2020 Security Addendum for Models LC7001 and AU7000

Abstract:

This document covers changes to LC7001 and AU7000 devices for compliance with California SB-327. This legislation requires Internet-connected devices to provide at least one of the following security mechanisms:

1. A unique, factory-assigned password (ADM)
2. A user defined password which must be set before normal operation (LCM)

Sections:

[1] Glossary of Terms

- ASCII Hex - The data encoding method used to exchange binary data between the client and host over a socket. Each data byte is encoded as two printable ASCII characters from this list: **`0123456789ABCDEFabcdef`**. A byte with all bits cleared is encoded as **`00`** while a byte with all bits set is encoded as **`FF`**. While the host will only transmit uppercase characters, it may receive lowercase characters as well.

- Client - A networked device initiating a connection to the host. This is most often a mobile device running an app, but can also be a third party device on the same local area network.
- Encryption - The process of transforming a 16-byte block of data (a challenge phrase or key) using 128-bit AES in ECB mode. Because all inputs and outputs to the AES function are 16 bytes in length, no padding is used.
- Factory Key - A 128-bit private key derived from the factory password.
- Factory Password - A unique, eight character password printed on a label, affixed to the AU7000 during manufacture.
- Host - This refers to either the LC7001 (LCM) or AU7000 (ADM).
- User Key - A 128-bit private key derived from the user password.
- User Password - A password entered by the user via a mobile application or third party device for the purpose of securing the host against unauthorized access.

[2] Compliant and Non-Compliant Hosts

	LC7001 / LCM	**AU7000 / ADM**
Compliant	An LCM without an endpoint added prior to January 1, 2020.	An ADM loaded with secure firmware and labeled with a unique password from the factory.
Non-Compliant	An LCM with at least one endpoint added prior to January 1, 2020.	An ADM not labeled with a unique password from the factory.

It is important to note that there are no physical differences between a compliant and non-compliant LCM, while a compliant ADM features a factory-affixed label and a corresponding firmware configuration to require authentication. This is due to differing strategies in dealing with existing inventory across the two product lines.

Firmware deployed in December 2019 marks an LCM as non-compliant by writing a signature value to flash memory if both of these conditions are true:

1. The current year is still 2019.
2. The LCM is configured with one or more endpoints.

[3] Message Description Notation

Literal message content is described in this font: **`EXAMPLE_MESSAGE_CONTENT`**

An arbitrary ASCII hex character is indicated by this symbol: □

An arbitrary decimal character is indicated by this symbol: ■

[4] Security Feature Overview

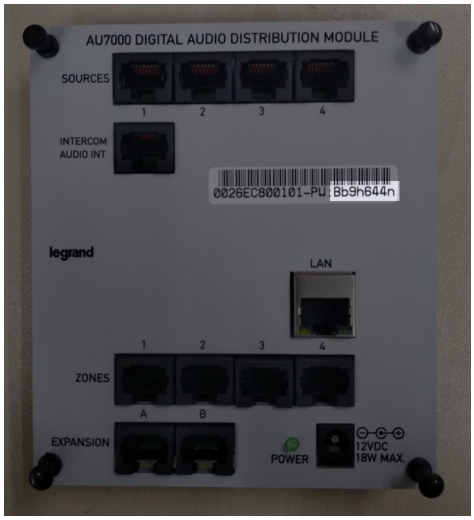
Security additions to the LCM and ADM prevent unauthorized access to the host by requiring a client encrypt a 128-bit block of random data using a shared secret key.

This table summarizes the main differences in security features between the LCM and ADM.

	LC7001 / LCM	**AU7000 / ADM**
User-defined key	Compliant: Required Non-compliant: Optional	Not available
Factory password label	Not equipped	Compliant: Equipped Non-compliant: Not equipped
Default key	Compliant: MD5("") Non-compliant: None	Compliant: MD5(label) Non-compliant: None
Key reset method	Switch	None

⚠Security measures described in this document are intended to provide basic authentication and access control. Because only the initial authentication and set-key operations employ encryption, the remainder of the session between a host and client, is visible to anyone with access to local area network traffic.

