1. Is LumaWatt Pro secure?

Yes, The LumaWatt Pro 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.

2. Does LumaWatt Pro provide a path to my building intranet (LAN)?

The LumaWatt Pro Energy Manger is the only device that connects physically to the building intranet. In addition to other security measures the Energy Manger isolates the wired Ethernet network from the wireless network which limits the possibility of someone using the LumaWatt Pro system to gain business confidential information.

3. Why AES 128-bit encryption, why not AES 256-bit?

LumaWatt Pro uses AES 128-bit encryption for device-to-device communications as recommended by the National Institute of Standard and Technology (NIST).AES encryption comes in three standard key sizes (128, 192 and 256bits). Many people think because there are three sizes AES 256-bit must be better. In fact there were three keys sizes because it was developed for US Military/Government communications which requires three security levels.

AES 128-bit encryption uses a 128-bit key to encrypt the data. That is 3.4 x 1038 possible combinations if someone wanted to brute force guess your encryption key. Assuming you were able to guess the correct key 50% of the way through the combinations it would still take over 1 billion years.

4. Can someone send a command or take over one of the LumaWatt Pro devices?

No, All LumaWatt Pro devices use AES 128-bit encryption and also require that the commands be sent only to and from the LumaWatt Pro Energy Manger.

5. Is the LumaWatt Pro Energy Manger application secure?

Yes, LumaWatt Pro Energy Manger application uses secure protocols to authenticate communications between the Energy Manger and the commissioning device. This inhibits other applications or software from sending commands to the LumaWatt Pro system.

6. If someone were to hack into my Energy Manger can they see the rest of my system or my building intranet (LAN)?

No, each Energy Manger employs its own unique key, which limits potential breaches to only a small area. Also the Energy Manger provides segmentation between the lighting Operational Technology (OT) network and the enterprise Information Technology (IT) network. Even if an attack within the lighting (OT) network and its devices is successful, the Energy Manger isolates the enterprise IT network from potential attack.

7. Are firmware updates secure?

Yes, LumaWatt Pro firmware updates are digitally signed which means that only our over the air (OTA) firmware updates will be accepted by each device.

Eaton
1121 Highway 74 South
Peachtree City, GA 30269
P: 770-486-4800
www.eaton.com/lightingsystems
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. SA503015EN
May 19, 2017

Powering Business Worldwide