System Network/IT Planning Guide

WaveLinx

This document is intended for Lighting Control Systems and IT professionals

Important: Engage appropriate network security professionals to ensure all lighting control system hardware and servers are secure for access.

Powering Business Worldwide

Table of Contents

1 WaveLinx System Overview

1.1 About the WaveLinx System

WaveLinx is a connected lighting control system that provides easy to install and implement energy code compliance, while providing a framework for future smart building requirements. The system can scale from a single wireless area controller with up to 150 (100 best practice) wireless. connected devices to control the lighting system for a small space to multiple interconnected wireless area controllers for large application spanning more than one building.

The WaveLinx system offers the following advantages:

- **Reduce commissioning time -** The WaveLinx built-in features, such as the construction group or auto creation of dimming and receptacle zones when an area is created, reduce the time by 40% or more compared to other addressable lighting systems. The WaveLinx Mobile App offers an intuitive user interface that allows the installer to program the lighting system conveniently from their smart phone.
- **Improve data collection for better decision making -** Using fixtures with the WaveLinx integrated sensor allows you to gather more granular data on how your space is being used. The data can then be used to make more informed decisions with regards to space and energy usage.
- **Monitor system health -** The Alarms console with Smart Tips allows facility manager to monitor the health of their WaveLinx system and quickly address issues using troubleshooting tips aggregated from years of industry experience. Alarms can also be sent to facility managers as emails.
- **Easily connect lighting system to other systems -** The BACnet/IP interface and Public (REST) API allows system integrator to easily integrate networked WaveLinx area controllers with a Building Automation System. The BAS can read and write to the WaveLinx areas, zones and devices.

1.2 About WaveLinx Wireless Protocol

The WaveLinx wireless network is built using the Institute of Electrical and Electronics Engineers (IEEE) 802.15.4 standard and follows strict IEEE guidelines to ensure long-term sustainability and reliable operation. The IEEE 802.15.4 standard is used for data exchange between WaveLinx input and output devices (sensors, receptacles, wallstations, etc…) and the Wireless Area Controllers. The wireless network is used to control the light fixtures and controlled receptacles as well as gather energy and occupancy data.

2 Acronyms

Acronyms	Description
API	Application Programming Interface
IEEE	Institute of Electrical and Electronics Engineers
LAN	Local Area Network
PoE	Power over Ethernet
REST	Representational State Transfer
TC	Trellix Core
WAC	Wireless Area Controller

3 References

1. Cybersecurity considerations for electrical distribution systems, Eaton White Paper, Nov 2016

4 System Architecture

This section covers the architecture of a WaveLinx system.

4.1 Device Types

The WaveLinx system comprises the following device types:

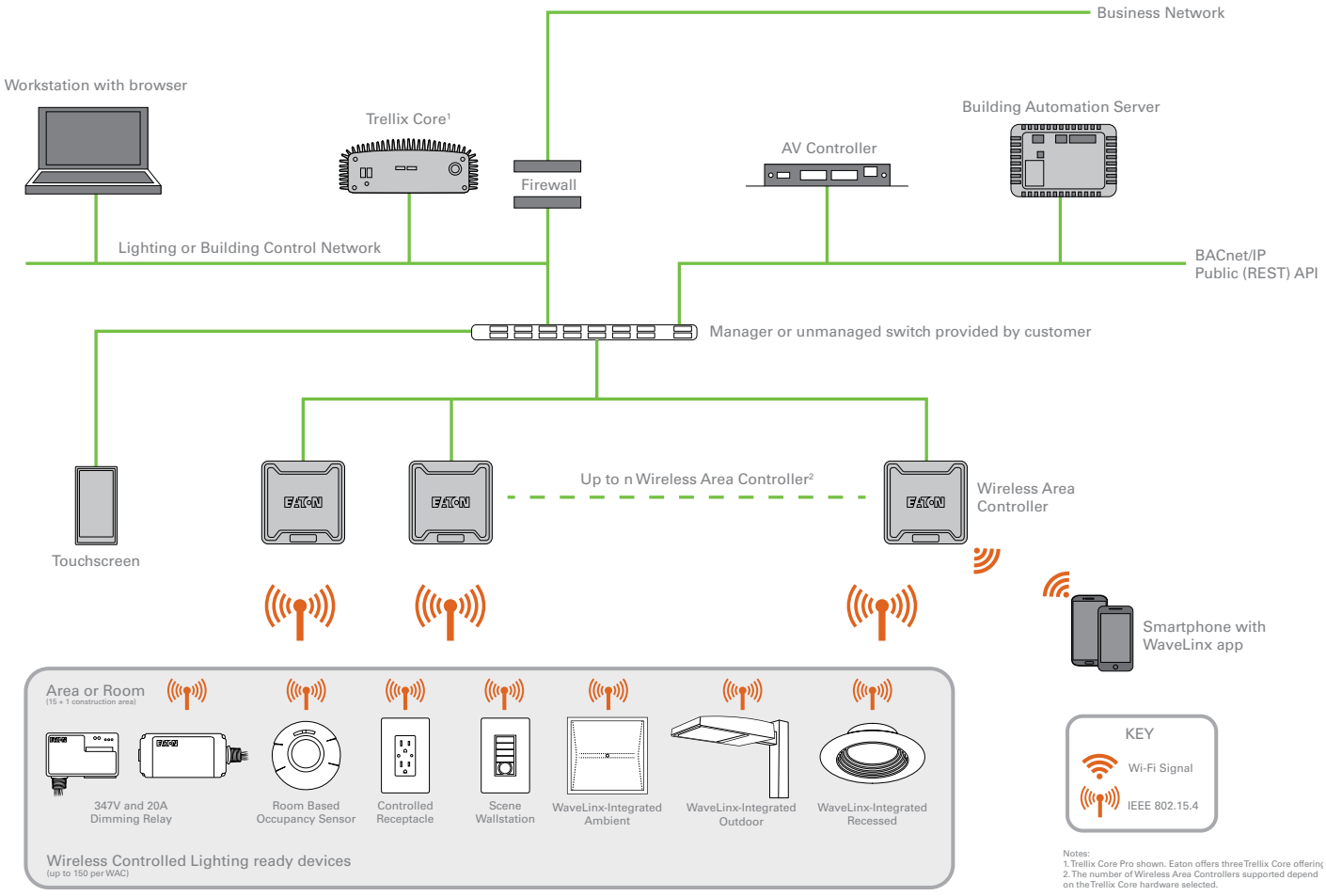
Output devices – A device that directly controls the voltage of the lighting load. This is typically a driver, ballasts, relay or other load control device such as receptacles.

Input devices – A device that issues a signal to the output device either directly or via a wireless area controller to control a lighting load. This may be an occupancy sensor mounting in a ceiling or within the fixture, a wallstation or contact closure.

Programmable Controller – A device that manages runs code-compliant control strategies for the spaces that it controls. The controller communicates with the input and output devices wirelessly.

Software application – A software applications that allows users to configure and manage a standalone or networked programmable controllers. The application aggregates data from the various controllers and exposes it to other systems via various interfaces.

