wavelynx

Ethos Reader - Technical Support Guide

Version 6.1

03/1/2023

Table of Contents

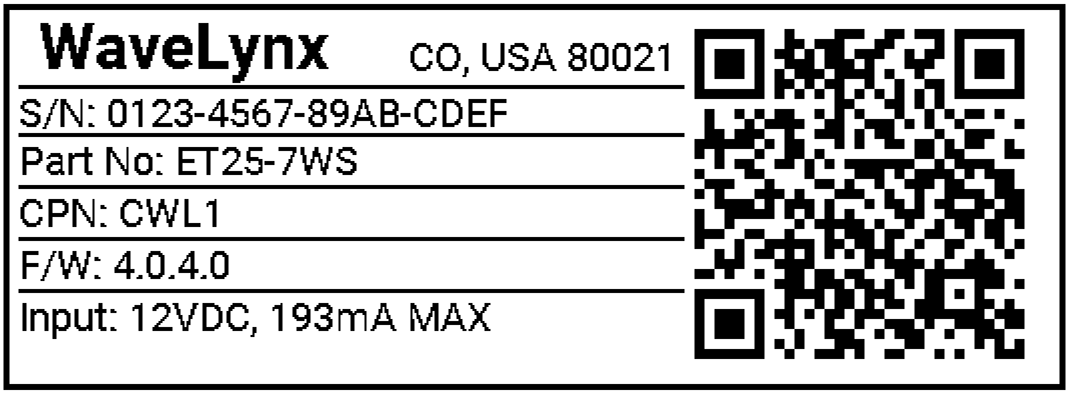
1 Identifying a Unit

All Ethos readers can be identified by their label. The product label can be found on the exterior of all units, located in the bottom right corner of the backplate.

The following key pieces of info are located on the label:

Serial Number	Unique unit serial number which also indicates the date of manufacture. *Old SN Example:* ***0821201900000043****, produced on: August 21, 2019.* *New SN Example:* ***0319-0000-0001-3357****, produced on: the 25th week (0x19) of 2021 (2018 + 0x03).*
Part No.	WaveLynx part number indicating any custom configurations applied to the unit.
CPN	OEM part/model number.
Firmware	The original firmware package loaded in the factory.

Example Label:



WaveLynx CO, USA 80021

S/N: 0123-4567-89AB-CDEF

Part No: ET25-7WS

CPN: CWL1

F/W: 4.0.4.0

Input: 12VDC, 193mA MAX

2 Custom Configurations

Ethos readers are offered with custom configurations for end users that require a product which differs in functionality and/or security from the default offering. Custom configurations can include modifications to any of the following:

- LEAF smart card keysets.
- Mobile credential keysets.
- A/V behavior (LEDs, Beeper, etc.).
- Disabling tamper
- Customized “Prox Filter”.
- Modified BLE behavior

2.1 Identifying a Custom Configuration

Custom configurations can be identified by the **CPN** field included in the product label. Records on the specifics of the configuration are kept by WaveLynx and should be referenced when dealing with a custom configured product.

One of the following identifiers will be present to indicate a custom configured product (note that “#” indicates a unique number or character sequence denoting the configuration):

Lk#####	Indicates a custom keyset.
C##	Indicates full custom configuration.
U####	Indicates full custom configuration.

Examples (custom config ID bolded):

- ET20-7FM-**U002**-LAM2
- ET10-6WS-**Lk40041**
- ET25-7FM-**CBI1**

2.2 Common Custom Configuration Features

Ethos readers offer a few common custom configuration features to enable higher security for an end user and allow them to transition their card holders from legacy technologies and systems. The details of these features are outlined below.

Custom LEAF DESfire Keyset

Ethos readers can be loaded from the factory with a custom DESFire smart card keyset to support the open **LEAF** EV2 application. A custom keyset provides an end user a higher security solution, as only cards programmed/encoded for their readers will function at their facility.

When supporting a custom keyed solution, the following should be noted:

- Only the end user's LEAF EV2 cards will result in a valid read (indicated by a beep/green flash) on the reader.
- When reading other smart cards, CSN reads may be disabled on the product.
- Custom keyed solutions only affect the card-reader communication and have no effect on the panel or PAC system connected to the reader.
- Any bitstream format can be encoded into a custom keyed LEAF EV2 smart card application, so there is no fixed format tied to a custom keyed solution.

