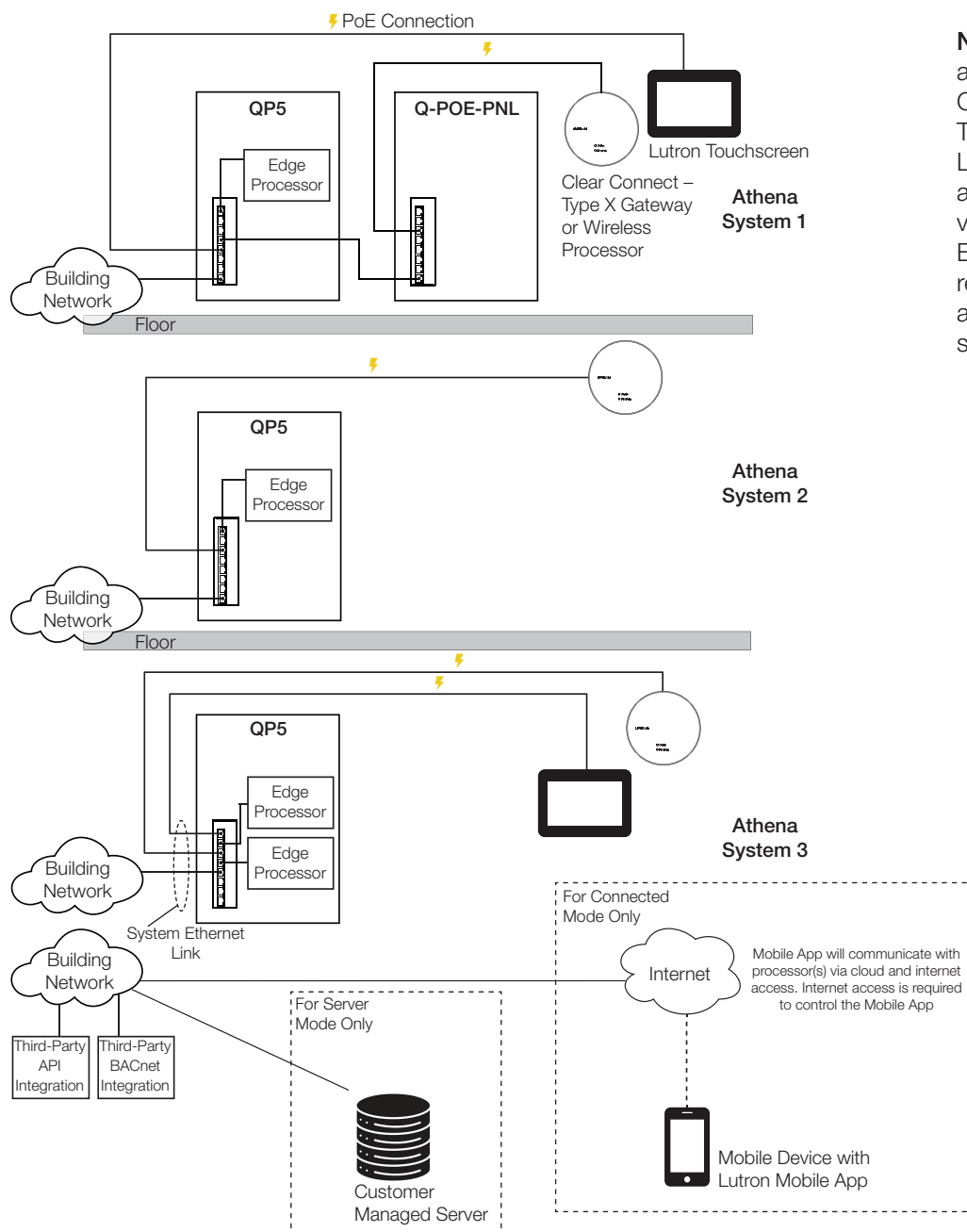
⁵ Multicast addresses used by the system will be configured by the FSE/HTI during system startup.

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 processors, the wireless processors, and Clear Connect – Type X Gateways to communicate to the Internet and the Lutron mobile app (in connected mode), or customer-provided server (in server mode). 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.

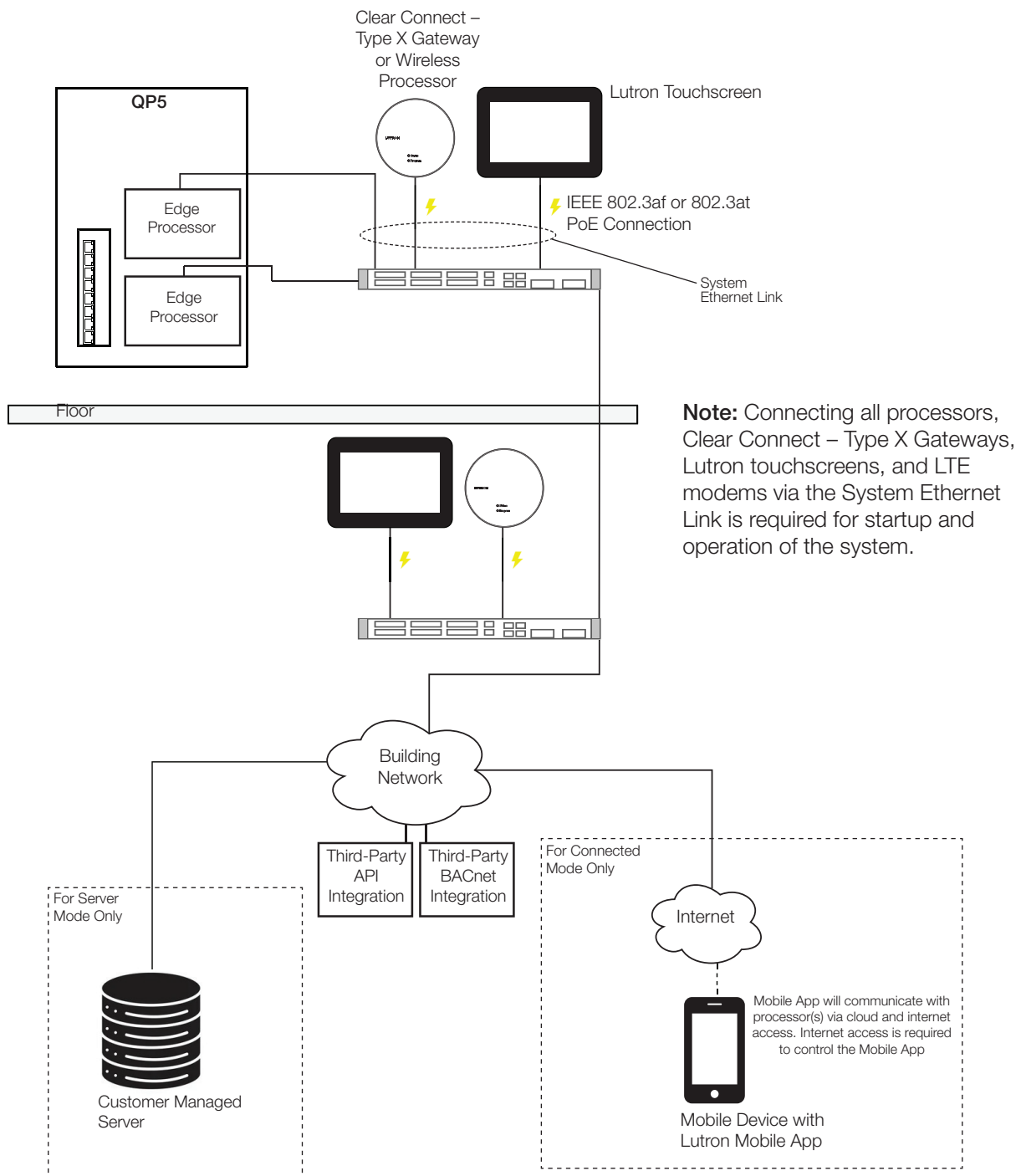


Note: Connecting all processors, Clear Connect – Type X Gateways, Lutron touchscreens, and LTE modems via the system Ethernet link, is required for startup and operation of the system.

Configuration Examples *(continued)*

Athena System Deployment Utilizing Customer-Provided PoE Ethernet Switches

This diagram 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–Type X Gateways, 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.

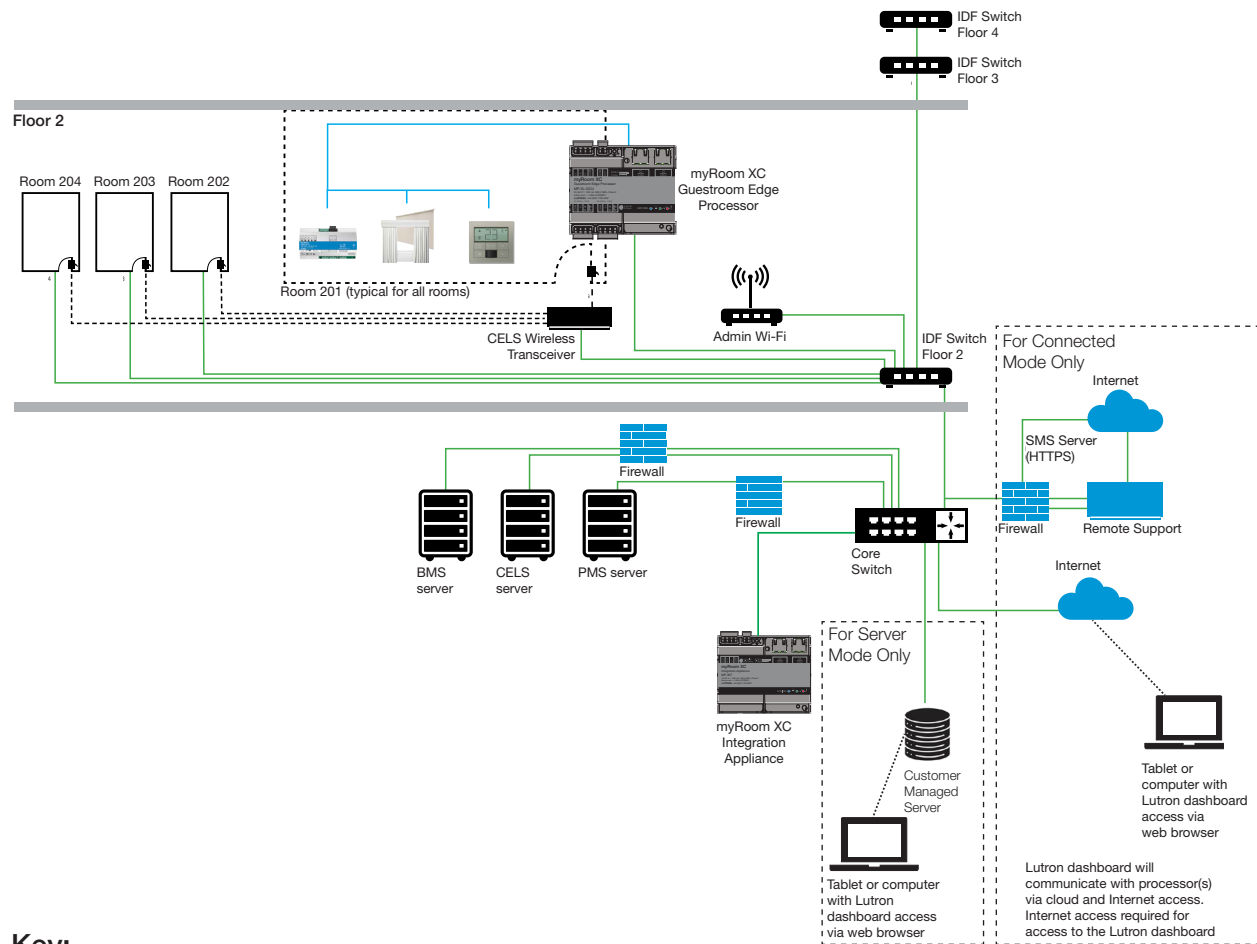


Note: Connecting all processors, Clear Connect – Type X Gateways, Lutron touchscreens, and LTE modems via the System Ethernet Link is required for startup and operation of the system.