This image shows the location of the password on a compliant ADM:



[5] Challenge Protocol

5.1. Opening Messages:

Upon first opening a connection to either the LCM or ADM, the host may respond in one of several ways:

5.1.1 JSON-Formatted Messages

An unsecured host (non-compliant or running pre-2020 firmware) begins exchanging JSON-formatted messages with the client. All commands are available to the client and no challenge takes place.

⚠There may be a delay of several seconds before the first JSON message is sent by the host under pre-2020 firmware. The client should be prepared for this possibility.

5.1.2. **[SETKEY]** Prompt (LCM only)

This message is sent by compliant LCMs, indicating a switch to a restricted JSON command set. No challenge takes place in this mode. Normal LCM function is disabled and the client must set the "Keys" property using the SetSystemProperties call. Upon success, the full JSON command set is enabled and the LCM exits **[SETKEY]** mode.

⚠ If the client attempts to execute a command other than SetSystemProperties, **ErrorCode** 2066 is returned, indicating an unrecognized command. If the client attempts to set a property other than "Keys" using SetSystemProperties, **ErrorCode** 2089 is returned, indicating an unrecognized property. These codes are not exclusive to **[SETKEY]** mode.

5.1.3. "Hello" Challenge

Hello V1 □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ □□□□□□□□□□□□

Challenge phrase MAC Address

This message presents a challenge to the client, indicating the host is secured with a key. The first 32 character block of ASCII hex is a 16 byte challenge phrase which the client must encrypt and return to the host in the same ASCII hex format. The second block of ASCII hex is the host's six byte MAC address which is optionally used by the client to identify the host.

[5.2] Challenge Response

The client must respond to the host's challenge with exactly 32 characters of ASCII hex. Extra characters, such as line terminators may cause this transaction to fail, even if the first 32 characters sent to the host are correct.

After the final character is sent by the client, the host waits between one and two seconds and responds to the client with one of the following messages:

[OK] - The challenge response is accepted by the host and communications continue in JSON format.

[INVALID] - The challenge response is rejected by the host and the socket is closed within a few seconds.

[6] Relationship Between Passwords and Keys

[6.1] Key

A key is a 16-byte shared secret value, represented in exchanges as 32 characters of ASCII hex. Keys are never transmitted without encryption.

[6.2] Password

A password is a human-readable string of numbers, letters and other characters. The length of the password and the characters it may comprise are determined by the application. Passwords are never received nor stored by hosts. The factory password as printed on the ADM, consists of eight characters of this subset of 7-bit ASCII:

B F G H L N R T V X 3 4 6 7 8 9 b d f g h j m n p q r t v w x y

Applications interfacing with the ADM must support these characters. Applications interfacing with the LCM should at a minimum support all printable characters in the 7-bit ASCII character set (32-126), though an exhaustive character set has not been defined at the time of this writing.

[6.3] Conversion

A key is derived from a password by taking its MD5 sum. A password string is converted to a byte array based on the ASCII mapping of each character. Only printable characters are used in the MD5 sum. Null string terminators must not be included.

There is no reliable or efficient method to convert a key back into a password in most cases. Because both keys and passwords are private assets and are never transmitted unencrypted, security is not compromised by MD5's potential reversibility.

[6.4] The Empty Key and Password

This special key results from the MD5 sum of an empty data set (0 bytes). It is used by the LCM's SetSystemProperties/Keys operation to decrypt the initial user key. It is unique in that it functions as the LCM's currently active key in set-key operations, but is not used to challenge a client.

⚠ Because the initial empty key can be trivially determined, the first user key assignment is vulnerable to capture. If the set-key operation is intercepted and the old key is known by an attacker, the new key is compromised.