Custom Mobile Credential Keyset

Just like DESFire keysets, Ethos readers can be loaded from the factory with a custom mobile credential keyset. A custom mobile credential keyset allows third party app/credential providers to issue customized credentials that integrate with their solutions.

When supporting a custom mobile keyed solution, the following should be noted:

- Only the specific mobile provider's applications will work with the readers (indicated by a beep/green flash) on the reader.
- Generic mobile credentials (such as MyPass) may not be compatible with the readers.
- Custom keyed solutions only affect the phone-reader communication and have no effect on the panel or PAC system connected to the reader.
- Any bitstream format can be encoded into a custom keyed mobile credential, so there is no fixed format tied to a custom keyed solution.

Custom Prox Filter

Ethos readers can also be configured with a custom "Prox Filter". A Prox Filter will block reads from FSK Proximity cards which contain a certain bitstream format or facility code (customer code). This allows an end user to transition from a legacy proximity card solution to a more secure smart card solution without rebadging their entire card population or replacing all of their readers at the same time.

The main advantage of a Prox Filter is to alleviate the issue of "double reads" from a dual-technology card when presented to a multi-technology reader. This also ensures that the secure smart card credential of the dual-technology card is authenticated and read when presented to a reader.

When supporting a product implementing a Prox Filter, the following should be noted:

- Prox Filters are configured differently for each end user based on their desired bitstream format and existing card population. Consult the custom configuration documentation for that end user for details on how their Prox Filter is configured.
- In most cases Prox Filters are set to ignore FSK Prox cards containing a specific bitstream and facility code (customer code). This means that Prox cards encoded with this data will **NOT** be read by the reader.

3 Reader Behavior

The following section describes normal operating behavior for each Ethos reader type with associated meanings. Any special features are also documented.

3.1 Standard AV Behavior

The following is the standard AV behavior for an Ethos reader. If a reader's AV behavior is behaving differently, it is likely behavior dictated by the controller or it may be a custom reader configuration (see section 2.1 Identifying a Custom Configuration).

Startup	On startup, the reader will flash to indicate which technologies it supports (1 or more of the following): ● **RED:** BLE. ● **GREEN:** 13.56 MHz Smart Cards (HF). ● **AMBER:** 125 kHz Prox (LF). ● **BLUE:** 4.0 Hardware Only The reader will then indicate which output mode it is in: ● **1 BEEP:** Wiegand Only. ● **2 BEEPS:** OSDP Only. ● **4 BEEPS:** OSDP Auto-Detect.
Idle	SOLID RED LED.
Physical/NFC Credential Read	1 BEEP + GREEN LED FLASH.
BLE Credential Read	**SOLID AMBER:** BLE Connected. **1 BEEP + GREEN FLASH:** Credential read success. **3 BEEPS:** Bad authentication/format.
Keypad	1 BEEP per press.

3.2 Wiegand-OSDP Readers

Wiegand-OSDP readers are considered a "slave" device when connected to a panel. Most LED and beeper functionality is dictated and controlled by the access control panel. Any autonomous behavior performed by the reader is documented in the **Operating Behavior** section.

Features

OSDP Auto-Detect	Upon first startup, the reader will enter OSDP Auto-detect: ● If an OSDP message is ever received from a panel, the reader will enter **OSDP** mode **until a reset is performed**. **Reset:** ***For firmware 3.0.1.0 and earlier:*** To reset a reader from **OSDP Only** to **OSDP Auto-detect**. 1. Remove power from the reader. 2. Place the reader in a **tampered** state (tilted at least 20 degrees from horizontal or vertical). 3. Power on the reader while in the tampered state and wait for the startup sequence to complete. 4. The reader will indicate it has been reset if **4 BEEPS** are emitted during startup. 5. Returning to OSDP Auto-detect will reset OSDP settings to default for these firmware versions. ***For firmware 4.0.0.0 to 4.0.4.0:*** 1. Remove power from the reader. 2. Tape any compatible access card to the reader face. 3. Power the reader. After 5 seconds, the reader LED will turn magenta. 4. Once the LED is magenta, power cycle the reader or remove the card and let the reader restart on its own once it completes its field configuration cycle. 5. When the reader restarts, it will indicate it has been reset if **4 BEEPS** are emitted during startup. 6. Returning to OSDP Auto-detect will not reset OSDP settings to default for these firmware versions. ***For firmware 3.1.0.0 and 4.1.0.0 and later:*** 1. Use configuration card *5044-FEA-OSDP-018* to send the reader back to OSDP auto-detect mode.
OSDP Defaults	● **Address:** 0. ● **Baud Rate:** 9600.

