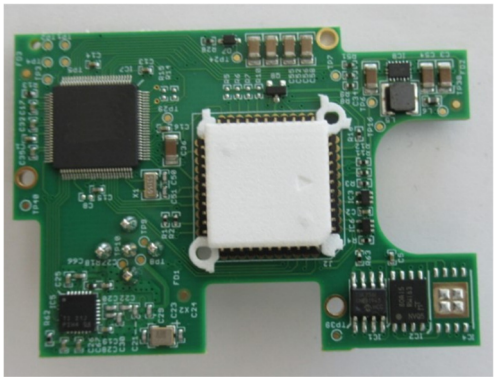
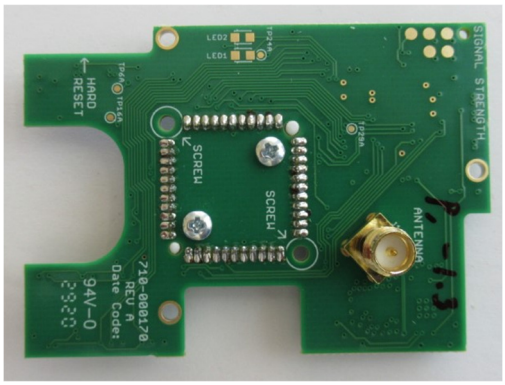
SA-OWL Installation and User Guide

(Onity Panic Wall Reader Retrofit Kit)





Document History

Version	Date	Author	Changes, Remarks
1.0	08/18/2020	AS	Initial document
1.1	08/20/2020	AS	Added installation section
1.2	08/27/2020	AS	Corrected photos

1. Purpose

1.1. This document provides instructions on how to install and use the SecureALL SA-OWL upgraded Onity Panic Wall Reader product.

1.2. This document provides information about:

1.2.1. Product Installation

1.2.2. Product Operation – Magnetic Card Access

1.2.3. Product Operation – Keypad Access

1.2.4. Directions on how to interpret LED Blink sequence on lock

Note: This is a living document that will change over the product lifecycle.

2. Product Overview

2.1. SA-OWL is a retrofit kit for Onity's CT30 Wall Reader controller (CT30WRC); Onity Model# C3XDU10. It upgrades it to provide more functionalities including making it a wireless lock with real-time communication with the SA-Guardian application server.

2.2. The retrofit involves following:

2.2.1. Using all parts of CT30WRC except its original controller IC.

2.2.2. Replace Onity's CT30WRC micro-controller IC with SecureALL's wireless controller board with built in IC adapter

2.2.3. Add an outside mounted antenna

2.3. SA-OWL draws 5V DC power from OEM CT-30 Wall reader controller

2.4. When a credential card (that is allowed access to the door at prescribed day of week and time) is presented to the CT30 Wall Reader, the unlock command signal is outputted by the CT30WRC.

2.5. The product dynamically discovers nearby SA-AP-200 router that in turn provides SA-OWL with data communication connectivity with SecureALL's SA-Guardian Application Server.