The diagram below shows as a typical WaveLinx system:



4.1.1 Output Devices

120-277VAC Wireless Relay Switchpack with 0-10V (Relay zone control) - This device offers 120-277VAC 20 amp zero crossing relay control and continuous 0-10V dimming control of LED and non LED loads. The device can also be used to control 20amp plug loads. The device is powered by the 120-277VAC circuit it is controlling. It communicates wirelessly with the WaveLinx Wireless Area Controller. The Wireless Relay Switchpack operates on the WaveLinx network based on IEEE 802.15.4 standards.

120-347VAC Wireless Relay Switchpack with 0-10V (Relay zone control) - This device offers 120-347 20 amp zero crossing relay control and continuous 0-10V dimming control of LED and non LED loads. The device can also be used to control 20amp plug loads. The device is powered by the 120-347VAC circuit it is controlling. It communicates wirelessly with the WaveLinx Wireless Area Controller. The Wireless Relay Switchpack operates on the WaveLinx network based on IEEE 802.15.4 standards.

Wireless Receptacle (Wall mounted power outlet) - The wireless receptacle provides simplified wireless plug load control. Plug load control is required now in many building codes as part of an energy saving control strategy. The wallbox mounted wireless duplex receptacle provides a constantly powered bottom outlet and a wirelessly controlled top outlet. The NEMA wireless receptacle includes the NEMA symbol for identifying a controlled receptacle as well as tamper resistant outlets for safety. The Wireless Receptacle operates on the WaveLinx network based on IEEE 802.15.4 standards.

4.1.2 Input Devices

Wireless Wallstation (Manual lighting and scene control) - WaveLinx wallstation is a multi-scene, single area dimming wireless wallstation which provides customized light level for each area. The wallstation provides default sequence of operations including 50% light level, scene light levels between 30-70% as well as 100% and full off. Many wallstation configurations also include scene raise/lower buttons to further adjust the light levels. Each button is fully configurable via the WaveLinx Mobile Application to provide local and multi-level control in each area. The wallstation are line-voltage powered and operate on a wireless mesh network based on IEEE 802.15.4 standard.

Wireless Integrated Sensor (Fixture integrated occupancy sensor, ambient light sensor and control) - The integrated sensor combines control within the light fixtures to reduce installation and design time; while meeting energy codes. The integrated sensor incorporates Passive Infra Red (PIR) technology for occupancy control with photocell technology for daylight harvesting. The integrated sensor's small form factor enables sensing capabilities to a wide breadth of lighting products. The WaveLinx Integrated sensor operates on a wireless mesh network based on IEEE 802.15.4 standard.

Wireless Tilemount Sensor Kit (Fixture with remote ambient light sensor and control) - The WaveLinx Tilemount Sensor Kit offers a 120-277VAC 3amp zero crossing relay control and continuous 0-10Vdimming control of LED and non LED loads. The intended use of the Tilemount Sensor Kit is to provide motion sensing, daylight dimming, and control for connected downlight luminaires or other luminaires that do not support the WaveLinx integrated sensor. The WaveLinx Tilemount Sensor Kit operates on the IEEE 802.15.4 wireless mesh network.

Wireless Ceiling Sensor - The wireless ceiling sensor offers Passive Infra Red (PIR) occupancy sensing. It has a coverage pattern of up to 1500 square feet. The sensor is battery powered and is one of the smallest ceiling mounted room based wireless occupancy sensors on the market. The sensor operates on the WaveLinx network based on IEEE 802.15.4 standard.

WaveLinx Touchscreen - The touchscreen provides an elegant and discreet light control for any WaveLinx controlled space by allowing users to recall the light scenes/presets defined for the area and to raise/lower the light level for the entire area or the zones defined within an area. The touchscreen communicates with the associated Wireless Area Controller via the ethernet network.

4.1.3 Area Controller

Wireless Area Controller (Gateway) - The Wireless Area Controller (WAC) hosts the wireless network manager, wireless network security manager, wireless network gateway and area controller application. The WAC coordinates the communication between the wireless input and output devices. The user will configure the control strategy for the areas/zones covered by the WAC using the WaveLinx Mobile App. A single WAC can coordinate up to 16 areas. The Wireless Area Controller provides centralized coordination of multiple areas for partial ON/ partial OFF scheduling, demand response, lighting, occupancy and daylight settings and scene control. Multiple WAC's can exist on a building LAN to scale the system to hundreds of areas all accessible for setup, configuration and control through the WaveLinx Mobile App.

4.1.4 Supervisory System

Trellix Core - The Trellix Core is an on-premise hardware platform hosting the Trellix Apps including Trellix Lighting and Trellix Admin which are used to manage the lighting system as well as the integration interfaces (BACnet/IP and Public (REST) API. To compliment WaveLinx, multiple Trellix Core hardware options are available to optimize the return on investment of a connected lighting system: Pro, Enterprise and Virtual. The Trellix Core Pro is used for WaveLinx systems composed with up to twenty (20) wireless area controllers while the Trellix Core Enterprise is used for systems composed with up to five hundred (500) wireless area controllers. For customer hosting their building automation systems on a VMWare vSphere environment, Trellix offers a virtual variant of its Trellix Core Enterprise.

4.1.5 Software and Interfaces

WaveLinx Mobile App - The WaveLinx Mobile App enables users to perform setup, configuration and maintenance of the WaveLinx system from a wireless smartphone. It allows users to easily define Areas, Zones, Occupancy Sets and Daylight Sets and associate devices to them. It also allows users to define the time-base control strategies for the spaces controlled by the Wireless Area Controller as well as the actions for the WaveLinx wallstations' buttons.

Trellix Lighting - The Lighting application allows users to configure and monitor a code-compliant connected-lighting system designed to create an energy-efficient space. With this application, you can perform high-level supervisory tasks such as making changes to the light levels, creating lighting schedules and viewing your lighting system's energy usage. It is also the foundation for the sensing network and other advanced applications that leverage the data gathered by the system.

Trellix Admin - The Admin application allows users to perform the administrative tasks required to manage the Trellix Core services such as enabling/disabling interfaces, creating/editing/deleting users and roles, backing up/restoring configuration databases and upgrading the platform.

BACnet/IP Interface - Trellix BACnet/IP Interface enables the integration between the WaveLinx systems with any BACnet/IP compatible Building Automation System (BAS). BACnet is a data communication protocol for Building Automation and Control Networks developed by the American Society of Heating Refrigeration and Air Conditioning Engineers (ASHRAE).