Panel Controlled Behavior

Wiegand Access Control Panel

RED, GREEN, AMBER LED	Asserted through control lines.
BEEPER	Asserted through control line.

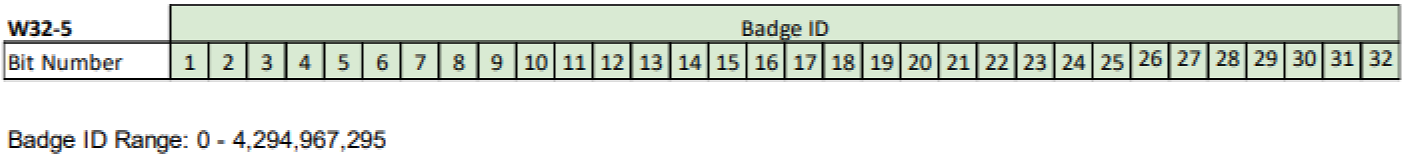
OSDP Access Control Panel

RED, GREEN, AMBER LED	Controlled through OSDP messaging.
BEEPER	Controlled through OSDP messaging.

3.3 MyPass Mobile App Behavior

MyPass Bit Format

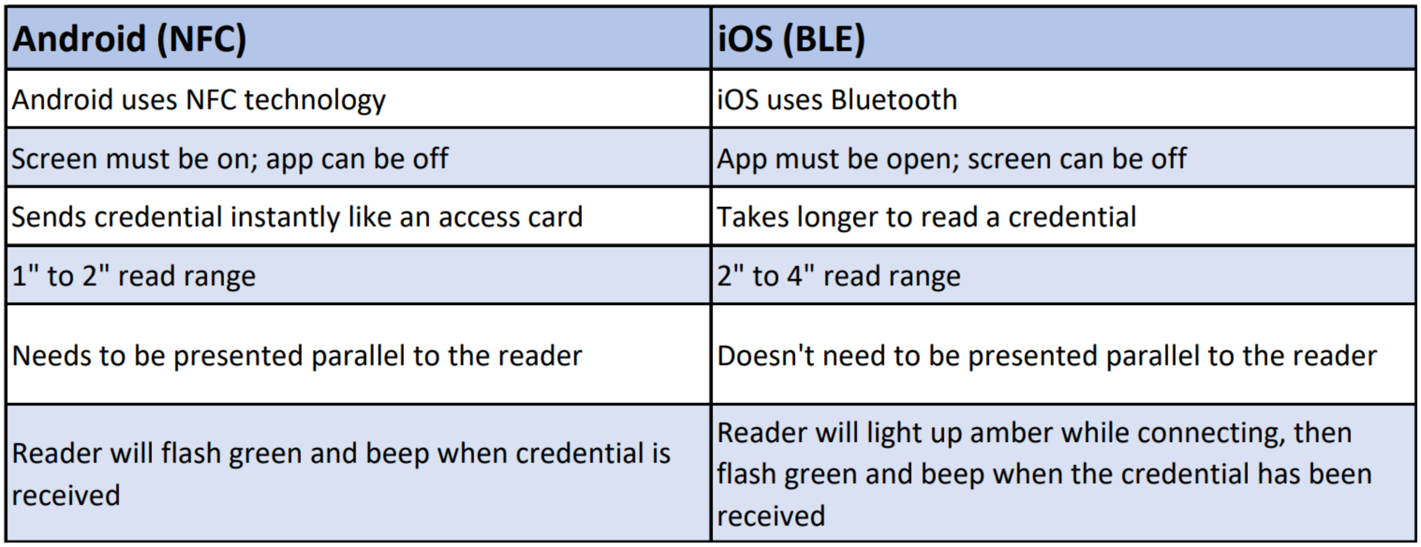
MyPass credentials are programmed to look like MiFare Classic CSN’s. They are 32 bit long credentials. The bitstream contains 32 bits of badge ID, no parity bits and no facility code bits.