Configuration Examples *(continued)*

myRoom XC Guestroom System Deployment

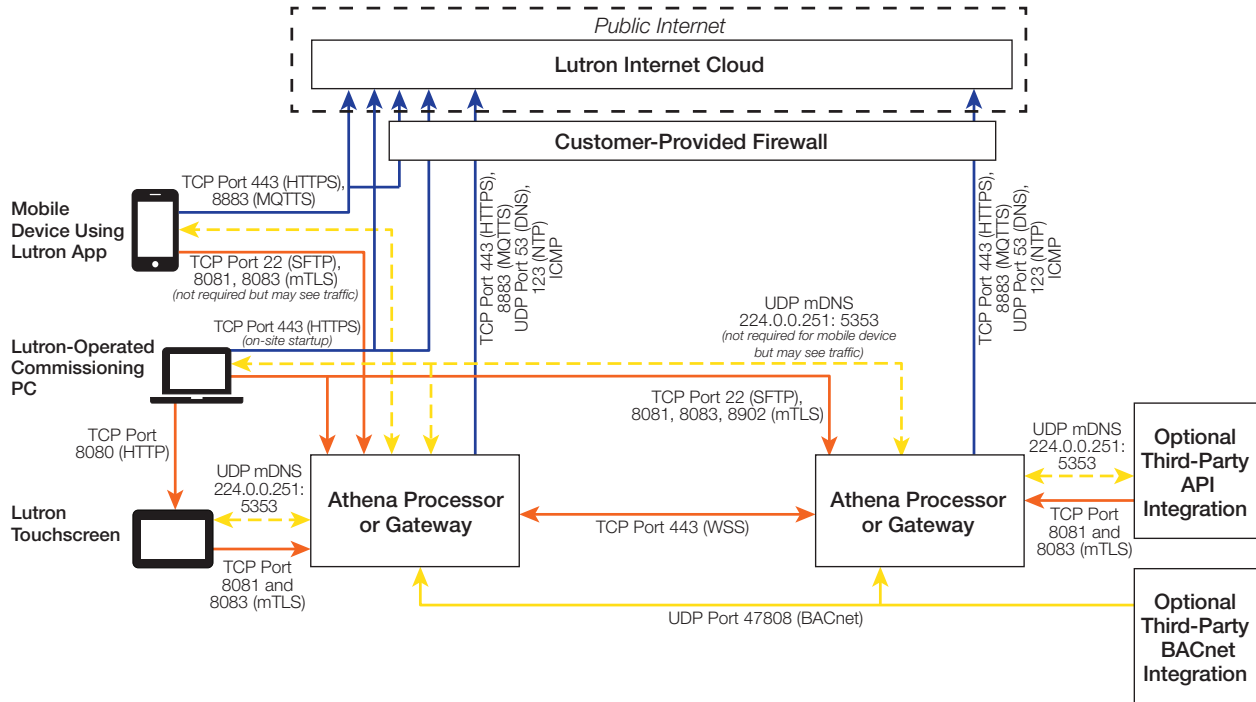
This digram shows the use of customer-provided Ethernet switches to connect processors to the building network infrastructure for the system Ethernet link. Each edge processor may contain two RJ45 Ethernet jacks, which should not be used for daisy chaining (the second port is used for FSE/HTI diagnostics).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



Network Diagram

Connected Mode

Athena System During Startup/Maintenance



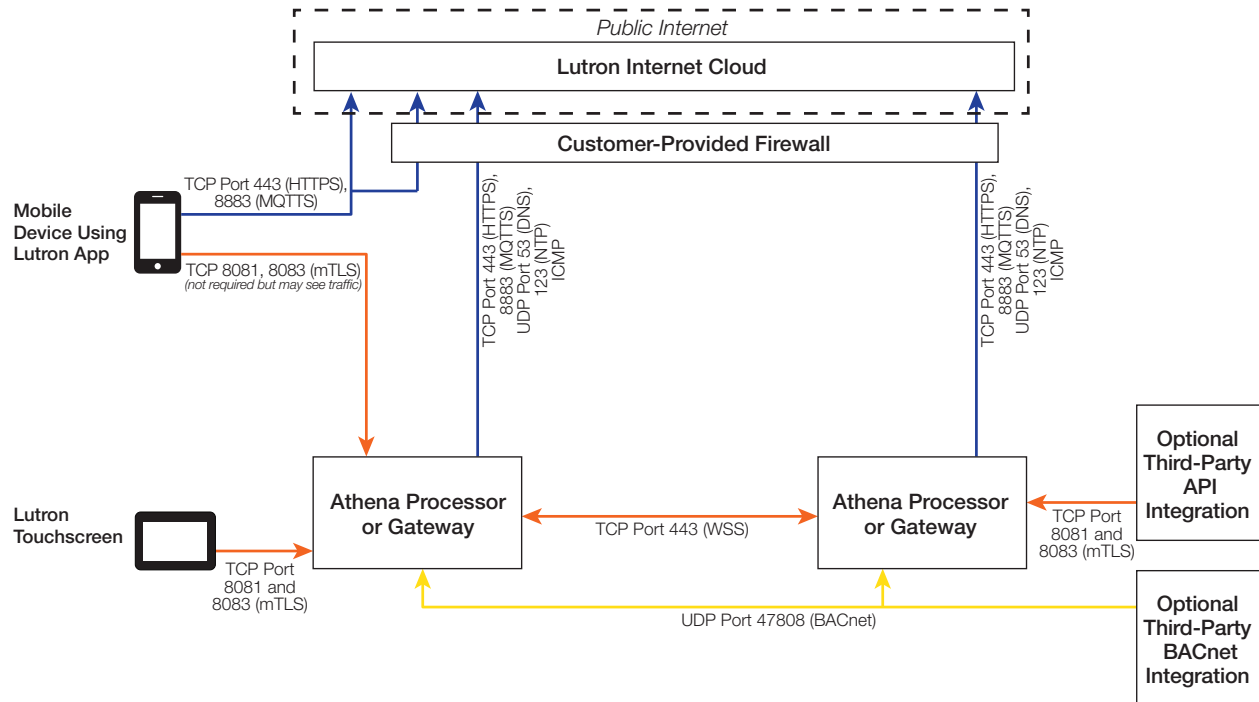
Connection Legend	
	Outgoing internet
	Local TCP
	Local UDP
	Local UDP multicast
Note: Arrows indicate the originator of the connection.	

The mobile device using the Lutron App must connect to the Lutron cloud in order to interact with the in-building Athena processor. Depending on the path to the cloud, the customer-provided firewall may be involved. Lutron cannot limit cloud access or mobile access from specific IPs.

Network Diagram *(continued)*

Connected Mode *(continued)*

Athena System During Runtime



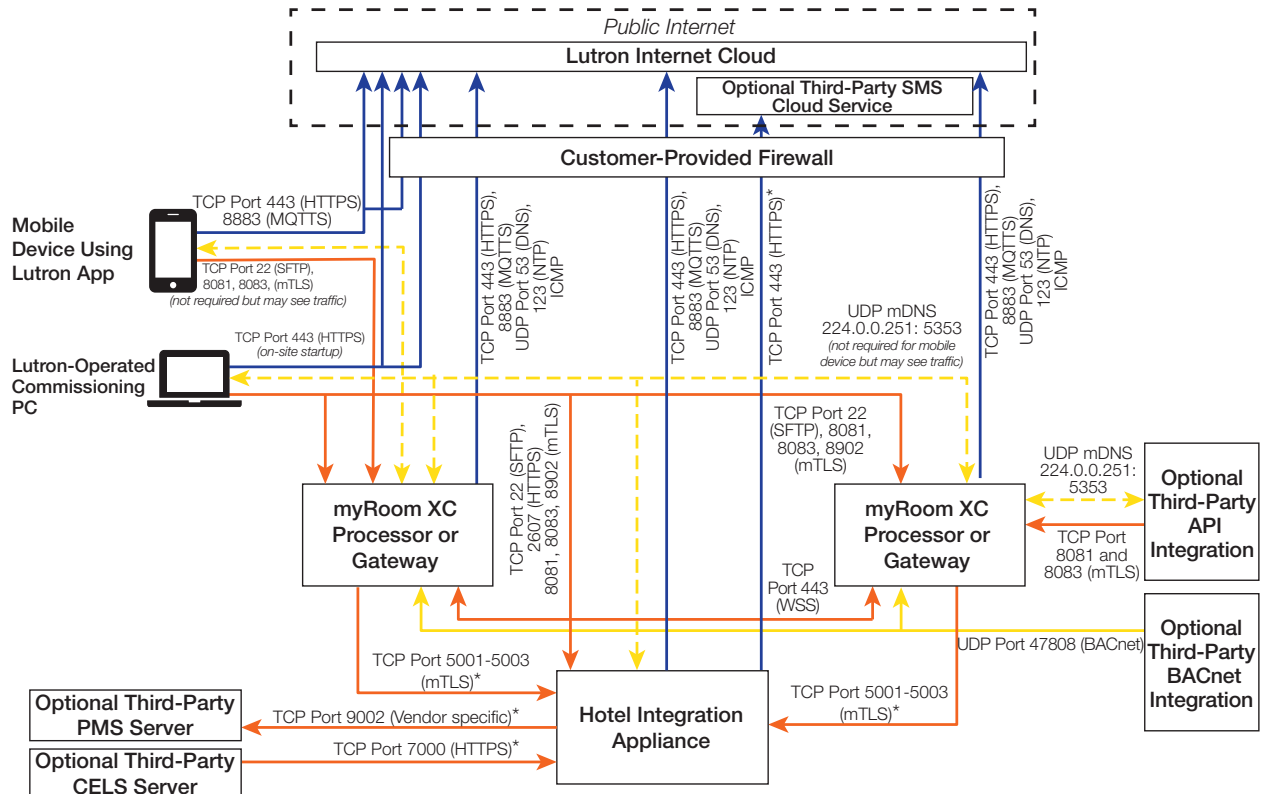
Connection Legend	
	Outgoing internet
	Local TCP
	Local UDP
Note: Arrows indicate the originator of the connection.	

