SA-ODL User Guide (Electronic Door Reader Lock)

**Document History**

| Version | Date | Author | Changes, Remarks |
|---|---|---|---|
| 1.0 | 05/04/2020 | JS | Initial document |
| 1.1 | 5/5/2020 | AS | Review & augmented |
| 1.2 | 5/10/2020 | AS | Edited per feedback from CT LLC. |

## 1. Purpose

1.1. This document provides instructions on how to operate the SecureALL SA-ODL electronic door reader / lock product.

1.2. This document provides information about:

1.2.1. Product Operation – Magnetic Card Access

1.2.2. Product Operation – Keypad Access

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

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

## 2. Introduction & Product Overview

2.1. **SA-ODL** is a retrofit kit that converts a standard Onity's CT30 lock (a standalone programming electronic door lock) into an on-line wireless lock. It provides real-time connectivity with the SA-Guardian application server, allowing system operators to remotely monitor, control and configures user's ability to use a credential to unlock the electronic door lock.

2.2. The retrofit involves the following:

2.2.1. Use all parts of Onity-CT30 door lock except its original controller PCB assembly.

2.2.2. Replace Onity's controller board with SecureALL's wireless controller board

2.2.3. Add an outside antenna plate assembly (in most cases it is sandwiched between CT30 outside escutcheon & the door)

2.2.4. Adds an inside scutcheon cover

2.2.5. Adds an inside adapter PCB assembly with switch sensors, LEDs, connectors and an antenna.

2.2.6. A cable assembly

2.3. The product dynamically discovers nearby SA-AP-200 router and after establishing credentials, the SA-AP-200 router provides SA-ODL with data communication connectivity with SecureALL's SA-Guardian Application Server.

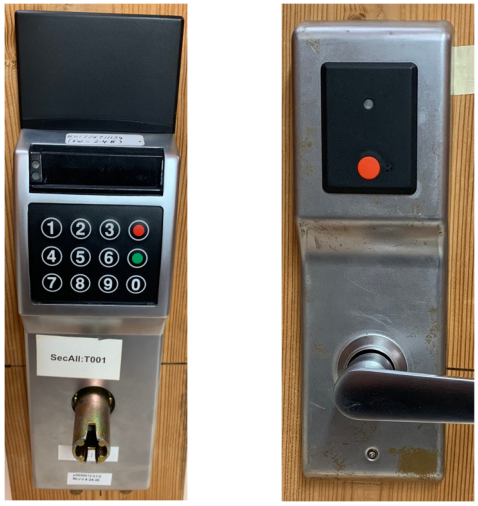


*Figure 1: SA-ODL upgraded CT30 Outside escutcheon and Inside escutcheon*

## 3. Caution & care

3.1. The SA-ODL is very simple to install and uses the same hole drill-out as a standard Onity-CT30 lock.

3.2. 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.

3.3. 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.

3.4. This device has been designed to operate with the antennas listed below, and having a maximum gain of 4dBi. Antennas not included in this list or having a gain greater than 4 dB are 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 proximity to the lock cover (escutcheon).

a. ODL Outside Antenna P/N: 810-000171

## 4. Modes of operation

4.1. Four operating modes are available to the SA-ODL 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 or Blocked Mode** – When a blocking card is presented to the lock, the Red LED will start flashing and the lock will enter blocking mode. When a lock is blocked, no guest keys, and only certain master users, will be allow access to the lock. To exit the blocking mode, present the blocking card again to the lock. The Green LED will flash once to indicate that the blocking has been removed.

4.3. **Privacy Mode** – When the privacy switch is engaged, typically when the deadbolt is engaged, only valid keys with the privacy override will be able to access the room.

## 5. SA-ODL Product Operation

5.1. The SA-ODL 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. SA-ODL LED indication codes**

8.1. The SA-ODL 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: **Y29-SA-ODL**
10. Industry Canada
    10.1. IC ID: ??

## USER INFORMATION FOR RF DEVICES

### Part 15 - §15.21

11. 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)

12. 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)

13. 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.

14. This is a Class A/B electronic device.
    14.1. Class A/B digital apparatus complies with Canadian ICES-003.
    14.2. Cet appareil numérique de la classe A/B est conforme à la norme NMB-003 du Canada.