[7] Setting the Host Key Directly

This section pertains only to the LC7001 (LCM) as it is the only host type capable of using a user-defined key. The purpose of this command is to securely assign a new, user-defined key to the LCM while confirming the validity of the client's old key. This command is not accepted in response to a challenge. In **[SETKEY]** mode, it is the only command accepted by the host.

[7.1] Command format

```
{"ID":■■,"PropertyList":
{"Keys":"□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□"},"Service":"SetSystemProperties"}
```

The "Keys" property is always 64 characters long, containing two keys encoded in ASCII hex format.

The first half of the keys property is the old key encrypted by itself with AES128 ECB.

The second half is the new key encrypted by the old key with AES128 ECB.

[7.2] Evaluation and Reponse

The host compares the content of its own key, encrypted by itself, to the first half of the "Keys" property sent by the client.

If the old key matches, the host decrypts the second half of the "Keys" property (the new key) using its current key and immediately adopts the result as its current key. All other clients connected to the host are disconnected without warning. The client which sent the "Keys" property receives this confirmation, indicating the operation succeeded:

{"ID":■■,"Service":"SetSystemProperties","Status":"Success","ErrorCode":0}

If the old key does not match, the operation fails and the following response is returned:

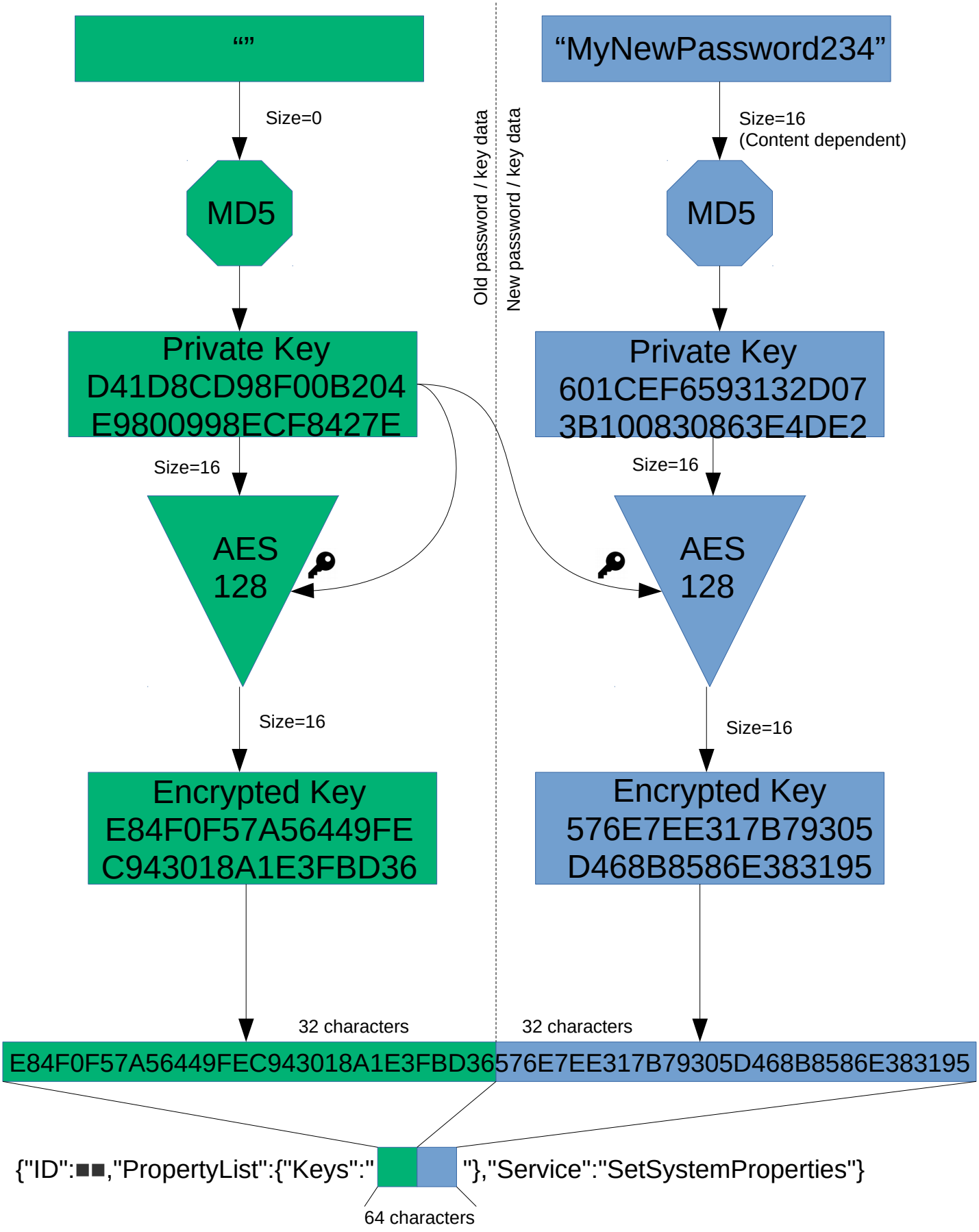
{"ID":■■,"Service":"SetSystemProperties","Status":"Error","ErrorText":"Old key mismatch","ErrorCode":-1}