The mobile device using the Lutron App must connect to the Lutron cloud in order to interact with the in-building Athena processor. Depending on the path to the cloud, the customer-provided firewall may be involved. Lutron cannot limit cloud access or mobile access from specific IPs.

Network Diagram *(continued)*

Connected Mode *(continued)*

myRoom XC System During Startup/Maintenance



Connection Legend	
	Outgoing internet
	Local TCP
	Local UDP
	Local UDP multicast
Note: Arrows indicate the originator of the connection.	

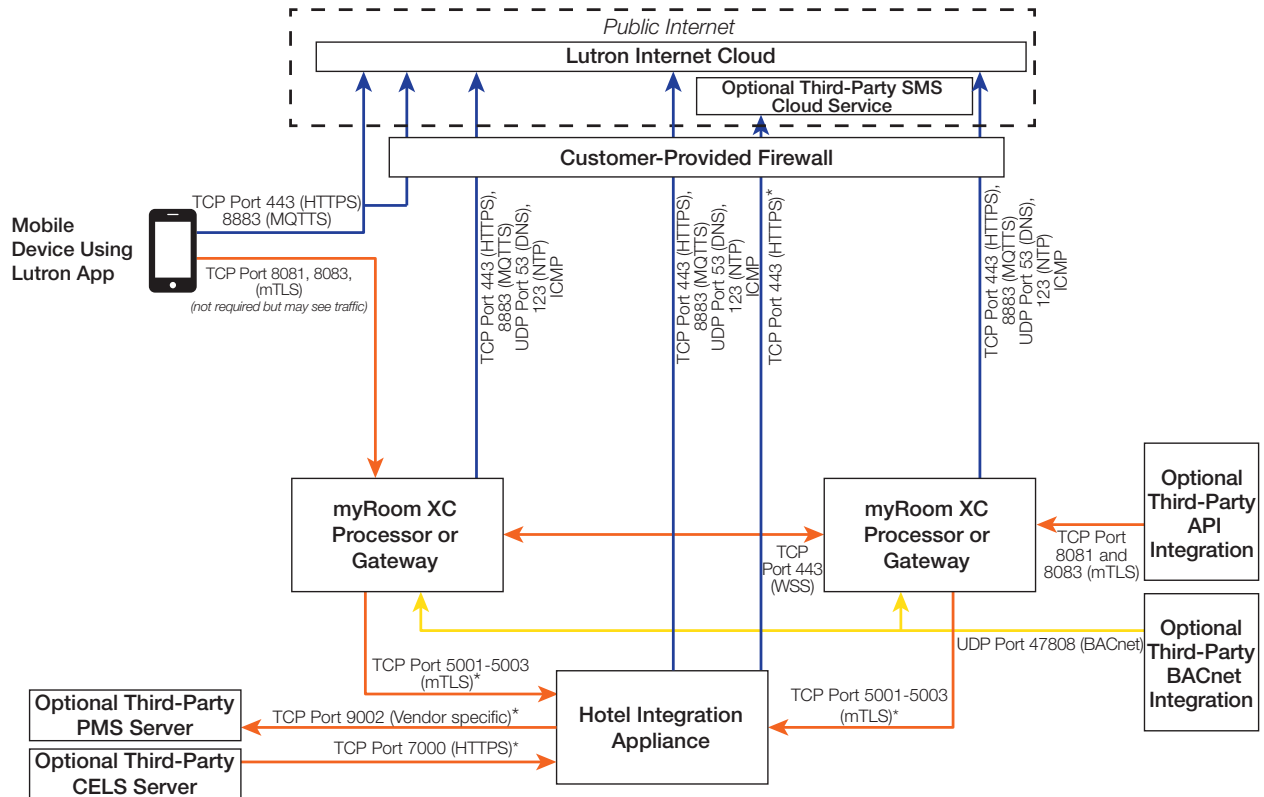
The mobile device using the Lutron App must connect to the Lutron cloud in order to interact with the in-building Athena processor. Depending on the path to the cloud, the customer-provided firewall may be involved. Lutron cannot limit cloud access or mobile access from specific IPs.

* Port number and connection may vary based on third-party server requirements.

Network Diagram *(continued)*

Connected Mode *(continued)*

myRoom XC System During Runtime



Connection Legend	
	Outgoing internet
	Local TCP
	Local UDP
Note: Arrows indicate the originator of the connection.	

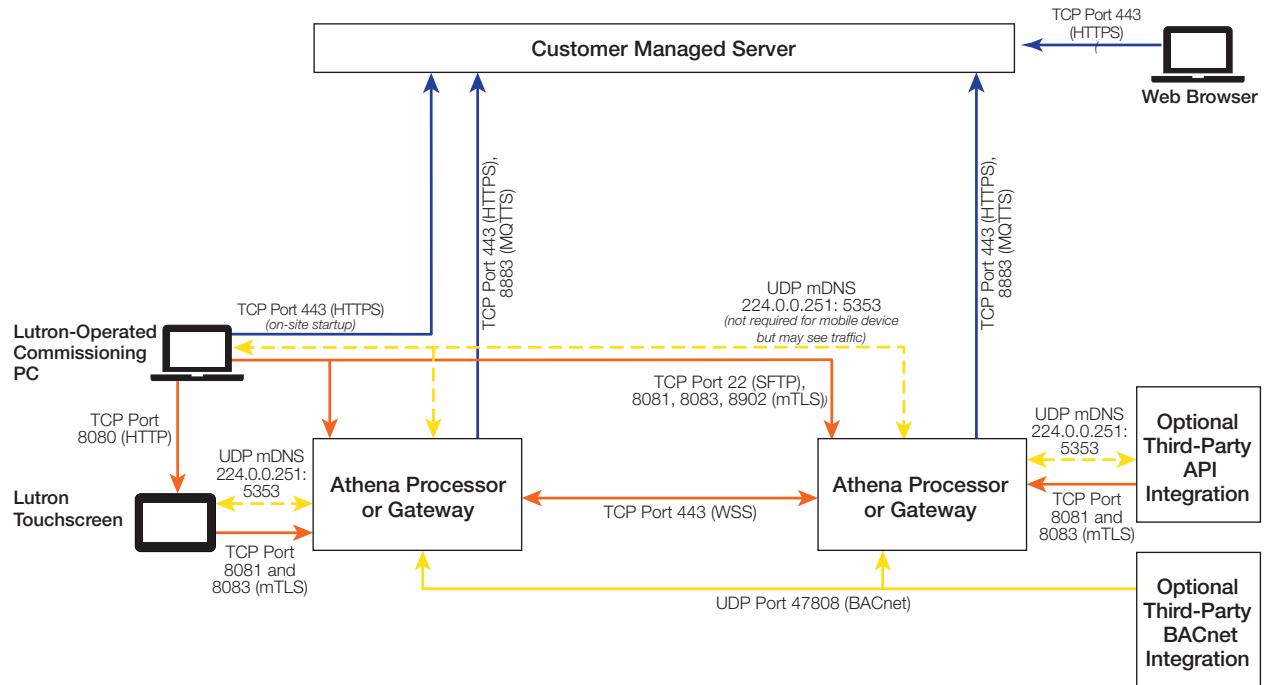
The mobile device using the Lutron App must connect to the Lutron cloud in order to interact with the in-building Athena processor. Depending on the path to the cloud, the customer-provided firewall may be involved. Lutron cannot limit cloud access or mobile access from specific IPs.

* Port number and connection may vary based on third-party server requirements.

Network Diagram

Server Mode

Athena System During Startup/Maintenance

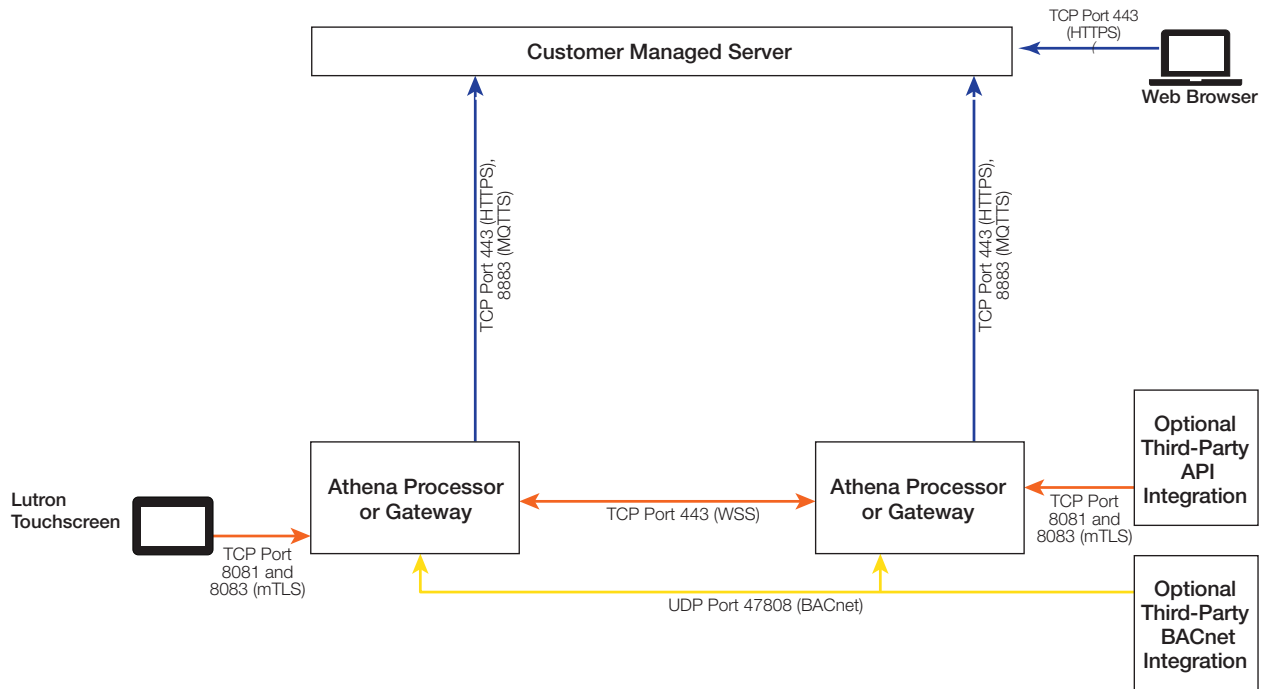





Connection Legend	
	Outgoing connection to server
	Local TCP
	Local UDP
	Local UDP multicast
Note: Arrows indicate the originator of the connection.	

