Technical Article

GreenMAX DRC Network Security

Product: GreenMAX DRC Room Control System **Article ID:** 011119-DB/TB-01

Date: January 11, 2019

Summary:
This document describes the network security for the GreenMAX DRC Room Control System, commissioned and controlled with the GreenMAX DRC App for smart devices.

Overview

Leviton takes the security of your lighting control and network systems seriously. Providing a cohesive, complete, and integrated end-to-end control solution allowing intended, safe communication while rejecting malicious communication has been built into each physical and software layer of the GreenMAX DRC Room Control System. The goal of this White Paper is to review each of these layers, the types of communication that occurs, and the steps we've taken to secure our system.

Physical Layers and General Network Architecture

Leviton's commercial lighting control network systems are broken into several different physical layers, each of which have different security concerns and approaches to network functionality and security. The components we will be reviewing are as follows:

- Configuration Tool (GreenMAX DRC App) communication to Room Controllers
- Configuration Tool (GreenMAX DRC App) communication to Leviton Cloud Services
- Room Controller Communication on IP Networks
- BACnet Communication on IP Networks
- LumaCAN/CAN Device Level Communication

Summary of Network Communication and Security

Physical Layer	Function	Communication Method	Security Method	Notes
GreenMAX DRC App to Room Controller	- Configuration and commissioning of system - Control of devices	- WiFi, Ethernet IP connectivity between smart device and DRC Room Controller - Interface may be through the building WiFi system OR direct with the room controller acting as an access point	- TLS Security using AES-128 encryption - Communication privileges secured by communication user token - User authentication through Leviton Cloud - Key storage on Leviton Cloud	- IP address can be statically assigned or provided through a DHCP server - DNS name resolution is required on networks using DHCP for address assignment

Physical Layer	Function	Communication Method	Security Method	Notes
GreenMAX DRC App to Leviton Cloud	- User privileges for each part of each building (User Access Control) - Storage of user and project/security information - Synchronization of project/security information between users	- Connect to Leviton Cloud Services through public internet using the configuration tool's cellular or WiFi connection	- TLS Security using AES-128 encryption - User authentication through Leviton Cloud	- Leviton Cloud Services are hosted on Amazon Web Services - Connectivity to Leviton Cloud Services is only required to (1) create a user account, (2) create a project, (3) asynchronously store/sync project information - Connectivity to Leviton Cloud Services is not required to (1) commission a project, (2) allow lighting controls to operate
Room Controller to Room Controller	- System message broadcast (load shed, group ON/OFF, etc.) - Using sensor/actuator data in from Room A in Room B	- WiFi, IP connectivity between room controllers	- TLS Security using AES-128 encryption - Communication privileges secured by communication system token, distributed at time of configuration	- Requires implemented WiFi backbone in space, provided by a 3rd party or Leviton - Each room controller is a WiFi client to the system access point
LumaCAN/CAN Communication	- Lighting control within the sub-net	- LumaCAN protocol over Category 6 cabling	- Proprietary CAN-based protocol secured at the physical layer - All interface points are secured using one of the other methods discussed herein	- Primary means of sensor, relay, and keypad communication within the room - Interface points are BACnet interface, or IP through and secured by a controller
BACnet Communication	- Interface to Building Management System (BMS), either at the micro or macro level	- Wired Ethernet, BACnet/IP, using NP00G Gateway	- See ASHRAE BACnet protocol documentation for details - Primarily secured and encrypted at the physical interface level	- BACnet standard PICS statement available at www.leviton.com which details interface specifics

NOTE: The industry has been drawing on standards and best practices such as ANSI/UL 2900-1, IEC standards, ISO 27000, and the NIST IoT Cybersecurity Framework. We are closely following these developing standards, and will implement as appropriate.

For more information visit www.leviton.com.

End of Document.