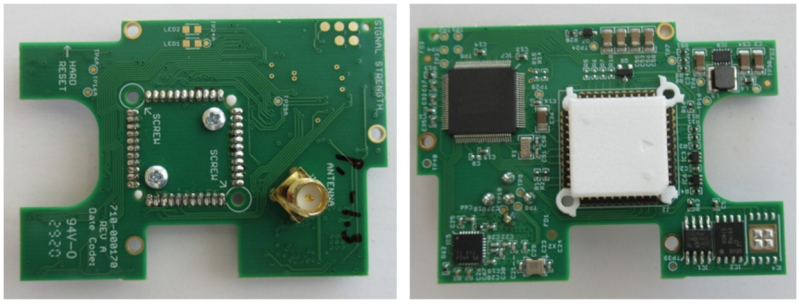


Figure 1: SA-OWL top and bottom view

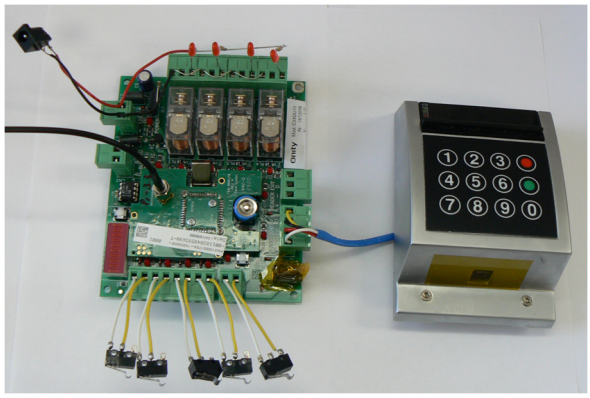
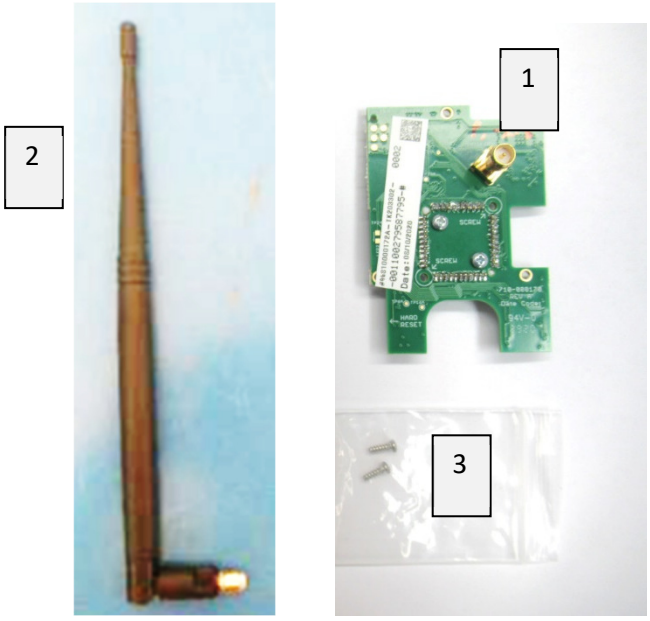


Figure 2: CT30WRC that is upgraded by SA-OWL kit and connected to CT30 Wall Reader. Representative digital Input/output.

Kit Components

Each retrofit kit contains the following component:

1. SA-OWL PCB Assembly
2. Antenna with cable
3. Mounting screws



Required Tools

1. Small Philips screwdriver
2. Large flat screwdriver or drill with 3/8” (10mm) drill bit to open knock-out or drill hole into door power supply enclosure.
3. PLCC Extraction tool: Manufacturer: “Jonard Tools”, Part Number: “EX-6”

   Available from SecureALL or Digi-Key:
   https://www.digikey.com/product-detail/en/jonard-tools/EX-6/K374-ND/135076

Installation

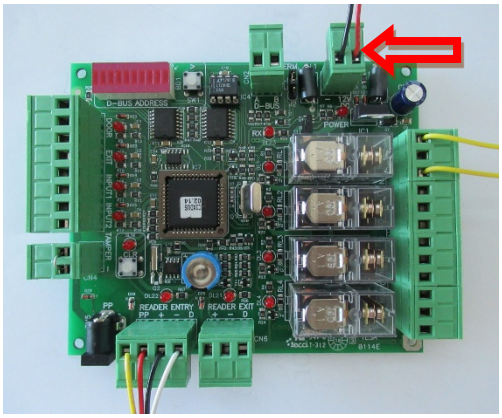
If you are installing the product from scratch, then follow the installation instructions that are included with the C3XDUS Stand Alone Door Unit.

In the process you will:

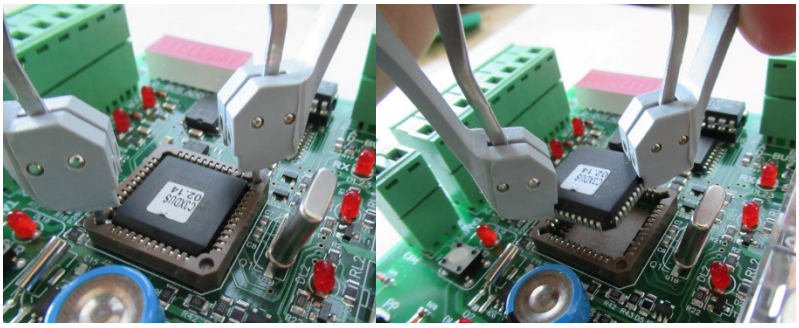
1. Install the Wall Reader unit and the wires leading to the power supply box.
2. Install the Stand Alone Door Unit (DUS) inside the power supply box and make the appropriate connections to the Reader, door controller, other inputs and outputs, and the 12V power source.
3. Please refer to **Error! Reference source not found.** for a list of the default input/output assignments of the SecureALL retrofit controller.