W32-5	Badge ID																															
Bit Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

Badge ID Range: 0 - 4,294,967,295

MyPass performs differently depending on the operating system of the phone you are using. These differences are shown in the table below.



Android (NFC)	iOS (BLE)
Android uses NFC technology	iOS uses Bluetooth
Screen must be on; app can be off	App must be open; screen can be off
Sends credential instantly like an access card	Takes longer to read a credential
1" to 2" read range	2" to 4" read range
Needs to be presented parallel to the reader	Doesn't need to be presented parallel to the reader
Reader will flash green and beep when credential is received	Reader will light up amber while connecting, then flash green and beep when the credential has been received

4 Troubleshooting

The following sections detail a "sanity check" procedure for identifying the source of a potential issue with a unit. These steps will attempt to decouple the reader functionality from panel and PACs software configuration.

4.1 Generic Troubleshooting

Power Up

1. Remove power from the reader
2. (Optional) Remove all other wires connected to the panel. This step may be performed to eliminate the panel interference completely when troubleshooting a unit.
3. Re-power the reader and observe its behavior upon startup.
4. **Does the reader perform its normal startup sequence and then return to the normal idle state?**

Credential Read

1. (Optional) Remove all wires except power(RED) and ground(BLACK) connected to the panel. This step may be performed to eliminate panel interference completely when troubleshooting a unit.
2. Present a supported credential to the reader.
3. **Does the reader perform its normal credential read behavior?**

Control Lines (Wiegand Only)

1. Remove all control lines from their connections to the panel.
2. Ground each control line (i.e. assert it to 0V) one by one and observe the behavior at the reader.
3. **Does the green LED illuminate when the blue control line is grounded?**
4. **Does the red LED illuminate when the orange control line is grounded?**
5. **Does the amber LED illuminate when both the blue and orange control lines are grounded?**
6. **Does the beeper sound when the yellow control line is grounded?**

OSDP Connection

1. Remove power from the reader
2. Connect the green wire to RS485A and the white wire to RS485B
3. Re-power the reader.
4. Verify that the panel is successfully communicating with the reader prior to reading a credential or pressing a key.
5. If the reader is still not communicating with the panel, try swapping the white and green wires. (Note: RS485A and RS485B are swapped on some panels. This is specifically common on Lenel panels)
6. **Is the reader still not connecting to the panel?**

4.2 BLE Troubleshooting

BLE can be difficult to troubleshoot as the issue most often lies with the user's device/mobile operating system. These steps provide a basic set of procedures which will alleviate or determine the cause of an issue in most cases. There may be instances when a user's device simply will not function correctly with BLE. In these cases, nothing can be done as it is outside the control of the PACs system and mobile applications.

Common Procedure

1. Restart the mobile device.
2. Ensure that Bluetooth is **enabled** on the device.
3. Ensure that the mobile application has permission to use Bluetooth.
4. Open the associated mobile app.
5. Hold the phone directly against the reader.
6. **Does the reader LED turn AMBER indicating a BLE connection?**
7. Wait ~3 seconds for the transaction to complete.
8. **After the transaction completes, does the reader blink GREEN and BEEP once?**
9. **Does the app indicate credential read success?**
10. If 1 through 9 were completed successfully, then the mobile application and reader are functioning correctly.

Common Issues and Solutions

- **Issue:** The reader LED is turning amber briefly and then goes back to idle. The reader never beeps or flashes green and the credential is never sent.
- **Solution:** The app and the reader have a key mismatch. Verify the correct mobile app is being used for the reader configuration.

4.3 NFC Troubleshooting

Common Procedure

1. Ensure the correct mobile credential application is installed and the credential is active on the device.
2. Restart the mobile device.
3. Ensure that NFC is **enabled** on the device and the app has appropriate permissions.
4. Ensure the mobile application has permission to use NFC and location.
5. Unlock the device or ensure the screen is on.
6. Hold the device directly against the reader.
7. **Does the reader blink GREEN and BEEP once?**
8. If 1 through 7 were completed successfully, then the mobile application and reader are functioning correctly.