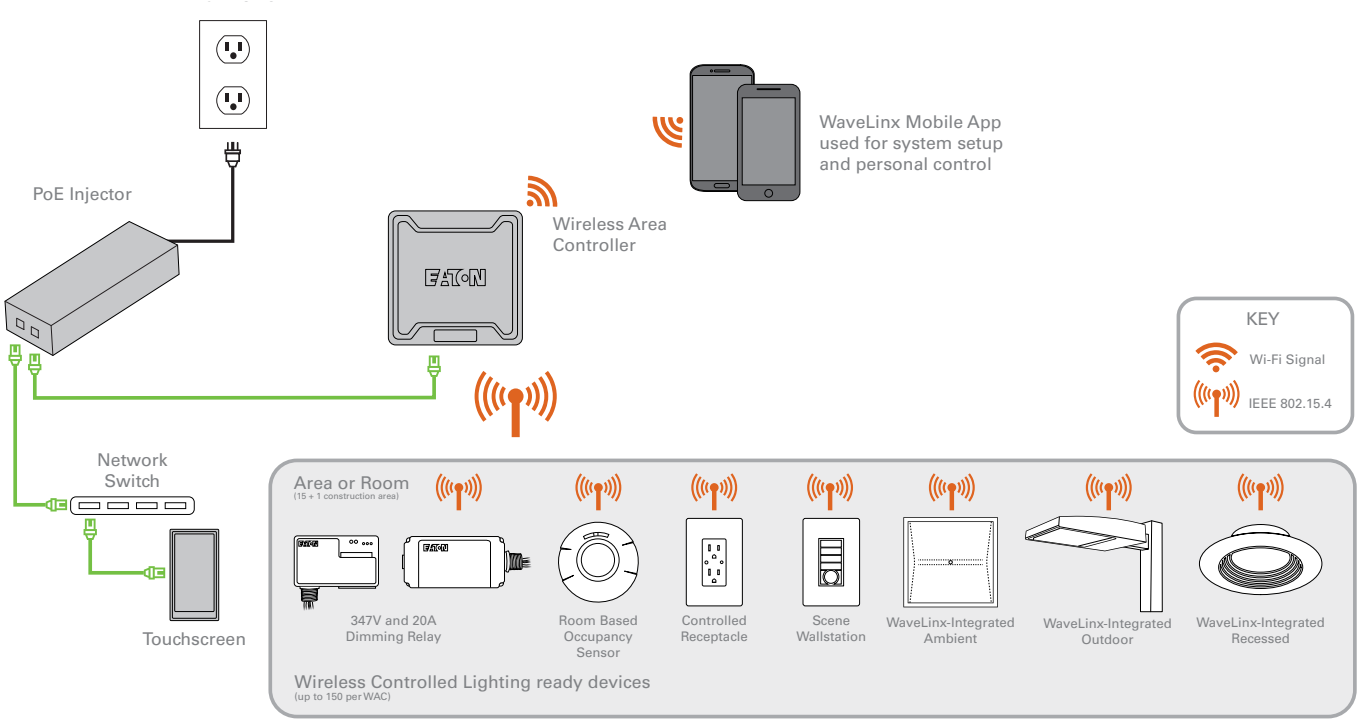
Public REST API - Trellix set of APIs enables third party IoT platforms to take control ofWaveLinx connected devices such as integrated sensors and incorporate them into a desired customer experiences. The Public REST APIs allow third party developers to issue control commands to areas, zones and devices and read lighting information from the areas, zones and devices as well as the lighting building hierarchy.

4.2 System Topologies

The WaveLinx system can be installed either with standalone area controller or as a distributed lighting control system, i.e. networked area controllers with a supervisory system. The section below explains the Dedicated and Network installation methods.

4.2.1 Standalone Topology

The standalone topology shown below is recommended for facilities/spaces where there is no need for a supervisory system, i.e. typically a small to medium size buildings



In a standalone topology, the Wireless Area Controllers installed within the building are not connect to a local area network (LAN) or a wireless local area network (WLAN). Each Wireless Area Controller would communicate to up to 150 wireless input/output devices in star-mesh topology. The Wireless Area Controllers are mounted centrally located above the ceiling in the spaces that they are meant to control. The power can be provided either via a POE switch or the POE Injector shipped with each Wireless Area Controller as shown in above illustration.

In a standalone topology the Wireless Area Controller acts as a:

Network Coordinator - As a network coordinator, the Wireless Area Controller is responsible for overall 802.15.4 network management. Each WAC only supports one 802.15.4 network. As a network coordinator, the Wireless Area Controller performs the following functions:

- Selects the channel to be used by the network
- Starts the network
- Manage devices addresses
- Permits other devices to join the network
- Holds a list of neighbors and routers
- Transfers application packets

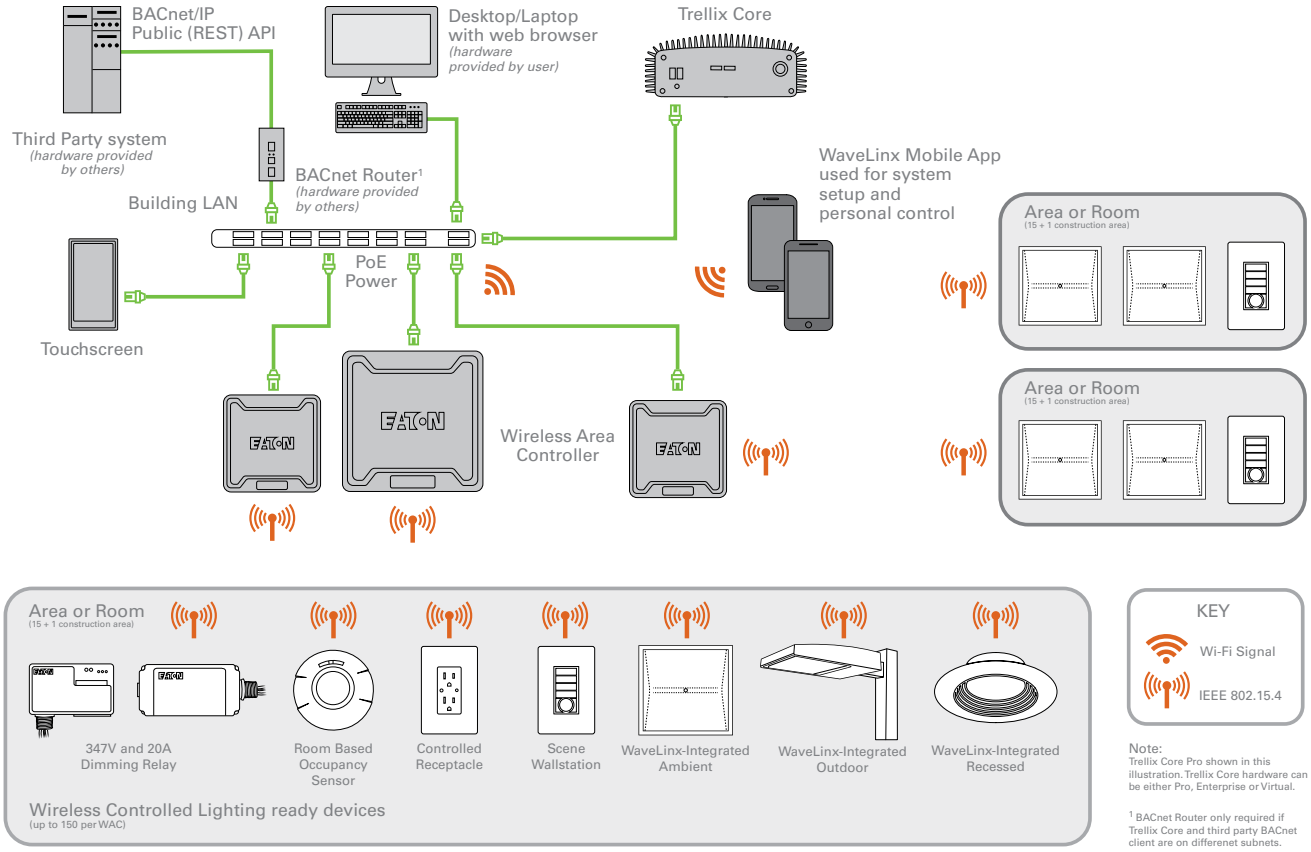
Security Manager - As a security manager, the Wireless Area Controller provides security management, security key distribution, and device authentication for the 802.15.4 wireless network.