If the "Keys" property is not exactly 64 characters in length, the operation fails and this response indicates the command is malformed:

{"ID":■■,"Service":"SetSystemProperties","Status":"Error","ErrorText":"Bad length","ErrorCode":-2}

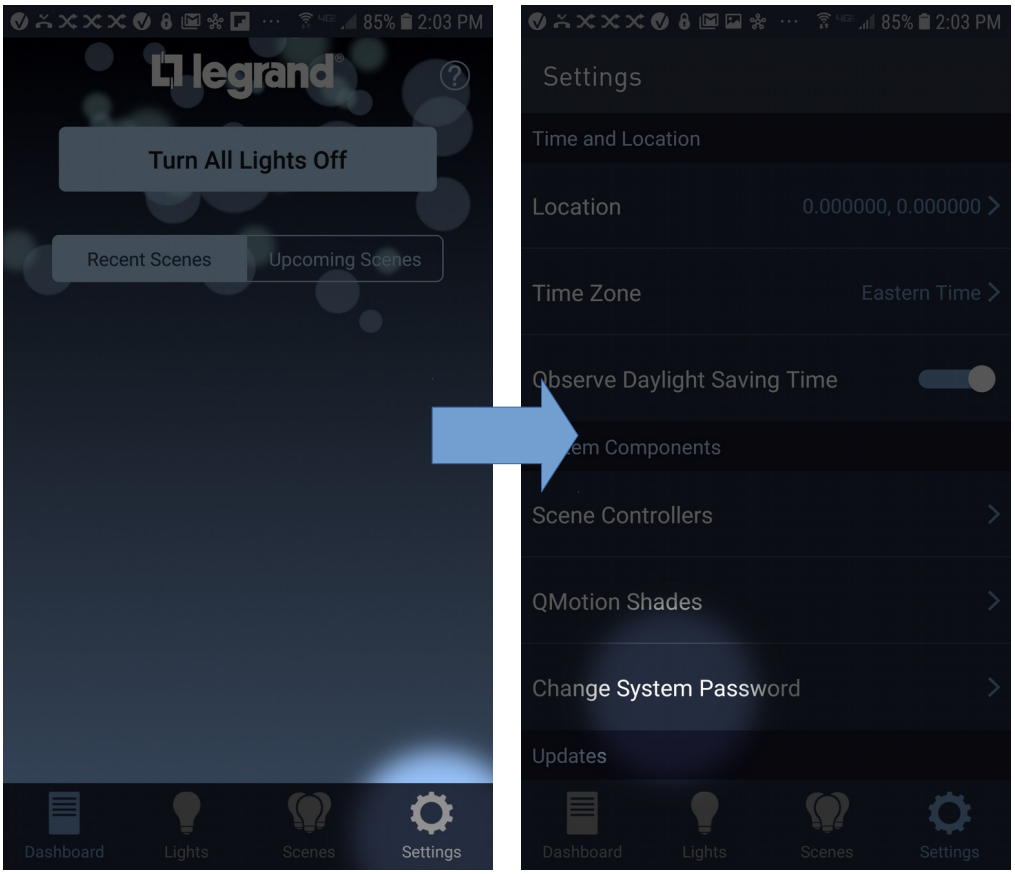
[7.3] Setting a User Key on the LC7001: A Practical Example