Network Diagram *(continued)*

Server Mode *(continued)*

Athena System During Runtime

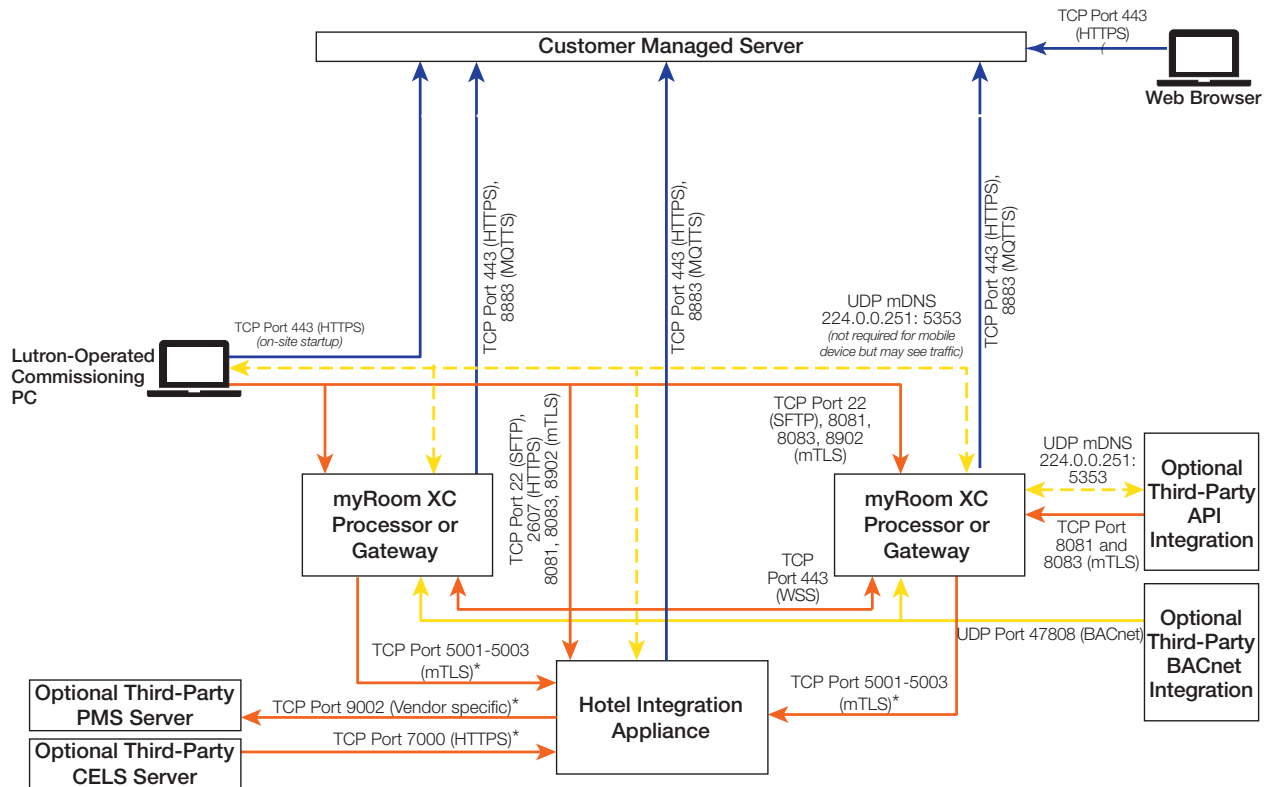


Connection Legend	
	Outgoing connection to server
	Local TCP
	Local UDP
Note: Arrows indicate the originator of the connection.	

Network Diagram *(continued)*

Server Mode *(continued)*

myRoom XC System During Startup/Maintenance



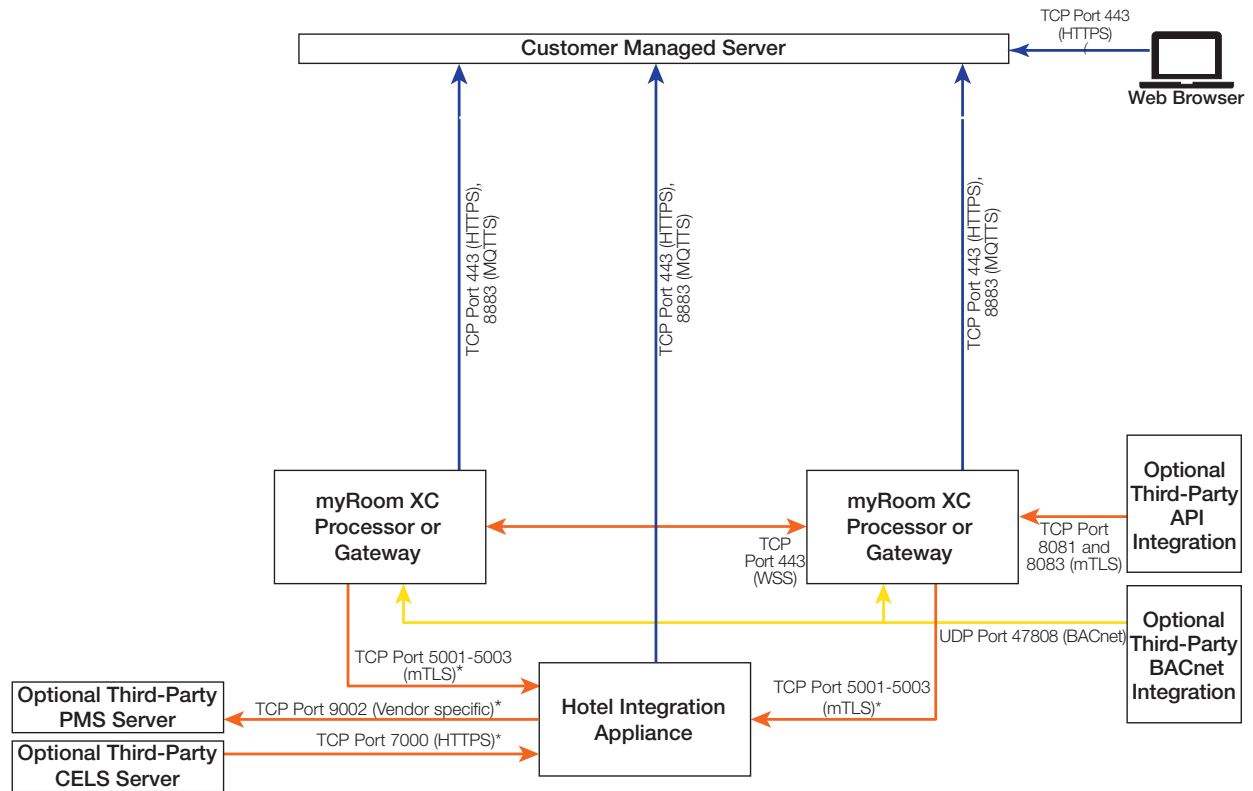
Connection Legend	
	Outgoing connection to server
	Local TCP
	Local UDP
	Local UDP multicast
Note: Arrows indicate the originator of the connection.	

* Port number and connection may vary based on third-party server requirements.

Network Diagram *(continued)*

Server Mode *(continued)*

myRoom XC System During Runtime



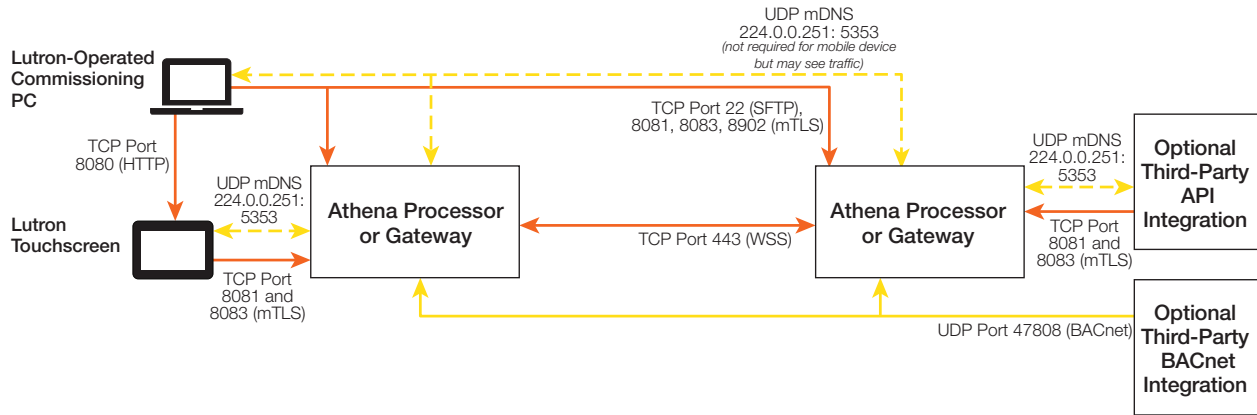
Connection Legend	
	Outgoing connection to server
	Local TCP
	Local UDP
Note: Arrows indicate the originator of the connection.	

* Port number and connection may vary based on third-party server requirements.

Network Diagram *(continued)*

Networked

Athena System During Startup/Maintenance

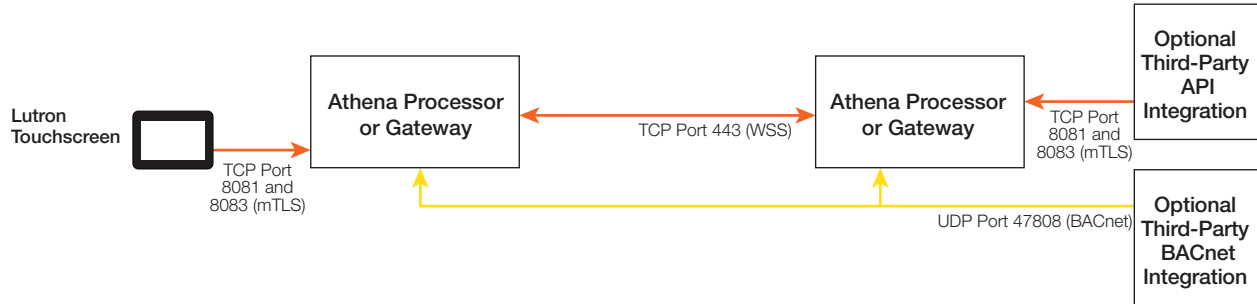



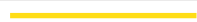
Connection Legend	
	Local TCP
	Local UDP
	Local UDP multicast
Note: Arrows indicate the originator of the connection.	