Area Controller - As the area controller, the Wireless Area Controller manages the control algorithm for the devices connected to it. The area controller sends the control commands to the output devices based on received data from the input devices (occupancy sets, daylight sets, wallstations, etc…). The device acts as the master clock for the system. As such all time-based actions are coordinated from the wireless area controller while occupancy and daylight-based actions are executed by the sensor (ceiling or integrated). The device also monitors the health of the devices connected to it.

Gateway - As a gateway the Wireless Area Controller connects the wireless network to other networks, i.e. a LAN and WLAN. The wireless area controller also acts as Wi-Fi access point which is used by a system installer to configure and monitor the areas covered by the devices connected to the Wireless Area Controller. The system installer uses a smart phone with the WaveLinx Mobile Application to configure the system. The smartphone connects to the Wireless Area Controller using WPA2 wireless encryption and secure network username and password. The system installer also uses the Wireless Area Controller's secure HTTPS (TLS1.2) web pages to setup the Wireless Area Controller's network settings.

4.2.2 Networked Topology

The networked topology shown below is recommended for facilities/spaces where users want to manage the WaveLinx from a central location and where the WaveLinx system needs to exchange data with other systems installed within the building such as the Building Automation System, security system, Audio Visual (AV) system, shades system. The networked topology is often required for medium to large size buildings.



In a networked topology, the Wireless Area Controllers and Trellix Core installed within the building(s) are connected to v a common local area network (LAN). The Trellix Core only supports wired Ethernet connections while the Wireless Area Controller can also communicate via a wireless local area controller (WLAN) as the Wireless Area Controller supports both wired and wireless Ethernet connections. The LAN can be dedicated to the lighting control system or shared with the other systems installed as part of the building's automation system.

Similar to the standalone topology, each Wireless Area Controller would act as the device network coordinator, security manager, zone controller and gateway for up to 150 devices connected to the 802.15.4 wireless network.

In addition to the Wireless Area Controllers, a networked topology includes Trellix Core. The Trellix Core is the supervisory computer that host the Trellix Apps, i.e. Trellix Admin and Trellix Lighting.

In a networked topology, the Trellix Core acts as:

- **Supervisory Software Host -** The Trellix Core hosts the Trellix Lighting and Admin apps, for its connected lighting systems. The Trellix Apps include web-based HMIs that allow users to configure and manage the lighting system.
- **System repository -** As the system repository, the Trellix Core gathers data from the devices via the Wireless Area Controllers and stores it on the hardware (limited to system faults).
- **System Management -** As the system manager, the Trellix Core will govern the lighting system and all devices connected to the system from a single location. It will monitor the health of the system's components and alert users when faults/issues are detected.
- **Gateway -** The Trellix Core acts as the IoT hub for the WaveLinx system. It hosts the interfaces used by third party systems to read/write to the WaveLinx system. These interfaces include BACnet/IP and Public (REST) API.
- **Security Manager -** As the security manager, the Trellix Core ensures that the data is securely accessed by only authorized users. events management, exposing the data from the area controllers to third party system via BACnet and Public API (REST), user management and system backup.

The Trellix Core will be connected to the LAN via its wired Ethernet port. Please note that unlike the Wireless Area Controllers, the Trellix Core does not offer a wireless Ethernet interface. The Trellix Core is typically installed in the server/IT room.

If the network switch provided by the customer is PoE enabled, there is an additional incentive to use the PoE ports to power and connect the Wireless Area Controllers. If there are no PoE ports available or the distance between the switch and the Wireless Area Controller exceeds the 300 ft limit for PoE then the POE Injector shipped with each Wireless Area Controller can be used to power the Wireless Area Controller (refer to standalone topology to learn more about the PoE injector).

In a networked topology, the Wireless Area Controller will obtain the IP addresses for their wired Ethernet address automatically via DHCP. Alternatively, the IT administrator can assign a static IP address for any Wireless Area Controller. For the Trellix Core, the IT administrator need to assign a static IP address which will be used when configuring the Trellix Core.

At the discretion of the building IT personnel, the WaveLinx system may be setup on a dedicated lighting network LAN/VLAN or be part of the building automation network LAN/VLAN.

Once connected the LAN, user can then integrate their WaveLinx system via the Trellix Core to third party systems such as Building Automation Systems, shades control system and AV control systems. Please refer to the Third-Party System Integration section to learn more about network considerations.

In a network topology, the user will program the WACs using the WaveLinx Mobile App while monitoring the system using the Trellix Lighting app. If the WaveLinx system is connected to a WLAN then the user can connect their smartphone to the WLAN to program the WACs. Alternatively, they can connect their smartphone to each WAC's Wi-FI access point to program the areas controlled by the WAC.

Note: The networked topology does not support peer-to-peer control nor virtual areas/zones spanning across multiple WACs.

5 Software/Firmware Compatibility Matrix

To ensure that the WaveLinx system is operating efficient, the user shall ensure that all the Trellix Cores and Wireless Area Controllers have compatible software/firmware. Please refer to the software/firmware compatibility matrix included in the software release notes.

6 IT Network Information

6.1 LAN/WLAN

A LAN or WLAN is only required in the case of a networked topology where third party systems need to exchange data with the WaveLinx system and users need to monitor the system from a central location using Trellix Lighting application hosted on the Trellix Core.

6.2 VLAN

The WaveLinx system support multiple VLAN topology, i.e. where the Wireless Area Controllers and Trellix Core are located on different VLANs.

When implementing in a multiple VLAN environment, you must ensure that all the IP based WaveLinx devices, i.e. Trellix Core, Wireless Area Controllers, computing devices (laptop, smart mobile), can exchange data across the VLANs. Please refer to the network ports section to ensure that the network switches/firewalls are properly configured to allow the data flow between these devices.

6.3 Network Ports and Usage

6.3.1 Wireless Area Controller

To ensure proper system operation, the following network ports and protocols must be available to allow users to interact with the Wireless Area Controllers via the LAN.

Protocol	Port	WaveLinx Device	Usage	Status	Security
TCP	80	WAC	Redirects to Configuration Webpages	Always Open	TLS 1.2
TCP	443	WAC	Configuration webpages	Always Open	TLS 1.2
TCP	52725	WAC	SSL secured Common API (CAPI) web services	Always Open	
TCP	52425	WAC	SSL secured CAPI web socket	Always Open	TLS 1.2
UDP	67	WAC	DHCP Server	Only open in Standalone Topology	
UDP	68	WAC	DHCP Server		
UDP	546	WAC	DHCPv6	Closed when in Connected Topology	
UDP	547	WAC	DHCPv6		
UDP	5353	WAC	mDNS (Avahi)	Always Open	
TCP	22	WAC	SSH	Closed by default. Admin may webservice request	TLS 1.2

6.3.2 Trellix Core

The following inbound and outbound ports are used by the Trellix Core in a networked topology.