Main Board Installation

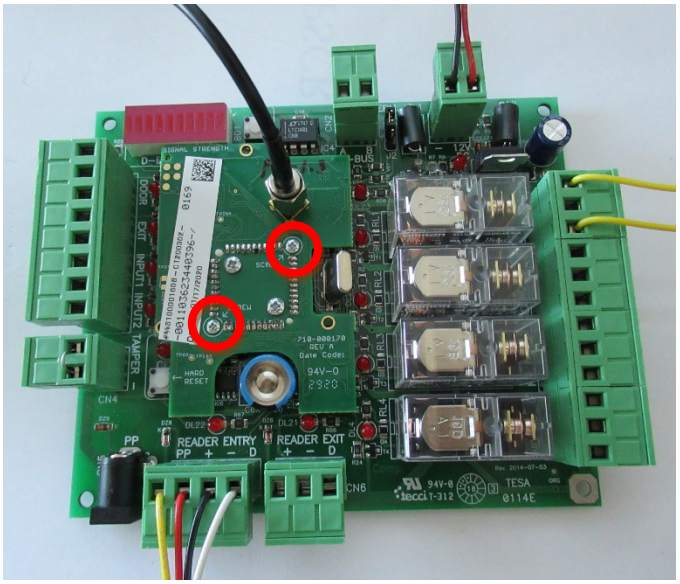
1. Disconnect power to the Stand Alone Door Unit (DUS) by pulling out the power connector CN1.



2. Use the PLCC extraction tool to remove the controller IC from the DUS:
    a. Insert the hooks into the two slots in the corners and push all the way down.
    b. Squeeze the handles of the tool together to lift the IC.
    c. If you want to keep the IC, you can store it in the bag that contained the SA-OWL PCB Assembly.



3. Insert the SA-OWL PCB Assembly into the socket and use the two provided mounting screws to secure it.



Input and Output Functions

The assignment of functions to inputs and outputs is configurable in SA Guardian. The default configuration corresponds to the configuration of Onity, with the addition of a lockdown button and the ability to control an automatic door opener:

Inputs:

Label on DUS	Name in SA Guardian	Default Function
DOOR	DC_IN3_FUNC	Door-closed sensor.
EXIT	DC_IN4_FUNC	Remote unlock or request-to-exit button.
INPUT1	DC_IN1_FUNC	Unused.
INPUT2	DC_IN2_FUNC	Unused.
TAMPER	DC_IN5_FUNC	Tamper switch (normally closed). If no tamper switch is used then add a jumper wire between the two terminals.

Outputs:

Label on DUS	Name in SA Guardian	Default Function
LOCK	DC_OUT3_FUNC	Unlock: Wire to door locking mechanism as described in the DUS installation manual, using the Metal Oxide Varistor.
SHUNT	DC_OUT4_FUNC	Unused.
OUT1	DC_OUT1_FUNC	Automatic Door Opener (ADO): Switch is closed when a card is read that is configured to operate the ADO. *Note: An SA-Guardian enhancement is required to activate this function.*
OUT2	DC_OUT2_FUNC	Alarm: Switch is closed in the event of an alarm, such as door-ajar-alarm or a tamper event.

Antenna Installation

The antenna comes with a magnetic base that attaches easily to metal without requiring any mounting hardware.

The antenna needs to be mounted outside of the power supply box, such that the antenna element is in a vertical orientation. It could be attached to the top or bottom of the power supply box. The position should be chosen to minimize the amount of metal between the antenna and the nearest router.

To route the antenna cable into the power supply box, a hole of at least 3/8" (10mm) diameter is required. If no hole can be found then open a knock-out or drill a hole.

Finally, thread the cable through the hole and attach it to the SMA connector on the SA-OWL PCB Assembly. Be careful to not apply too much force on the PCB when tightening the connector.

Caution:

Per FCC rules, the customer must only use the antenna provided by SecureALL as part of the product package.

Power Up

Attach the power connector (CN1) that was disconnected in the beginning.

Under normal circumstances the following LED states can be observed after connecting the power:

1. The LED near the power input turns on.
2. Initially, the reset LED (near the TAMPER input) is on briefly, but it can stay on for several seconds when the reader is started for the first time or after a hard reset.
3. Once the reset LED turns off, the LED near the READER ENTRY connector should turn on. This indicates that communication with the Wall Reader unit is working.
4. After another 10-20 seconds: One of the 10 LEDs in the signal-strength bar graph (top-left) goes on to indicate that there is connectivity with a router. It can take longer if wireless connectivity is poor.
    a. If the reader is started for the first time or after a hard reset, the LED flashes to indicate that the cryptographic handshake with the server has not happened yet. Once the handshake is complete (typically after another 20-30 seconds) and the device reconnects to the router, the LED should be solid.

Antenna Optimization:

The signal strength indicator shows whether there is a connection with a router and the signal strength. When all LEDs are off, the reader is not connected to a router. Otherwise, one LED is on, with the leftmost LED indicating poor connectivity, and the rightmost LED indicating good connectivity. The indication is updated approximately every 10 seconds.

If the signal strength is poor (one of the three leftmost LEDs), then try to position the antenna in different locations and orientations. After repositioning the antenna, keep away from it by at least 3 feet and wait 10 seconds to see if the signal strength has improved.