Assembling the SetSystemProperties message



[8] Setting a User Key on the LC7001 Using the Mobile Application

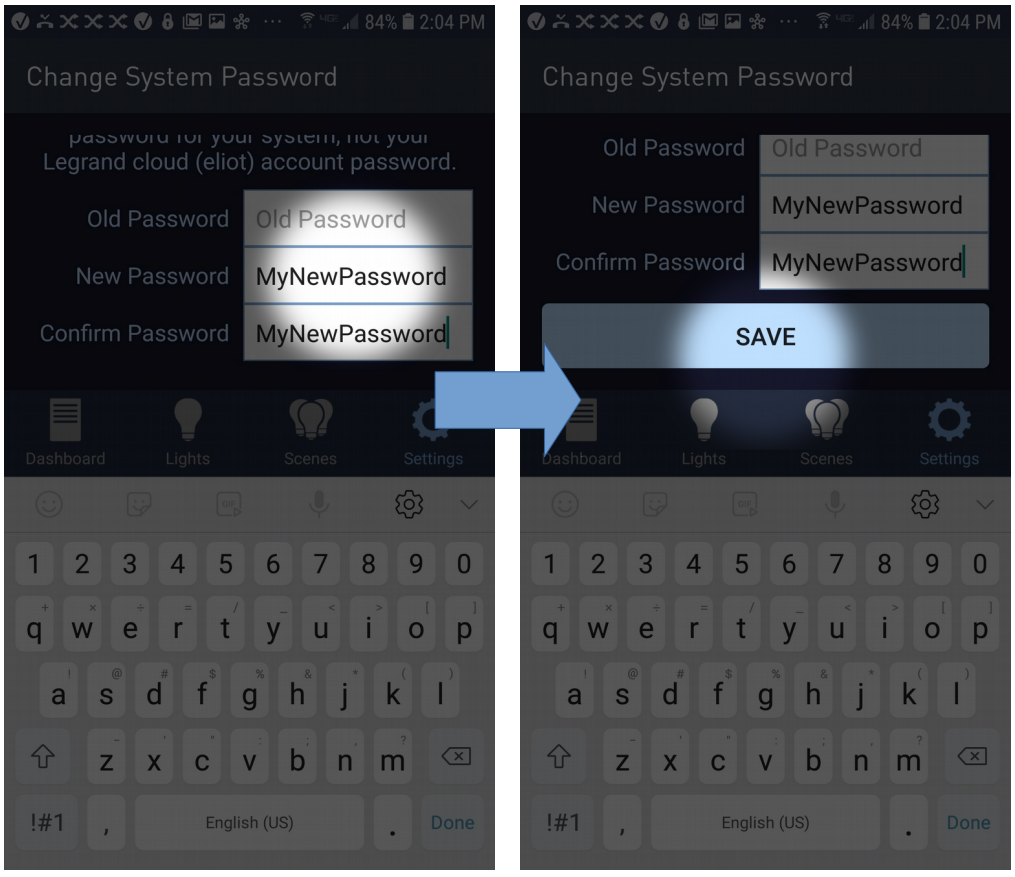
If the LCM is non-compliant, setting a password is optional. This is done using "Change System Password" option under "Settings".