Inbound Protocol to IM	Inbound Port to IM	Outbound Protocol from IM	Outbound Port from IM	Usage	Status
TCP	443			WEB Application	HTTPS. Always Open
TCP	443			Public API	HTTPS. Always Open
UDP - Braodcast	47808			BACnet	BACnet. Open when BACnet is enabled. Same subnet otherwise BACnet router is needed.
UDP - Multicast	5353			Discovery (mDNS) of the Wireless Area Controllers (optional)	Always open. **Same subnet** otherwise enable multicast over subnets using L3 switch by bridging/forwarding.
TCP	8761			Web Eureka Access	HTTPS . Always open for troubleshooting.
		TCP	52425	Connection to WAC	Secure WebSocket to WAC
		TCP	25 or 465 or 587 or any other port	SMTP Access	Depends on the SMTP server used
		UDP	123	NTP Client	if configured
		TCP/UDP	53	DNS	If configured

6.4 IP Address Assignment

6.4.1 IP Address Assignment (DHCP or Manual)

Below table captures how the various WaveLinx components obtain their TCP/IP address.

Table 2: IP Address Assignments

Device	Interface	Dynamic Addressing	Static Addressing	Notes
Wireless Area Controller	LAN Interface	Supported (default)	Supported	
			Default: 192.168.1.XXX Note: 192.168.100.XXX subnet cannot be used as it is reserved for the Wi-Fi AP.	• The WAC is the controller and gateway to the WaveLinx devices. • The WAC separates the IT and OT networks • The WAC is centrally located in the space above the ceiling (preferred) to wirelessly communicate to the OT WaveLinx devices via IEEE 802.15.4 • 192.168.100.XXX subnet is reserved for the Wi-Fi AP interface
	WLAN Interface	Supported	Supported Default: 192.168.1.XXX Note: 192.168.100.XXX subnet cannot be used as it is reserved for the Wi-Fi AP.	
	Wi-Fi Access Point	Not Supported	192.168.100.1	
Smart Device (phone or tablet)		Supported		• DHCP address provided by WAC when installed as a dedicated WaveLinx installation • DHCP address provided by building IT wireless access point when installed as a network WaveLinx installation
Trellix Core		Not Supported		• DHCP server can be used to reserve an IP address for the Trellix Core.

6.4.2 IPv6 Readiness

The Wireless Area Controller and Trellix Core hardware are designed to be IPv6 capable. The input/output devices, currently using IEEE 802.15.4 MAC/PHY, are also Thread and IPv6 capable.

7 WaveLinx Wireless Network

7.1 Wireless Network Overview

The Wireless Area Controller communicates with the lighting control devices (wallstations, sensors, receptacles, etc…) wirelessly. WaveLinx wireless ecosystem uses the Institute of Electrical and Electronics Engineers (IEEE) 802.15.4 standard and follows strict IEEE guidelines to ensure long-term sustainability and reliable operation.

The IEEE, a non-profit organization, is the world's leading professional association for the advancement of technology. IEEE is a globally respected standards development group whose members are volunteers working in an open and collaborative manner. Other well-known technologies like Bluetooth® (802.15.1) and Wi-Fi® (802.11) are also part of the IEEE 802 standards family.

The IEEE 802 group continually evaluates its standards to identify areas of ambiguity or concern and works to improve its standards to ensure robustness and long-term success. To be approved as an IEEE 802 standard, IEEE 802 wireless standards must develop a Coexistence Assurance Document and implement a plan as part of the standard that ensures that all 802 wireless standards can operate and coexist in the same space.

The 802.15.4 standard is a low duty cycle, narrow-band standard that operates in the 2.4GHz ISM band with 16 channels for the 2.4GHz band. Each Wireless Area Controller and associated wireless devices (typically up to 150 wireless devices) can be configured to use a specific IEEE 802.15.4 channel to avoid co-channel interference with other installed devices that also communicate over the 2.4 GHz ISM band. IEEE 802.15.4 channels 11-25, corresponding with 5 MHz-wide frequency bands from 2.405 GHz to 2.480 GHz may be assigned to specific wireless mesh networks.

The wireless communication is secured and encrypted using AES 128-bit encryption.

Other wireless specifications:

- Radio: : 2.4GHz
- Standard: IEEE 802.15.4
- Transmitter Power: +7dBm
- RangEe: 150ft (50m) LOS
- # of Walls: 2 interior walls standard construction

If considering the use of ZigBee Home Automation (HA) based devices not available with the WaveLinx Connected Lighting system, please contact WaveLinx Tech Support.

7.2 Coexisting with Wi-Fi networks

The 2.4GHz ISM band has become particularly popular in the last few years such that households, and virtually all commercial buildings, are likely to have equipment that operates in this band. In today's commercial buildings, one will find many of the following users and possible interferers within the 2.4GHz spectrum:

- 802.11b networks
- 802.11g networks
- 802.11n networks
- Bluetooth
- 802.15.4-based Personal Area Network (PAN)
- Wireless headsets

The policies of the IEEE which require that each standard to include a coexistence statement along with the text of the standard itself. A standard will not be approved until this coexistence statement has been deemed satisfactory. As a result, the IEEE 802.15.4 – 2003 specification provides support for coexistence at both the physical (PHY) layer and the MAC sub-layer.

However despite this requirements, with so many 2.4 GHz devices, one might reasonably be concerned that crowding in the 2.4 GHz band would be a problem.

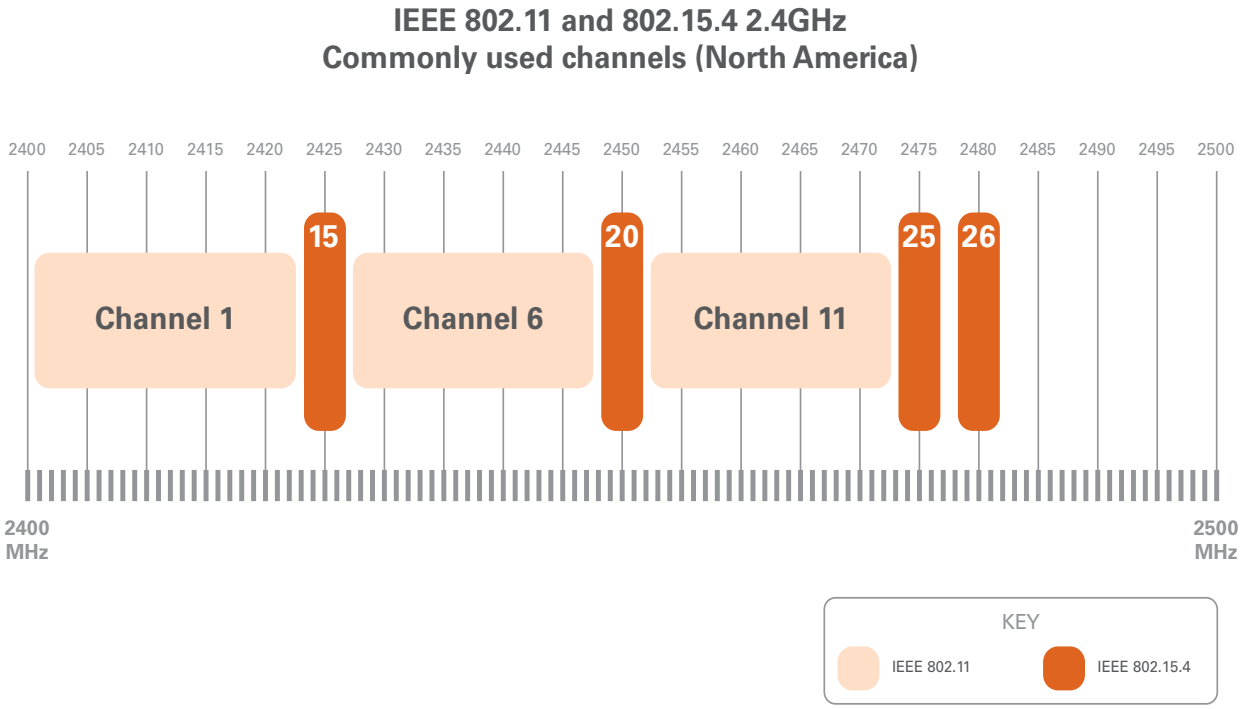
The WaveLinx system employs three techniques to co-exist with the IEEE 802.11 (Wi-Fi) networks in the 2.4 GHz frequency spectrum within the building:

- Channel Selection: This technique involves identifying the IEEE 802.15.4 communication channels that do not overlap with the the deployed IEEE 802.11a/b/g (Wi-Fi) deployment.
- Low Airtime Consumption: WaveLinx is designed to reduce wireless communications during steady state operation, greatly reducing the probability of collision with Wi-Fi traffic.
- Interference Tolerance: WaveLinx is designed to work reliably despite encountering some interference, by detecting if communications packets are lost and retransmitting if needed.

7.2.1 WaveLinx Channel Selection

WaveLinx devices have access to 16 separate, 5MHz channels in the 2.4GHz band. Several of these do not overlap with US and European versions of Wi-Fi. As illustrated in below diagram, channels 15, 20 and 25 fall within the gaps of the Wi-Fi channels. When a wireless network is formed, the Wireless Area Controller is required to scan through the list of available channels using the features provided by 802.15.4, and automatically select the best channel with the least interference. In most instances, the Wireless Area Controller selects the channels that do not overlap with the IEEE 802.11b/g/n channels.

Ultimately this means that IEEE 802.11 Wi-Fi and IEEE 802.15.4 wireless devices can co-exist in the same space without interference if they are properly set with the correct channels.



7.2.2 Low Air time Consumption

WaveLinx recognizes that it is not always possible to select non-overlapping channels. Many Wi-Fi access points aggressively use all available spectrum to maximize performance. To coexist with such solutions, WaveLinx is designed to send two messages every five minutes per sensor. The following example shows the airtime consumption for a 50,000 square foot installation.

- • Airtime Consumption = # sensors*msgs_per_sensor*airtime_per_msg/5mins*100%
- • 50,000 square feet = 500 sensors
- • 1.5 ms of airtime per message
- • Airtime Consumption = 500 * 2 * 1.5ms/5mins * 100%
- • Typical Airtime Consumption = 0.5%

The duty cycle of the WaveLinx network is therefore extremely low; relatively few packet data units are transmitted, reducing the likelihood of an unsuccessful transmission. With such low airtime consumption, the WaveLinx system will easily coexist with Wi-Fi networks whether or not non-overlapping channels are used.

7.2.3 Interference Tolerance

In addition to ensuring that there is no impact on Wi-Fi installations, the WaveLinx system must be tolerant of interference by other Wi-Fi and IEEE 802.15.4 networks. The selection of non-overlapping channels serves to avoid the potential problem.

In addition, WaveLinx is designed to be loss tolerant. The WaveLinx communications increase transmission reliability through the use of acknowledgments and packet retransmission. As a result, when a packet is lost, the loss is detected and corrected through retransmission.

Finally, the WaveLinx system is designed to perform lighting control without requiring network communication at all. Lighting control will continue to operate in the event of a complete wireless failure.

7.3 Potential causes for signal disruption

As stated above, the WaveLinx system should be able to co-exist in buildings with Wi-Fi installations. However, there are many causes of interference and degradation that go beyond the scope of this document. Some basic actions can be addressed during the design phase that may aid in preventing issues include:

Review the network range and the distance between the devices. The further the distance between wireless devices, the lower the signal strength. Both IEEE 802.15.4 wireless and IEEE 802.11 Wi-Fi have a maximum unobstructed "line of site" range of 150 ft (50 m). However, we also need to factor in obstacles which are prevalent in our indoor spaces.

Of special consideration are the quantity and materials of walls and other obstacles that are between transmitting and receiving devices. Wireless signals can have trouble communicating through these solid objects reducing the wireless range.

Transmitter and end device placement planning during the design phase is critical to ensure proper coverage range and proper device functionality. Manufacturers may have specific recommendations for ranges for their devices that are important to pay attention to.

Review the location of the transmitters. Placing two transmitters within the same space, even if they are on different frequencies and channels can lead to disruption if they are too close together. If too close together, they may increase their signal to "shout" over the other transmitters in the space. If both transmitters are shouting, devices cannot hear or respond. Commercially available wireless products often state in their instructions to maintain at least a 5 to 10 feet air gap between other wireless transmitters to prevent this type of interference by proximity.

The quantity of devices on the network can also be a factor of signal degradation. Different network types may support different quantities of nodes. In addition, depending on the design, the quantity of devices may slow or degrade the signal. It is important to review recommendations of device limitations described by the wireless system manufacturers and incorporate this into the design.

8 Configuration and Maintenance

8.1 Standalone Topology

In a standalone topology, the user will be using the WaveLinx internal webpages to configure the Wireless Area Controller and the WaveLinx Mobile App to program the controller's control logic.

8.1.1 Internal web pages

The WaveLinx internal web pages allows the user to configure the Wireless Area Controller. The following features are offered by the web pages:

- Network settings for all three IP interfaces, i.e. Wi-Fi AP, WLAN and LAN:
  - WLAN/LAN DHCP/Static
  - Wi-Fi AP
    - SSID
    - Password
- Time setting
  - Manual or NTP
- User setting
  - Administrator - user name and password
  - User – username and password
- Certificate management
- Backup/Restore
- Firmware update for the WAC and all connected devices
- EULA

8.1.2 Mobile application

The WaveLinx mobile application permits the following configuration settings:

- Create/modify Areas
- Create/modify Zones
- Add/identify discovered devices
- Create/modify occupancy sets
- Configure the occupancy sensors attributes
- Create/modify daylight sets
- Create/modify schedules
- Configure demand response %
- Configure wallstations and program their buttons

8.2 Networked Topology

In a network topology, the Wireless Area Controllers are connected to the Trellix Core. User will continue to configure the WAC using the WAC's internal web pages and program the WAC using the WaveLinx Mobile App. The Trellix Core host the Trellix Lighting and Trellix Admin apps.