Network Diagram *(continued)*

Networked *(continued)*

Athena System During Runtime

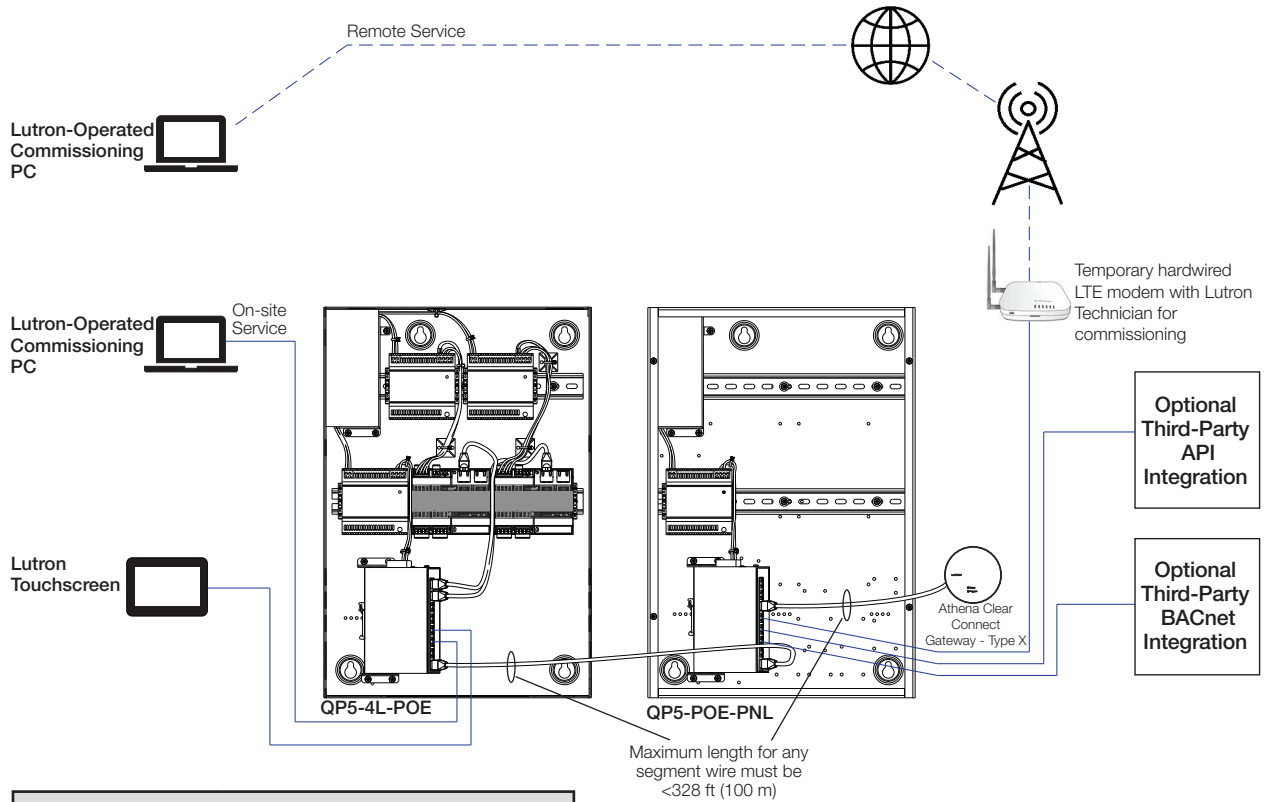


Connection Legend	
	Local TCP
	Local UDP
Note: Arrows indicate the originator of the connection.	

Ethernet Cable Wiring Diagram

Connected Mode

Athena System During Startup without Building Network

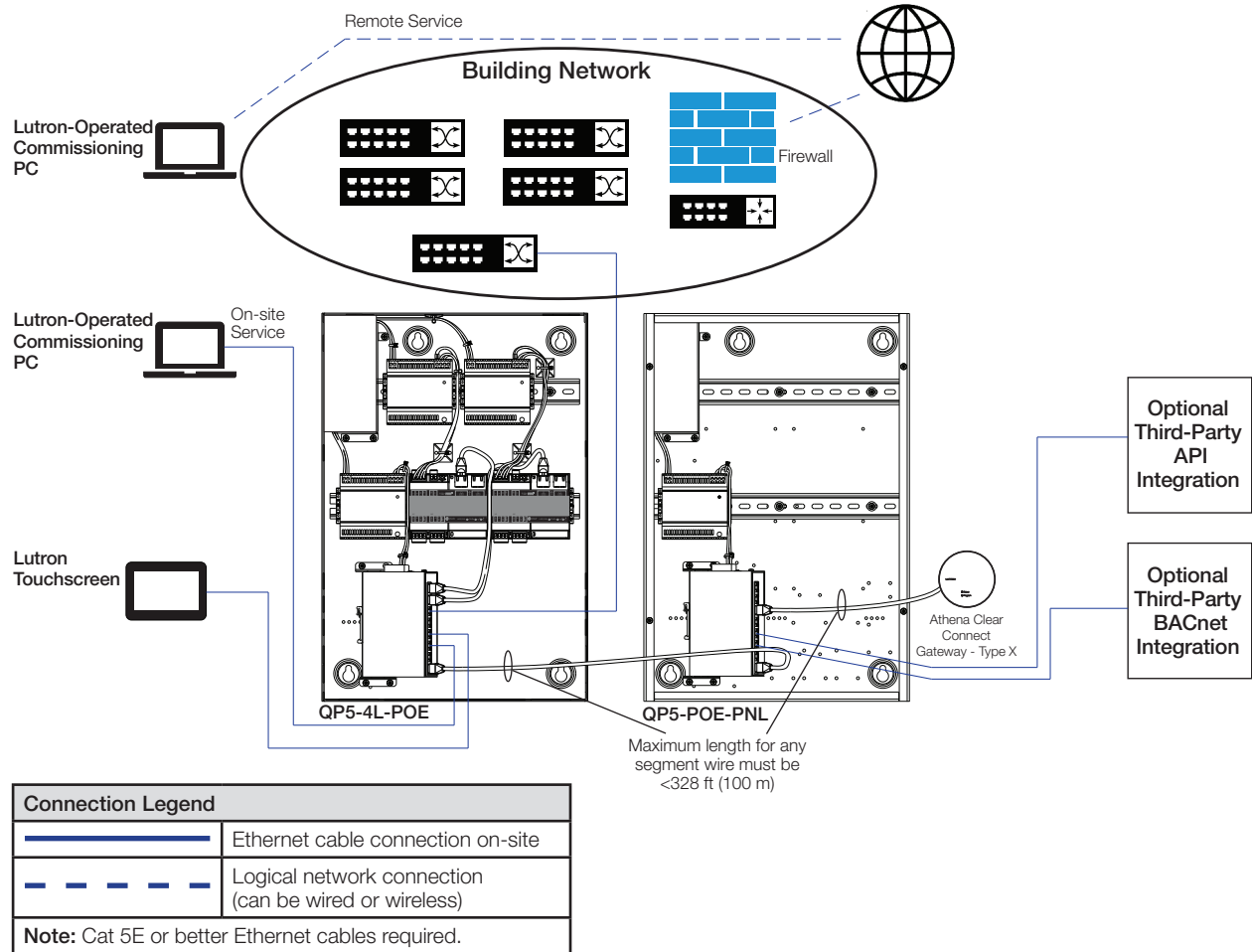


Connection Legend	
	Ethernet cable connection on-site
	Logical network connection (can be wired or wireless)
Note: Cat 5E or better Ethernet cables required.	

Ethernet Cable Wiring Diagram *(continued)*

Connected Mode *(continued)*

Athena System During Startup/Maintenance with Building Network (Option 1: Single Connection to Customer LAN)

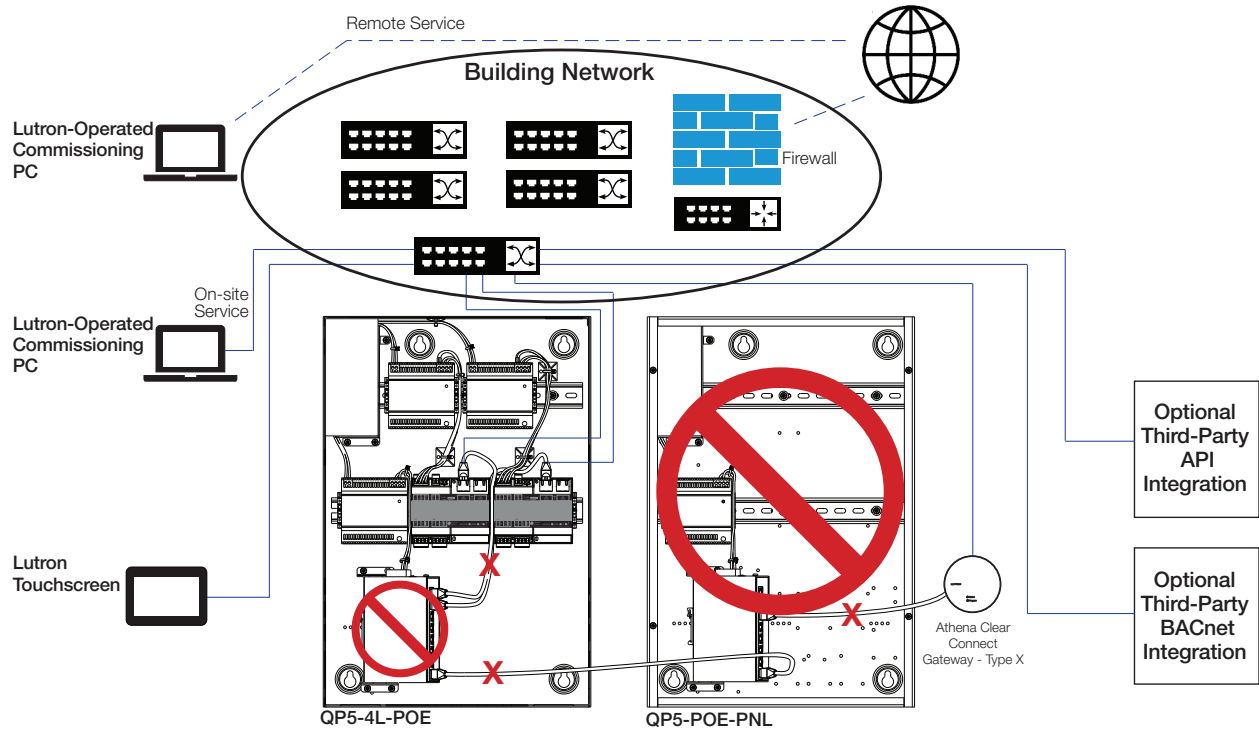


Ethernet Cable Wiring Diagram *(continued)*

Connected Mode *(continued)*

Athena System During Startup/Maintenance with Building Network (Option 2a: Multiple Connections to Customer LAN)

Note: Under this wiring configuration, if the building network fails, lighting controls may fail.