Common Issues and Solutions

- **Issue:** The mobile application says there is an NFC error.
- **Solution:** This may occur if there is another application on the phone which has registered support for the WaveLynx reader. Uninstall the other application and attempt to restart the current one.

4.4 Escalation

If an issue cannot be resolved in the field or with Tier 2 support staff (device reseller), the following info can be provided for an escalation to Tier 3/WaveLynx support staff:

- Detailed description of the issue.
- Steps taken to resolve the issue (follow common procedures from previous sections).
- What PACS software and Panel are being used?
- Reader details, including:
  - Label details:
    - Serial Number
    - Part Number
    - CPN
    - Firmware version
  - Panel Connection (OSDP/Wiegand).
  - Credential connection (physical, BLE, NFC, etc.)
- Mobile App/Phone Details (if mobile credential issue):
  - Model
  - OS Version
  - Mobile application being used
  - Mobile application version
- Physical Credential Details (if physical credential issue):
  - Card type (125 kHz, DESFire, etc.)
  - Credential part number
  - Bitstream format (if known)
  - Credential badge ID and facility code number (if known)

5 Field Configuration and Upgrades

Field Configuration can be performed on any Ethos reader through the use of a configuration card or by means of OSDP File Transfer. Field firmware upgrades can be performed using OSDP File Transfer.

5.1 Obtaining Configuration and Firmware Files

Configuration and firmware image files are distributed in the form of encrypted and signed binary (.bin) files. These may be obtained from WaveLynx upon request.

5.2 Configuration Card Application

1. Reset reader power, wait for the reader to complete its startup sequence and return to an idle state.
2. Within **1 minute**, present the desired configuration card to the reader.
3. The reader should **Beep 3 times**, followed by a reset.
4. When the reader has fully restarted, the new configuration will be applied.

5.3 OSDP Configuration

OSDP configurations do not need to occur within 1 minute of a power cycle and can be performed at any time.

1. Use the associated PACs software to push a configuration file to the panel and associated reader.
2. Once the file has been pushed successfully to the reader via OSDP file transfer, it will **Beep 3 times,** followed by a reset.
3. When the reader has fully restarted, the new configuration will be applied.

5.4 OSDP Firmware Upgrades

OSDP firmware upgrades do not need to occur within 1 minute of a power cycle and can be performed at any time.

1. Use the associated PACs software to push a firmware image file to the panel and associated reader.
2. Once the file has been pushed successfully to the reader via OSDP file transfer, the following A/V sequence will take place depending on the MCU being upgraded:
   a. **BLE MCU (3.X.X.X firmware):**
      i. Solid Amber LED for ~45 seconds.
      ii. Single beep denoting success.
   b. **Reader MCU (3.X.X.X firmware):**
      i. Alternating RED/GREEN LED.
      ii. 3-5 BEEPS followed by a reset.
      iii. Normal startup sequence.
   c. **Reader MCU (4.X.X.X firmware):**
      i. Solid Blue LED for ~45 seconds.
      ii. 3-5 BEEPS followed by a reset.
      iii. Normal startup sequence.

6 Wallet Support Details

6.1 Minimum Compatible Firmware Version

The minimum compatible firmware versions for wallet are 3.1.0.0 for Rev 3 hardware and 4.1.0.0 for Rev 4 hardware.

6.2 Customer Profile Explained

The reader configuration's Lk Number determines the TCI, DFName and encryption key settings used for the wallet. These settings together are referred to as the **"customer profile"**.

Readers can be ordered with the customer profile loaded in the factory or can have the customer profile loaded in the field. This can be done using OSDP file transfer, a BLE bootload or (if a firmware update isn't required) with a configuration card.

To see the correct TCI/DFNAME values for a given customer profile, check the TCI/DFNAME master list and reference the necessary Lk Number assigned to the customer profile. The TCI/DFNAME master list will be provided during onboarding for approved WaveLynx wallet partners.

6.3 When to use a Custom End User Specific Wallet Profile

A custom wallet profile needs to be assigned once an end user's wallet user base exceeds 500 users. A wallet profile can be assigned/created using the same process utilized for custom encryption keys.