8.2.1 Trellix Lighting

The Trellix Core hosts the Trellix Lighting application which acts as the supervisory application for the WaveLinx system. The following features are offered by the Trellix Lighting app:

- Network settings for the Trellix Core
- System settings for the Trellix Core, i.e. discover Wireless Area Controllers and import their system information (device, etc…)
- Time settings (static IP) for the Trellix Core
- User settings for the users access the Trellix Core
- Configure the BACnet/IP interface
- Configure the Public (REST) interface
- View the Alarms and events generated by the WaveLinx system

8.3 Certificates

WaveLinx uses SSL certificates to secure the communication between the Wireless Area Controller and the Mobile App as well as between the Wireless Area Controllers and the Trellix Core. The SSL certificates are installed at the factory.

Customers can create their own SSL certificates to allow the secure communication between the Mobile devices, Wireless Area Controllers and the Trellix Core.

8.4 User management, Roles and Access

8.4.1 Standalone Topology

User authentication is required to allow a user to configure the Wireless Area Controller using the controller's web pages and to program the control logic using the WaveLinx Mobile Application. The Wireless Area Controller currently supports two roles:

- Administrator
- User

Single sign-on or LDAP access is not supported.

8.4.2 Networked Topology

User authentication is required to allow a user to configure the Wireless Area Controller using the controller's web pages, to program the control logic using the WaveLinx Mobile application and to configure the Trellix Core using Trellix Lighting app. The Trellix Core current supports the following roles:

- System Administrator
- IT Administrator
- Facility Manager
- Tenant
- Viewer
- Third Party Integration
- Demand Response

The Trellix Core does not currently support single sign on or LDAP access through the building network. The Wireless Area Controller users and roles are different than the Trellix Core users and roles.

8.5 Backup and Restore

The system allows users to back up their WACs and Trellix Cores and restore the backed up images. It is recommended that users perform a temporary backup of data prior to doing a firmware update to the system, in the event something should be updated incorrectly. Once the firmware update has completed successfully a permanent backup can be done and stored per standard building IT processes.

8.5.1 Standalone Topology

In a standalone topology, the user must backup manually each standalone Wireless Area Controllers (WACs) using the WAC's internal admin web pages.

Each WAC performs its own backup of all programming and network information. The restore function is used in the event of a WAC failure and replacement or if the user has to revert back to a previous programming.

8.5.2 Networked Topology

In a networked topology, users must manually backup each Wireless Area Controller (WAC) using the WAC's Internal admin web pages and the Trellix Core using Trellix Lighting app.

The Trellix Core and each WAC perform their own backup of all programming and network information. Both the Trellix Core and the WAC support the restore function. The restore function is used in the event of a Trellix Core or Wireless Area Controller failure and replacement or if the user has to revert back to a previous programming.

8.6 Firmware and Software updates

Users can update the software/firmware of the WaveLinx devices. For the wireless devices, the firmware is update over the air (OTA). Firmware and software updates are typically released on a semi-annual basis for normal activities. Software patches are handled as needed.

If the user has registered to mycb.eaton.com then the user will get an automatic notification of firmware and software updates. Additional information will be provided through website information.

8.6.1 Standalone Topology

In a standalone topology, the user updates the software/firmware of the WAC and all devices connected to the WAC via the WAC's internal web page. The device files are encrypted for each product (ex: wireless wallstations, wireless switchpacks).

For the Wireless Area Controller and the wireless devices connected to the WAC, the firmware updates are handled via the WAC internal web pages. The firmware update package is uploaded to each Wireless Area Controller. The WAC then manages the distribution and installations of the updates to all wireless devices connected to it such as integrated sensors, wallstations, etc.…

Mobile application updates are handled through standard application updates through Android and iOS stores.

8.6.2 Networked Topology

In a networked topology, the user updates the software of the Trellix Core using the Trellix Lighting application. The firmware update package is uploaded to the Trellix Core and then the user will initiate the update process.

8.7 Remote support

For some configuration and diagnostics purposes our technical services staff may offer remote access services. This may be accomplished in several ways depending on the customer's network configuration and IT requirements.

Most often temporary access is provided by the facility's IT department via a VPN access to the building automation network. In some facilities, 4G modems have been installed allowing the technical support team to access the system's programming.

Please contact technical support to learn more about after-market services.

8.8 Firewalls (packet filtering, stateful inspection, proxy gateways)

These items should be handled as needed by the local building IT department. The implementation of these security features would be the responsibility of the IT network architect and would not interfere with the standard operation of the lighting system as that is occurring on the OT network.

Additionally, the WaveLinx Wireless Area Controller/Gateway includes a firewall isolating the IEEE 802.15.4 based lighting device and sensor network communications from the IEEE 802.3/IEEE 802.11 based LAN/WAN network.

8.9 Communication Failure to the WAC

In the event of a loss of communication between the Wireless Area Controller and associated devices, the light fixtures will remain at their current light level for approximately one (1) hour. After one (1) hour of lack of communications the wireless devices will continue to operate in disconnected mode with individual luminaire occupancy being the primary method of control.

The WaveLinx system is designed to be able to be compliant with UL924 emergency lighting standards as long as the appropriate devices are included in the system design.

8.10 Third party integration

The WaveLinx system interfaces with other systems via the Trellix Core. The Trellix Core hosts the BACnet/IP interfaces and Public (REST) API which can be used by third party systems to read/write to the WaveLinx system.

8.10.1 BACnet/IP

The Trellix Core hosts a BACnet/IP Interface that enables the integration between the WaveLinx systems with any BACnet compatible system such as Building Automation Systems (BAS). BACnet is a data communication protocol for Building Automation and Control Networks developed by the American Society of Heating Refrigeration and Air Conditioning Engineers (ASHRAE).

Through the BACnet/IP, users can change the light levels for individual devices, zones and areas; and similarly, the user can read the value of the individual devices (occupancy sensors, drivers, ballasts and daylight sensors) and individual space outputs (zone light levels, area scenes) from their BAS console.

8.10.2 Public (REST) API

The Trellix Core hosts a Public (REST) API which allows third party application to exchange data with the WaveLinx system. The API does not provide the ability to change software programming of the system. API's are used for status and override of current state.

8.11 Demand Response

Demand Response is currently supported through an IP connection into each WAC from the building management system or other third-party system. See the WaveLinx Demand Response application note for more information on the connection.

9 Security

Both WaveLinx and Trellix view security as a cornerstone of a safe, dependable and reliable electrical system. Accordingly, the WaveLinx system employs current industry best practices to reduce, identify, contain and manage security risks. WaveLinx has been designed and engineered with wireless security as a key requirement with flexibility to accommodate improvements if new security attack surfaces are identified. The Product Cybersecurity Center of Excellence (PCCoE) provided guidance throughout the development of WaveLinx and offers customers an Internet accessible portal to identify emerging threats, find ways to secure products against them and help customers deploy and maintain product solutions in a secure environment. More information on the PCCoE can be found at www.eaton.com/cybersecurity

The WaveLinx System uses a multi-tiered approach to addressing industry best practices for security risk management and utilizes guidelines promulgated by the Department of Homeland Security (DHS), National Institute of Standards and Technology (NIST) and industry standards organizations to achieve a secure and adaptable lighting control platform.

9.1 Physical security

An architecture that isolates the wired Ethernet network from the wireless network, which strictly limits the possibility of the WaveLinx wireless being used as an access point to the corporate network and gain confidential information.