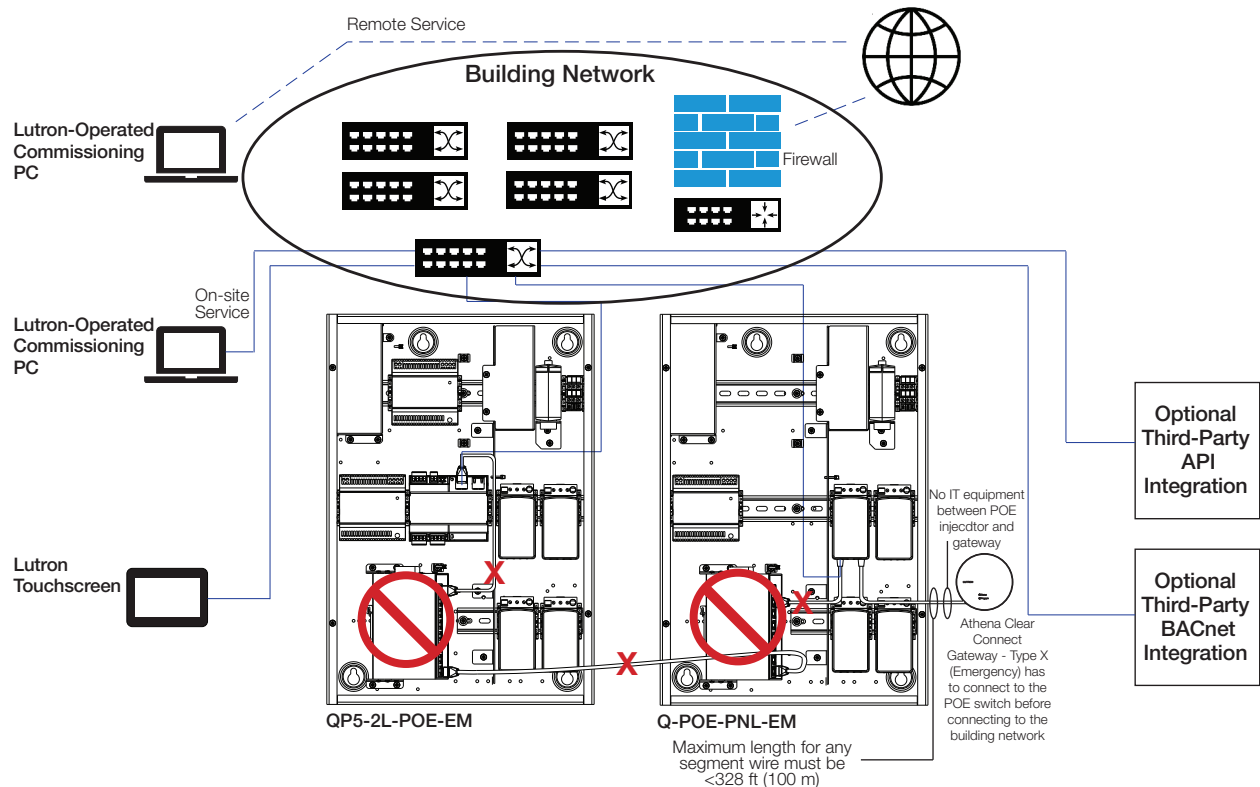
Connection Legend	
	Ethernet cable connection on-site
	Logical network connection (can be wired or wireless)
	Disconnect and abandon in place
Note: Cat 5E or better Ethernet cables required.	

Ethernet Cable Wiring Diagram *(continued)*

Connected Mode *(continued)*

Athena System During Startup/Maintenance with Building Network (Option 2b: Multiple Connections to Customer LAN - with QP5-2L-POE-EM)

Note: Under this wiring configuration, if the building network fails, lighting controls may fail.

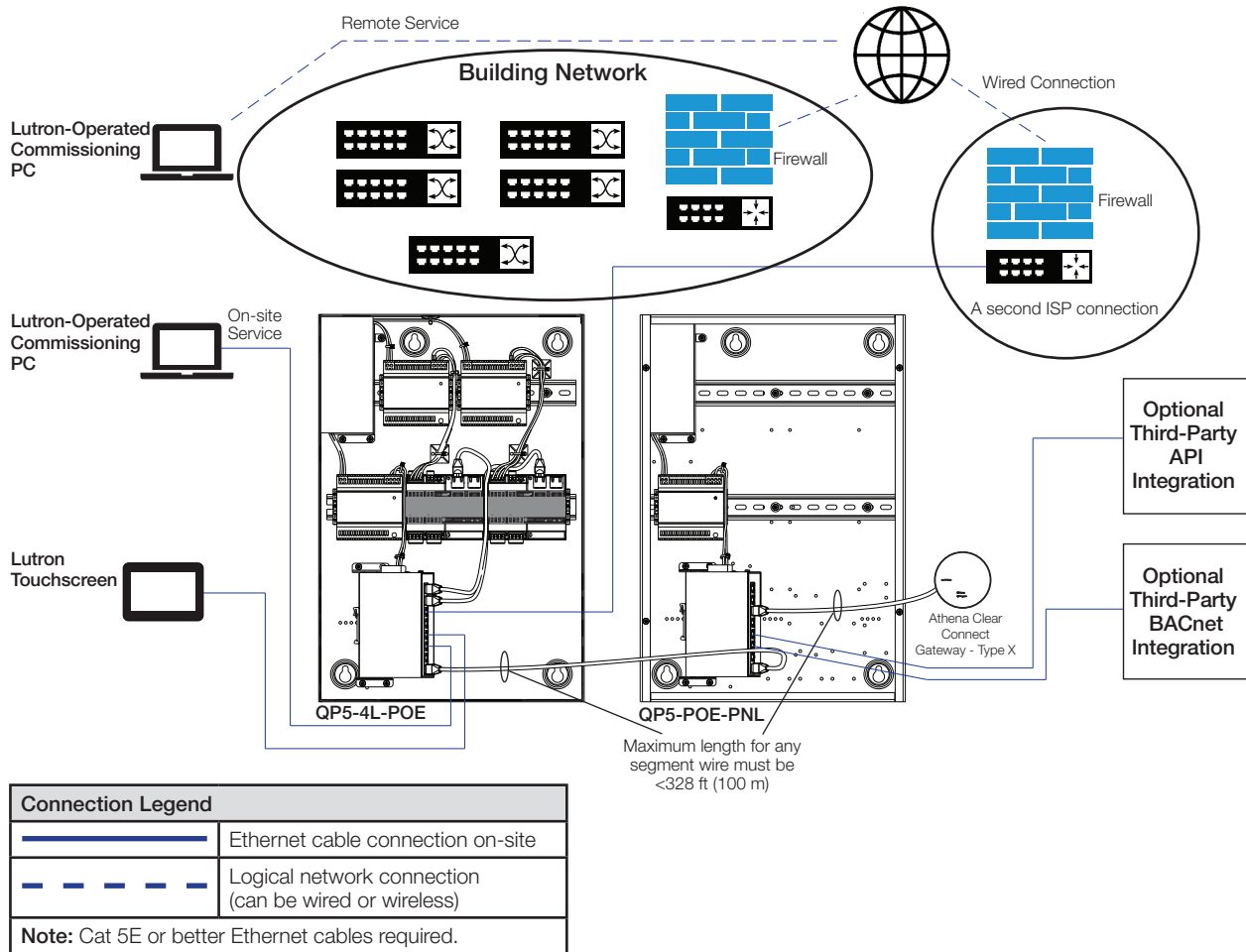


Connection Legend	
	Ethernet cable connection on-site
	Logical network connection (can be wired or wireless)
	Disconnect and abandon in place
Note: Cat 5E or better Ethernet cables required.	

Ethernet Cable Wiring Diagram *(continued)*

Connected Mode *(continued)*

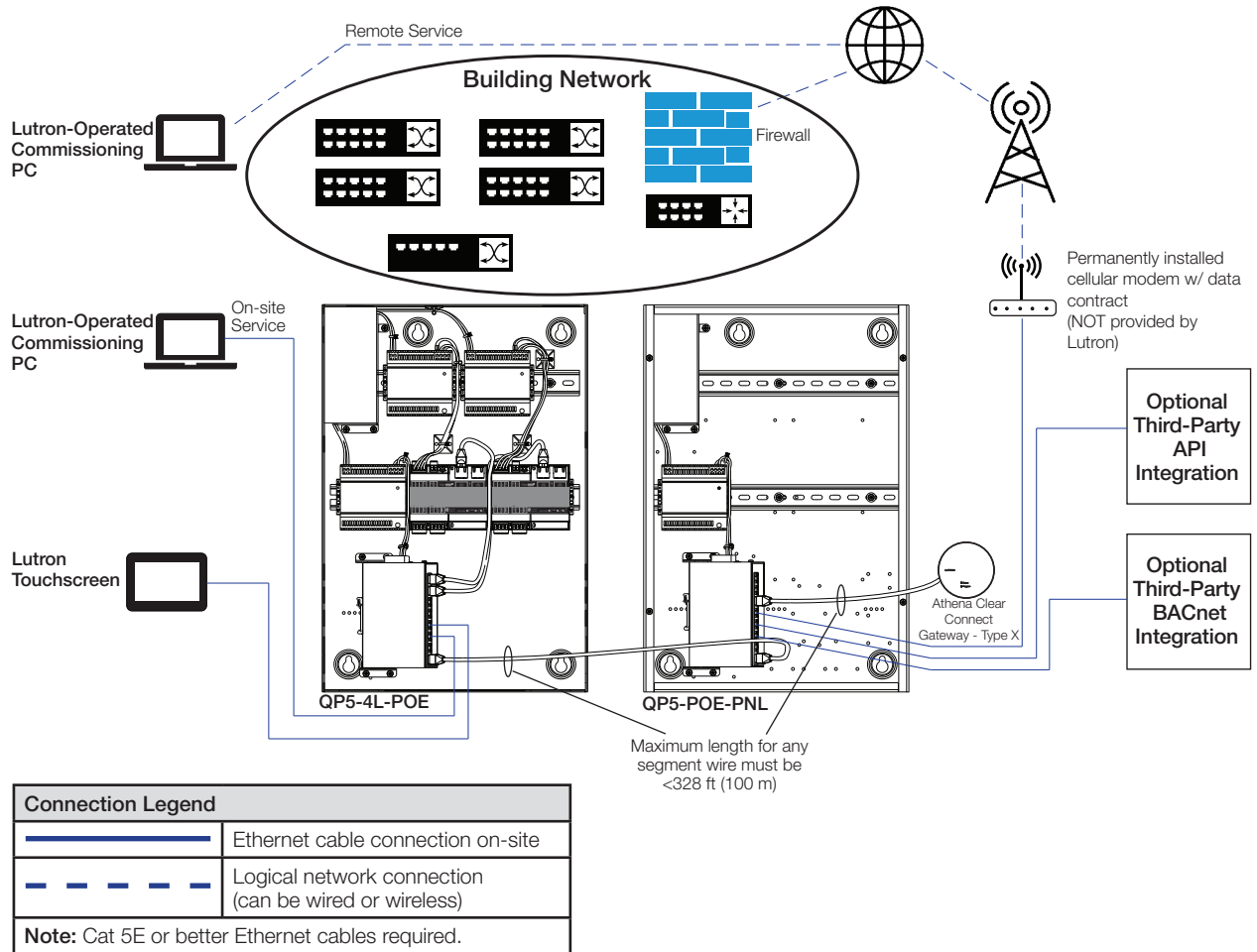
Athena System During Startup/Maintenance with Building Network (Option 3: A Second ISP Connection)