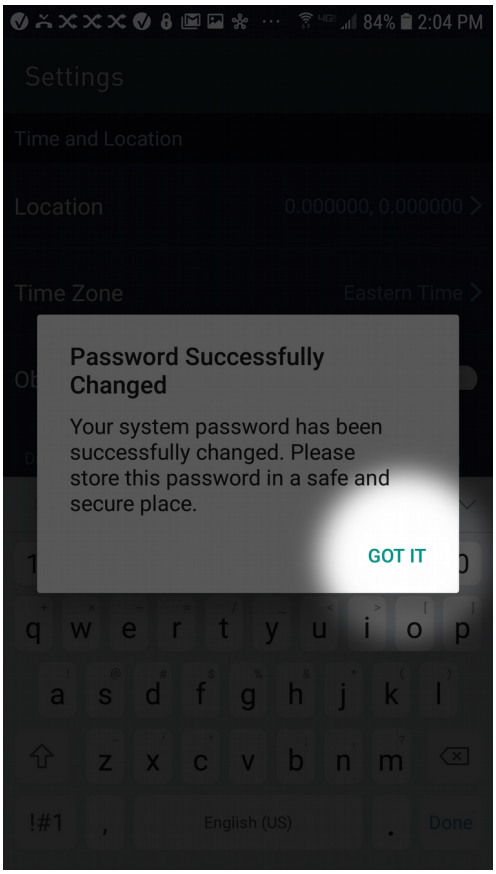
If the LCM is compliant and requires a key to be set, the application initiates this process automatically once connected.

The user must then enter the same password of at least eight characters in both the "New Password" and "Confirm Password" fields. If the no password has been set previously, the "Old Password" field must remain blank.

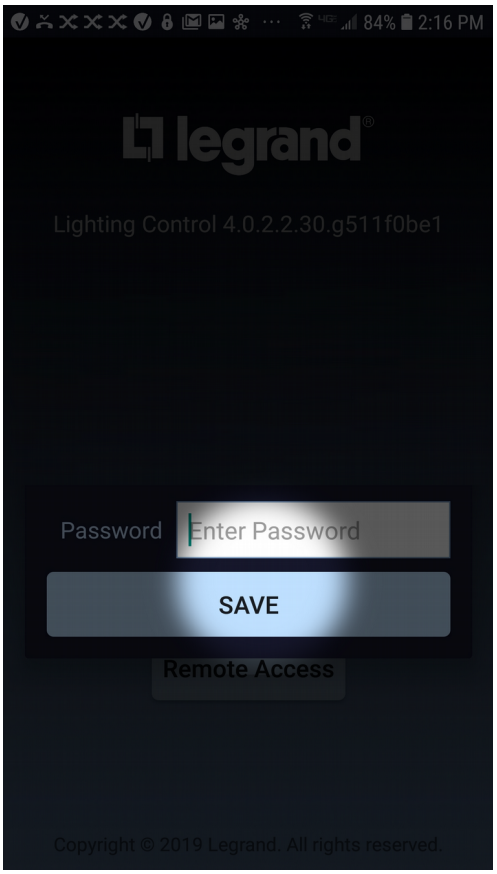
When the password has been set, the user must select the "SAVE" button below the "Confirm Password" field.



If the change password operation was successful, this confirmation dialog is displayed and can be dismissed by selecting the "GOT IT" button.



The user is then prompted to enter the same password before gaining access to the LCM.



[9] Additional Resources

Cryptomathic AES Calculator (ASCII hex input and output, ECB 128-bit):
http://extranet.cryptomathic.com/aescalc/index

MD5 Calculator (String input without terminating characters, ASCII hex output):
http://md5-hash-online.waraxe.us/

Password to key conversion under Linux:
echo -n "password" | md5sum -t