Physical access also involves the customer location. This includes not allowing unauthorized personnel in areas where they do not belong, or access to devices they should not be connecting to.

9.2 Customer security

Customer security process is a partnership with the customer and involves multiple levels of password and network access protection.

Beyond physical access the customer provides an additional layer of security with strong authentication to access their corporate wired or wireless network and limiting the devices that can access those networks.

WaveLinx provides additional protection with unique username and password requirements for each Wireless Area Controller that are securely stored per NIST-recommended best practices.

9.3 Device communication security

For secure device-to-device communications, encryption is an important factor to reduce the potential of someone reading data sent on the network. For that reason, all WaveLinx communications use AES 128-bit encryption, recommended by NIST as part of FIPS publication 197.

9.4 Network communication security

WaveLinx uses secure HTTPS (TLS1.2) protocols for securing connections to the Wireless Area Controller over the wired network.

WaveLinx uses secure WPA2 Enterprise technology for secure connections to the Wireless Area Controller over the Wi-Fi network when acting as an access point. If the Wireless Area Controller is connected to a wired network for communications this connection method is disabled.

WaveLinx mobile applications uses HTTPS (TLS1.2) as part of its communications to the Wireless Area Controller regardless of connection method, which means only our mobile application can send data to the WaveLinx system.

9.5 Network segmentation security

Each Wireless Area Controller employs its own unique keys, which limits any potential breach to only a small area of the system.

The WaveLinx Wireless Area Controller (WAC) provides segmentation between the lighting Operational Technology (OT) network and the enterprise Information Technology (IT) network.

The IT/OT network segmentation provides a barrier to possible IT network attack surface exposure. Even if an attack within the lighting (OT) network and its devices is successful, the WAC isolates the enterprise IT network from potential attack.

9.6 OTA update security

WaveLinx provides a method to allow for digitally signed/encrypted firmware update files to be sent to the devices over the air (OTA). It is imperative as part of network security to ensure OTA updates are digitally signed firmware images from their manufacturer, so the devices recognize they are valid updates from that manufacturer and not sent with a malicious intent.

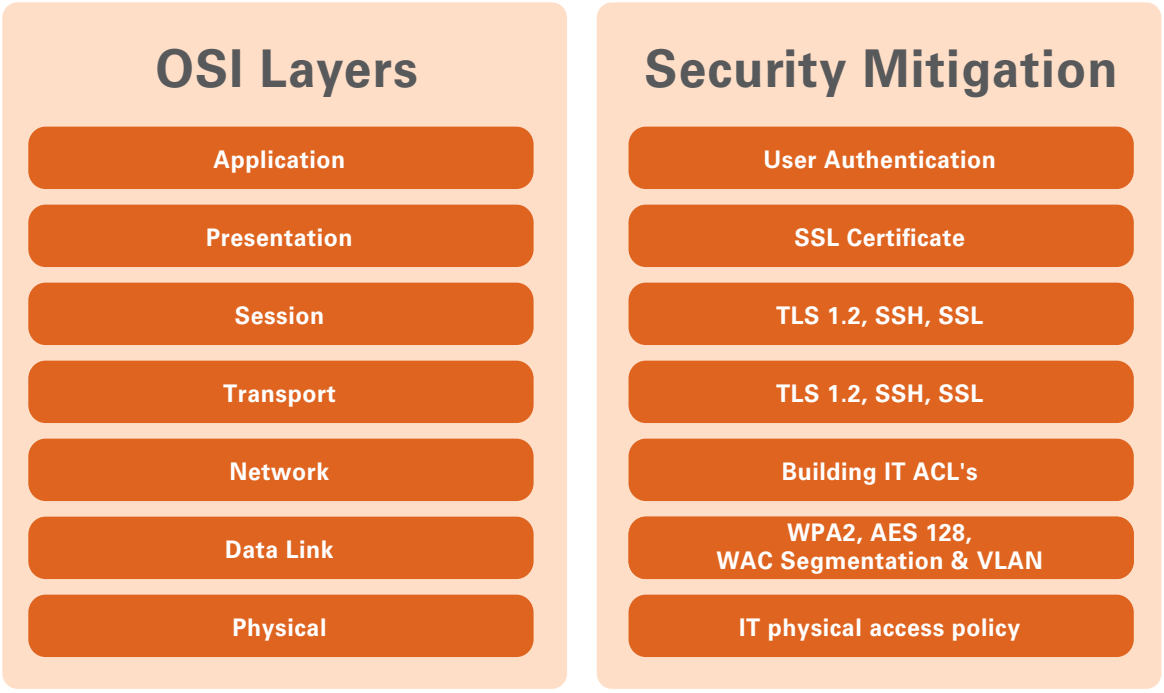
9.7 Cybersecurity Center Of Excellence

Cybersecurity Center of Excellence (COE) involvement and guidance was key as part of the WaveLinx development to ensure our product incorporates industry and governmental network security best practices.

The COE also provides a publicly accessible site for information and feedback concerning cybersecurity threats and responses, as well as a method for you to monitor network breach risks.

9.8 OSI model security

WaveLinx supports a seven-layer multi-tiered approach to security, below we illustrate how WaveLinx supports security through the entire seven layer OSI model, not just the WaveLinx application.



9.9 Cybersecurity reporting and mitigation plans

Cybersecurity Center of Excellence (COE) involvement and guidance is key as part of all current and future development to ensure our product incorporate industry and governmental network security best practices.

COE considers latest available best industry practices (DHS, NIST, FIPS) to reduce, identify, contain and manage risks: Deter, Protect, Detect, React, Recover

The COE also provides a publicly accessible site for information and feedback concerning cybersecurity threats and responses, as well as a method for you to monitor network breach risks.

See www.eaton.com/cybersecurity for more detail.

9.10 Cybersecurity or functionality issues and reporting

Issues found in the field can be reported to technical support, who will attempt to replicate the issue. If the issue can be replicated it is reported through internal issue tracking software which assigns the issue to the engineering team for resolution.

Depending on the severity and priority of the reported issue, this could include standard firmware or software updates published to the website or a proactive service visit by field services.

9.11 WaveLinx Views on Cyber Security

WaveLinx views security as a cornerstone of a safe, dependable and reliable electrical system. Accordingly, WaveLinx employs current industry best practices to reduce, identify, contain and manage security risks. These systems have been designed and engineered with wireless security as a key requirement with flexibility to accommodate improvements if new security attack surfaces are identified. The Product Cybersecurity Center of Excellence (PCCoE) provided guidance throughout the development of each system and offers customers an Internet accessible portal to identify emerging threats, find ways to secure products against them and help customers deploy and maintain product solutions in a secure environment. More information on the PCCoE can be found at www.eaton.com/cybersecurity

Eaton
1121 Highway 74 South
Peachtree City, GA 30269
P: 770-486-4800
www.eaton.com/lighting
For service or technical assistance:
1-800-553-3879

Canada Sales
5925 McLaughlin Road
Mississauga, Ontario L5R 1B8
P: 905-501-3000
F: 905-501-3172

Printed in USA
Publication No. AP503036EN
October 2019

Powering Business Worldwide