Ethernet Cable Wiring Diagram

Connected Mode *(continued)*

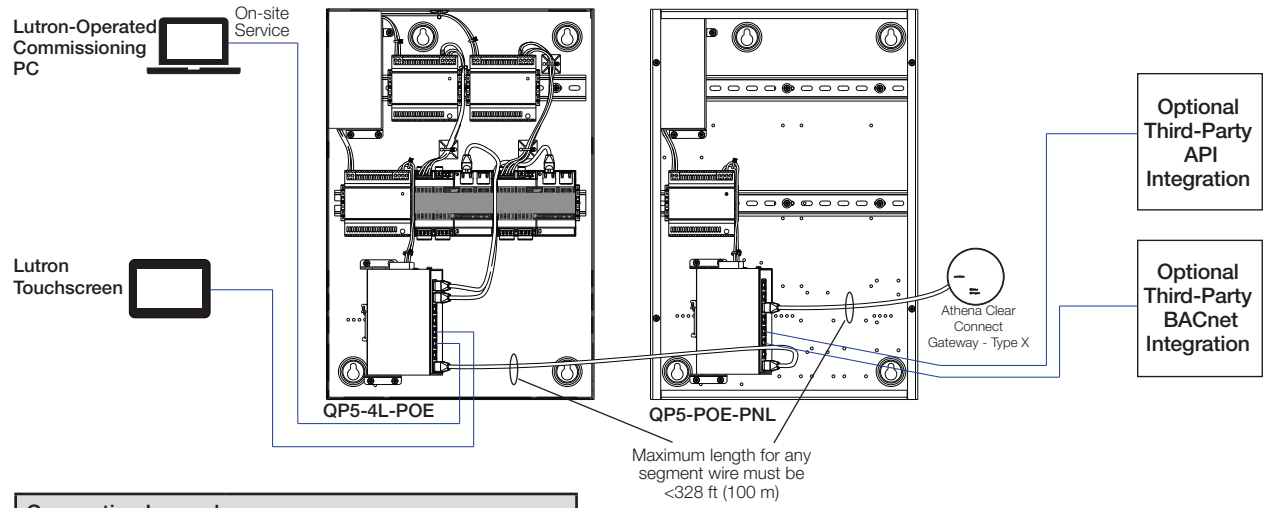
Athena System During Startup/Maintenance with Building Network (Option 4: Permanently-Installed Cellular Modem)




Ethernet Cable Wiring Diagram

Server Mode

Athena System During Startup without Building Network

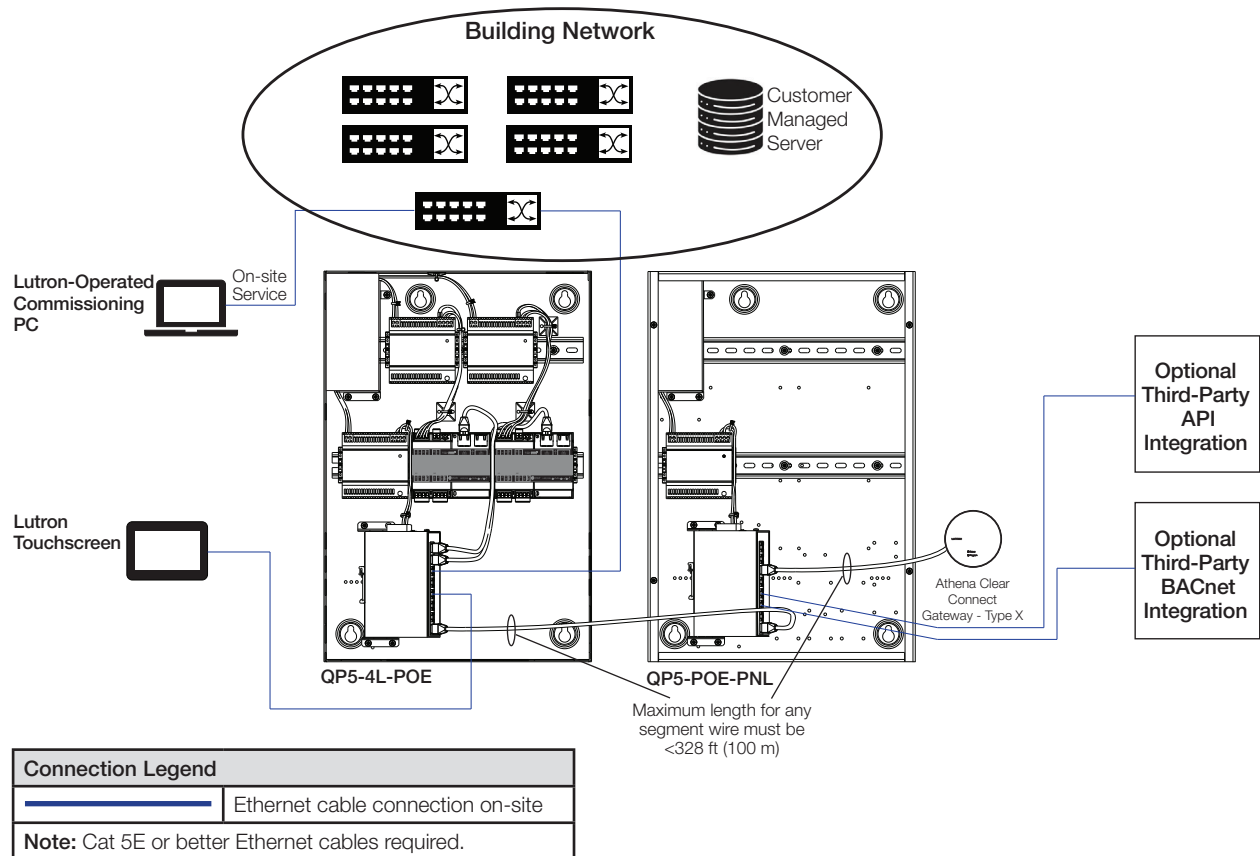


Connection Legend	
	Ethernet cable connection on-site
Note: Cat 5E or better Ethernet cables required.	

Ethernet Cable Wiring Diagram *(continued)*

Server Mode *(continued)*

Athena System During Startup/Maintenance with Building Network (Option 1: Single Connection to Customer LAN)

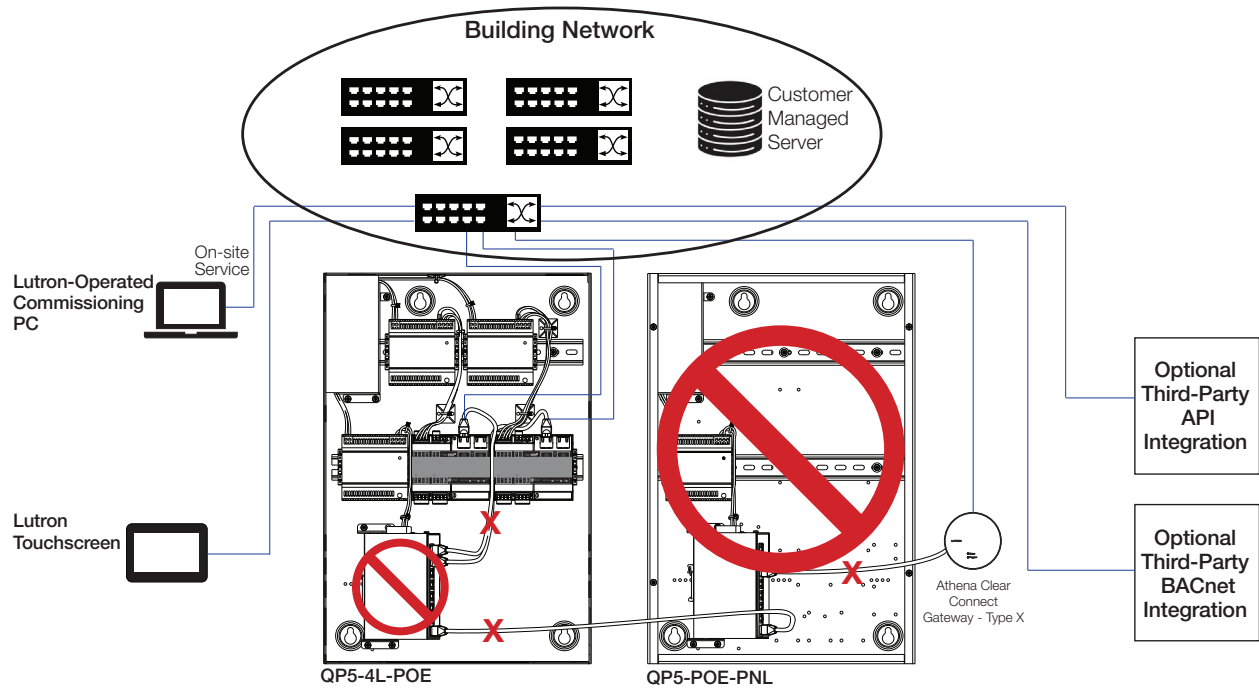


Ethernet Cable Wiring Diagram *(continued)*

Server Mode *(continued)*

Athena System During Startup/Maintenance with Building Network (Option 2a: Multiple Connections to Customer LAN)

Note: Under this wiring configuration, if the building network fails, lighting controls may fail.