Hard Reset:

Under some circumstance, SecureALL's technical support team may ask you to perform a hard reset. To do this, press and hold the button labeled "Hard Reset" for at least 2 seconds. The reader will go through the power-up sequence described above, with the reset LED on for a few seconds, and the signal-strength indicator LED initially flashing.

3. Caution & care

3.1. This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

3.2. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (E.I.R.P) is not more than that permitted for successful communication.

3.3. This device has been designed to operate with the antennas listed below and having a maximum gain of 5dBi. Use of any antennas having a gain greater than 5 dBi is strictly prohibited for use with this device. The required antenna impedance is 50 ohms. Different Antenna mounting plate may be used to position the antenna in desired orientation for best polarization.

4. Modes of operation

4.1. Four operating modes are available to the SA-OWL upgraded lock:

4.1.1. **Standard Mode** – When the lock is in standard mode, a valid credential (card key) is required to gain access to the lock.

4.1.2. **Office (Free) Mode** – The locks may be configured to allow Office (or Free) access. When in this mode, no key is needed to gain access as the lock remains in the unlocked position. The locks may be placed in and out of office mode in two ways:

a. Present certain authorized cards twice
b. Automatically as per programmed schedule

Note: Only credential cards that are valid for the lock may be used to put the lock in and out of office mode.

4.2. **Lockdown (Blocked) Mode** – SA-Guardian server can command the lock to change operating mode to Lockdown (Blocked) mode, alternatively if the lock is equipped with an inside CT-30 reader with keypad, a user may rapidly press the red button 3 time to put the lock in Lockdown mode. When in Lockdown mode the Red LED (on the inside CT-30 reader with keypad) will start flashing. When a lock is in lockdown, no guest keys, and only certain privileged users, will be allow access to the lock.

To exit the Lockdown mode, SA-Guardian server can command the lock to change operating mode to exit Lockdown (Blocked) mode, alternatively if the lock is equipped with an inside CT-30 reader with keypad, a user may rapidly press the red button 3 time to put the lock out of Lockdown mode. The Green LED will flash once to indicate that the blocking has been removed.

5. SA-OWL Product Operation

5.1. The SA-OWL can be configured (as desired) for either:

5.1.1. Single-factor authentication (SFA): User may use either

5.1.1.1. Present a credential card

5.1.1.2. Press a secret PIN (personal identification number) code number on the Lock's keypad.

5.1.2. Two-factor authentication (2FA): User shall first present a credential card followed by a pressing a secret PIN code number on the lock's keypad.

5.2. Upon successful SFA or 2FA authentication

5.2.1. The LED turns green and

5.2.2. the lock is unlocked (for 4 seconds).

Else

5.2.3. the LED turns red

6. Presenting a Credential card: Magnetic Card Access

6.1. Using a programmed magnetic-stripe card.

6.2. The user inserts the card into the lock'd card slot

7. Entering secret PIN number on the Keypad

7.1. The user presses on the lock's keypad the secret PIN number.

8. LED indication codes

8.1. The CT-30 card reader (connected with Onity C3XDU10 wall reader controller) has two LEDs which can be used in various combinations to provide the user feedback on their access attempts.

8.2. The meaning of various LED indications are as follows:

8.2.1. **Solid green** – Valid authentication. Door either unlocks or can proceed to next authentication step.

8.2.2. **Solid red** – Invalid card (or pin code). The user credential or PIN is not authorized access to the door lock.

8.2.3. **Delayed solid red** – Unreadable card. The lock recognizes that a card was inserted but is unable to interpret the information on the card. The card may be damaged, blank or from another site. Access is not granted.

8.2.4. **Flashing green** – "Office mode" enabled. The door has been unlocked by the SA-Guardian software or has been activated by an owner for that particular door.

8.2.5. **Flashing red** – "Lockdown lock". Access is only provided to credential of those users who:

8.2.5.1. Have schedule access to the lock at that moment of time

And

8.2.5.2. Whose "Lockdown" capability is equal or greater than the lock's "Lockdown Level". (See Sa-Guardian application manual for more detail).

8.2.6. **Alternating red and green –** Out of valid time shift. The user is attempting to use a valid card outside the assigned parameters for that specific card for that door. Access is not granted. Contact your administrator to make necessary adjustments.

Appendix -1 Certifications

9. Federal Communications Commission
   9.1. FCC ID: **Y29SA-OWL**

USER INFORMATION FOR RF DEVICES

Part 15 - §15.21

10. Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Part 15 - Class A digital device or peripheral§15.105(a)

11. This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Part 15 - Class B digital device or peripheral§15.105(b)

12. This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

    —Reorient or relocate the receiving antenna.

    —Increase the separation between the equipment and receiver.

    —Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

    —Consult the dealer or an experienced radio/TV technician for help.