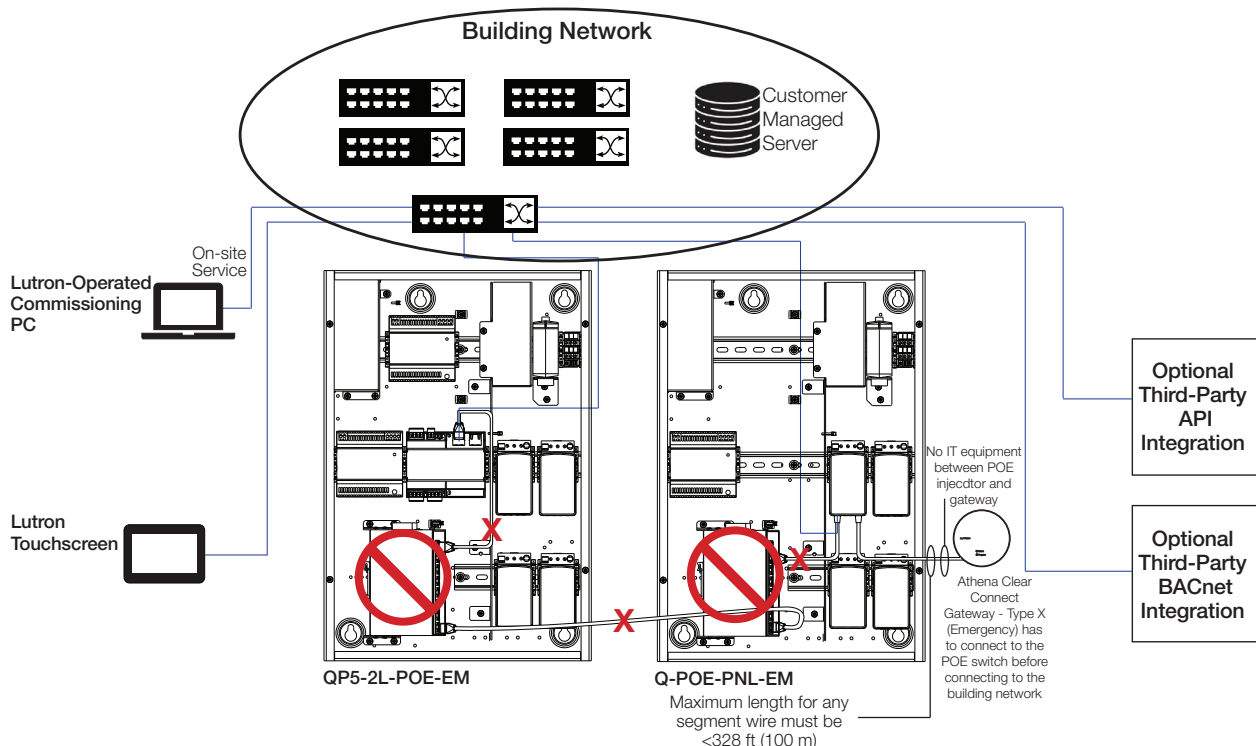
Connection Legend	
	Ethernet cable connection on-site
	Disconnect and abandon in place
Note: Cat 5E or better Ethernet cables required.	

Ethernet Cable Wiring Diagram *(continued)*

Server Mode *(continued)*

Athena System During Startup/Maintenance with Building Network (Option 2b: Multiple Connections to Customer LAN - with QP5-2L-POE-EM)

Note: Under this wiring configuration, if the building network fails, lighting controls may fail.



Connection Legend	
	Ethernet cable connection on-site
	Disconnect and abandon in place
Note: Cat 5E or better Ethernet cables required.	

Server Mode Setup Overview

Purpose of Server Installer

The server installer is designed to install, configure, and initialize the server application stack within customer-managed environments. It provides a structured, guided, and repeatable deployment process to ensure consistent and reliable installation. Refer to the **Infrastructure and Server Preparation** for available operating systems and further details.

The server installer supports the following installation scenarios:

- Fresh installation onto a new server
- Upgrade of an existing installation to a newer build version
- Re-installation or repair to an existing server

This section of the guide outlines the system prerequisites, installation procedures, post-installation validation steps, and troubleshooting guidance required to successfully deploy and operate the Server Installer.

Installer Files

Latest server installers will be made available at <https://designer-installers.iot.lutron.io/releases-server-mode/archive.html>

There are two installers available:

- Windows Installers
 - Lutron-server-mode-installer-`<“latest version”>-windows.zip`
- Linux Installer
 - Lutron-server-mode-installer-`<“latest version”>-linux.tar.gz`

Pre-requisites for Server Installer

Before starting server installation, the FSE must obtain a completed “IT Checklist” from the IT team responsible for preparing the server environment for the Lutron dashboard.

All prerequisites in the below checklist must be completed before installation begins. Failure to meet these prerequisites may result in installation failure or an unsupported deployment. Both the FSE and the IT team should retain a copy of the completed checklist for future reference.

IT Checklist

Infrastructure & Server Preparation	Check Item	Required Condition	Confirmed (Yes/No)	Remarks/Enter value
	Server created	Server provisioned & accessible		
	OS Installed	A supported OS is installed and running on server		
	Server access	Able to login in to server as root/administrator access		
	System Time & Timezone	Correct date & Timezone		
Network Ports	Protocol/Port	Required Condition	Confirmed (Yes/No)	Remarks/Enter value
	Inbound - TCP/443	As per Firewall rules		
	Inbound - TCP/8883	As per Firewall rules		
	Outbound - TCP/587(SMTP Port)	As per Firewall rules		
	Outbound - TCP/443	As per Firewall rules		
Domain Name and Certificate Requirements	Check Item	Required Condition	Confirmed (Yes/No)	Remarks/Enter value
	FQDN Defined	Customer has provided domain name Ex: dashboard.lutron.com Make sure it should not have https prefix		
	FQDN Resolves to Target IP	DNS Entries has been created for domain name with server IP		
	Certificates file	Customer shared the certs with below filenames 1.Key File(server.key) 2.CERT File(server.crt) 3.CA File(ca.crt) and above files are copied in to /etc/ssl/lutron_dashboard_certs/ directory		
	CERTS Validation	Certificate Not Expired		
	Cert Copy	Cert file has been copied in to machine in following directory Ubuntu: /etc/ssl/lutron_dashboard_certs/ Windows: /etc/ssl/lutron_dashboard_certs/		
IDP (BYOI – Bring Your Own Identity)	Check Item	Required Condition	Confirmed (Yes/No)	Remarks/Enter value
	Confirmed IDP Provider	The IDP is confirmed to be either SAML or OIDC		
	If OIDC -> Client ID Client Secret Tenant ID	OIDC credentials are available and shared		
	If SAML-> IDP Metadata (File/URL) Entity ID SSO Endpoint Signing Certificate	SAML credentials are available and shared		
SMTP Server Configuration (Optional)	Check Item	Required Condition	Confirmed (Yes/No)	Remarks/Enter value
	Is SMTP server required by customer	SMTP is optional, though recommended to have available for initial installation if needed		
	If SMTP is required-> SMTP Host or IP address SMTP Port Username Password Sender Email TLS/SSL Requirements (if appl.)"	If SMTP required, Customer should provide all those information		
Administrative Access	Check Item	Required Condition	Confirmed (Yes/No)	Remarks/Enter value
	Root / Admin access	Person responsible to execute the installer on the server has this access.		
Copy Installer	Check Item	Required Condition	Confirmed (Yes/No)	Remarks/Enter value
	Installer file must be copied in to VM	For Ubuntu: /opt/lutron/downloads For Windows: C:/lutron/downloads		

Pre-requisites for Server Installer *(continued)*

Infrastructure and Server Preparation

The target system must be provisioned and ready before installation as per the the specifications outlined in the **Athena Dashboard Software** specification submittal (P/N 3691245) at www.lutron.com

- Virtual/physical machine must be created and accessible via the defined network ports.
- Operating system installed must be Ubuntu 24.04, Windows Server 2022 (64-bit), Windows Server 2025 or Windows Pro 11.
- The FSE must have administrator/root access to the server.
- System time and time zone must be configured appropriately.

Network Ports

Please see the **Firewall/Routing Requirements** section. Refer to **Mode** column for the requirements applicable for **Server Mode**.

Pre-requisites for Server Installer *(continued)*

Domain Name and Certificate Requirements

The Lutron dashboard server mode application is accessed over HTTPS and requires a customer-provided TLS certificate corresponding to the domain name on which the application will be deployed.

The installer does not generate public TLS certificates. Certificates must be provisioned prior to installation.

Domain Name Requirement

IT must define a fully qualified domain name (FQDN) for the application (example: dashboard.customer-domain.com)

- The selected FQDN must resolve to the target system IP address and that should be stable for the lifetime of the deployment.

Certificate Ownership and Responsibility

TLS certificates must be provisioned and managed by the customer. Certificates should be issued by a publicly trusted Certificate Authority (CA). See below for the list of supported CAs. The customer is responsible for the timely renewal and rotation of certificates in accordance with industry best practices.

- Certificates may be issued by one of the following publicly trusted Certificate Authority.
 - Actalis
 - Amazon Trust Services
 - Buypass
 - DigiCert
 - emSign
 - Entrust
 - GeoTrust
 - GlobalSign
 - GoDaddy
 - HARICA
 - IdenTrust
 - Let's Encrypt
 - Microsoft
 - QuoVadis
 - Sectigo (Comodo)
 - SSL.com
 - Starfield
 - SwissSign
 - Telia
 - Trustwave

The customer is responsible for renewal and rotation – follow the industry standard.

Pre-requisites for Server Installer *(continued)*

Identity Provider (IDP)

This section describes the steps required to configure a customer-managed Identity Provider (BYOI – Bring Your Own Identity). This can be done during installation (recommended) or post-installation. Server mode supports the following Identity Provider types:

- SAML
- OIDC

Each IDP type requires a defined set of configuration inputs provided by the customer during onboarding.

OIDC IDP – Required Installation Inputs

During installation, the administrator shall provide the following inputs for OIDC configuration:

- Input 1: Tenant ID
- Input 2: Client ID
- Input 3: Client Secret

SAML IDP – Installation Inputs

During installation, the administrator shall provide the following inputs for SAML configuration:

- Input 1: IDP Metadata URL
- Input 2: IDP Entity Identifier
- Input 3: Single Sign-On (SSO) Endpoint
- Input 4: IDP Signing Certificate

SMTP Server Configuration (Optional)

The application supports email notifications for system alerts and operational events. This configuration is optional and not required at time of installation. Lutron dashboard Server mode will function normally with exception of email notifications.

Configuration Requirements

If the customer requires email notifications, the following SMTP details must be available prior to installation:

- SMTP server hostname or IP address
- SMTP server port
- Authentication username & password
- Sender email address
- TLS/SSL requirements (if applicable)

Pre-requisites for Server Installer *(continued)*

Administrative Access

Installer must be executed from an elevated shell or command prompt. IT will need to provide admin access to FSE in order to perform the installation process

- Linux: Root or sudo access is required
- Windows: Local administrator privileges are required

Copy Installation File

The latest installation file must be copied onto the server into the appropriate location listed below using the company's approved internal process to download the installer from the URL.

<https://designer-installers.iot.lutron.io/releases-server-mode/archive.html>

- For Ubuntu: /opt/lutron/downloads
- For Windows: C:/lutron/downloads

Important Notes:

- Do not extract, rename, or modify the installer package before installation.
- Ensure the file transfer is completed successfully.
- Hand off to the FSE to proceed with installation only after the package is fully available at the standard location.

Finalize and Share Checklist with FSE

Perform final review of all items in the **IT Checklist** section and provide full checklist to the FSE / person performing the installation on the server.

It is strongly recommended to keep a copy of the checklist for future reference when or if needed.

Revision History

Date	Change
March 2026	Added support for server mode
August 2025	Added SOC2 statement
March 2025	Updated some firewall/routing information and added network diagrams
October 2024	Added SSO and proxy information. Updated some firewall/routing information and added network diagrams

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: +1.610.282.3800

Fax: +1.610.282.1243

Visit us on the web at www.lutron.com

Lutron, Athena, Caséta, Clear Connect, HomeWorks, Ketra, myRoom, Pico, Quantum Vue, Radio Powr Savr, RadioRA 2, and any related trade dress and logos are trademarks or registered trademarks of Lutron Electronics Co., Inc. in the US and/or other countries.

All other product names, logos, and brands are property of their respective owners.

