IRXTO/IRXPTO Turnstile Reader Instructions

Part Number(s): IRXTO, IRXTO-BLE, IRXPTO, IRXPTO-BLE
Output: OSDP compatible format, default unit 0, & 9600 baud, or Wiegand (Jumper selectable) open format.
Operating Voltage: 5V DC +/10% or 12 VDC +/-10%, 250mA, Max (3W)
Temperature: -34° C to +65° C (-30° F to +150° F)

Wire connections

Wire Color	Description;
Red	5V or 12V
Black	Ground
Orange	RS485 B, OSDP Mode only
Violet	RS485 A, OSDP Mode only
Green	User Output 1 in OSDP mode or D0 in Wiegand Mode
White	D1 in Wiegand Mode only
Brown	User Input 1 in OSDP mode or LED toggle, (use open collector drive only), in Wiegand Mode
Yellow	Audio toggle, (use open collector drive only), Wiegand mode only

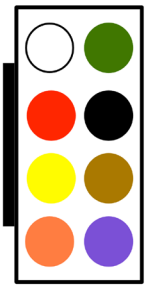
The following card formats are supported. For IRXTO & IRXPTO models;

iCLASS®
iCLASS SE®/SR
iCLASS® Seos®
MIFARE® Classic 1K/4K & SE
MIFARE® DESfire® EV1/EV2

The following Proximity technologies are supported. For IRXPTO Models only;

HID Prox	T5557
Indala Prox	FDX-B
EM4100	EM4450
EM4102	EM4305
EM4200	AWID Prox

For other formats, contact Essex Electronics for details.



WHITE - Data 1

GREEN - User output or Data 0

RED - Input Voltage, pos of power supply

BLACK - Circuit ground, neg of power supply

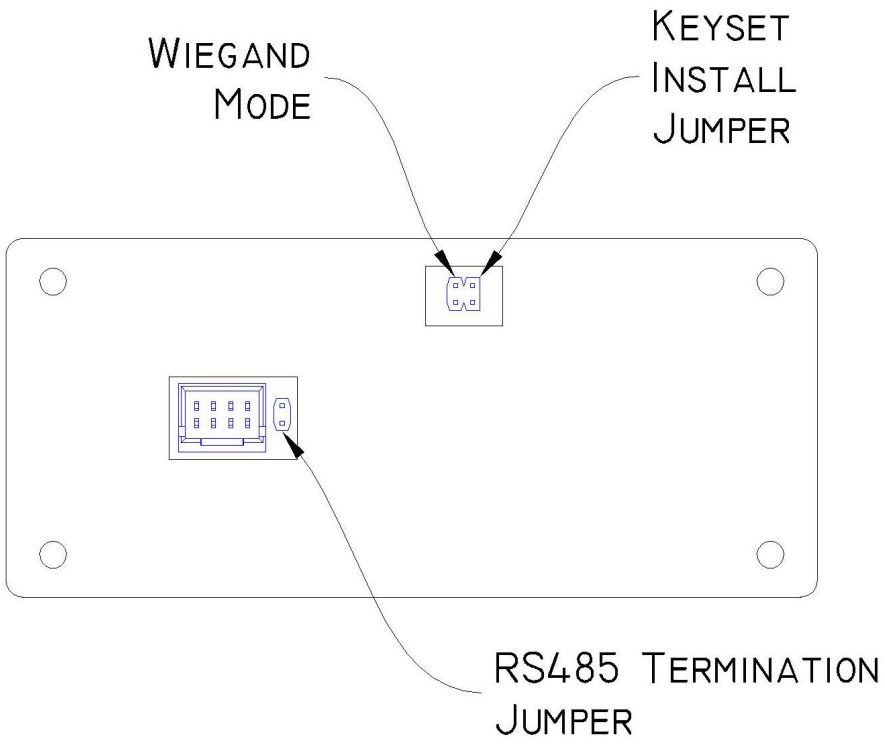
YELLOW - Audio Control;
ground = beep, open = off

BROWN - User input or LED Control;
ground = toggle to green, off = white standby

ORANGE - RS485 B

VIOLET - RS485 A

CAUTION: Do NOT run this low voltage wiring in conduit with or adjacent to line voltage wiring.



Modes

This reader has two modes of operation; it is shipped in Wiegand Mode. The OSDP mode, which conforms to the SIA standard 2.1.7 is selected by removal of the jumper. There are jumpers on the reader, visible through the windows. The installer may select the Wiegand mode by the installation of a jumper, (J1), located in a window on the cover of the enclosure.

Wiegand Mode

The reader is placed in this mode when the jumper on J1 is connected. Use this mode for control panels that require a Wiegand data stream.

In this mode, the yellow wire will control the audio when it is grounded. The brown wire will toggle the LEDs from white, in the X pattern, to green, in the O pattern.

OSDP Mode

The reader is placed in this mode when the Jumper on J1 is not installed. Use this mode for control panels that require OSDP inputs from the reader. Install mode jumper, (J4), is used to install a secure key through the controller.

The unit supports the standard OSDP version 2.1.7 commands that are appropriate for readers and keypads. It supports clear channel and secure channel communications. Install mode is available using a jumper on J4, at power up and must be initiated within 30 seconds of power on. Install mode allows the installation of a new SCBK.

The new version 2.2 commands ACURXSIZE, KEEPACTIVE, ABORT, PIVDATA, GENAUTH, CRAUTH, FILETRANSFER and XWR are not supported at this time.

Secure channel notes:

The standard installation procedure is used (commands CHLNG, SCRYPT, KEYSET). When an encryption key, other than the default, is installed, it must be used and secure channel communications are required. In the secure channel mode, certain OSDP commands are available on a clear channel. These are Poll, ID, CAP, CHLNG, and SCRYPT. Other commands will be answered with a NAK code 6 (encryption required).

In the OSDP mode, the brown input is a general purpose active low reported on the OSDP ISTATR command. The Wiegand D0 line becomes a general-purpose output line, osdp_OUT command.

The white leds that are in the X pattern are controlled by the OSDP LED command for Red leds. The green leds that are in the O pattern are controlled by the OSDP LED command for green leds.

Communications modes

The system can be in four different modes, three of which are for normal communications.

1. No custom key installed. No default security setup. All commands are available except the command to install the custom key. This mode is not recommended except for special circumstances since the communication is no more secure than Wiegand.

2. No custom key installed. Default key security enabled. All commands are available in secure mode except the install custom key command is only available when the install mode jumper is installed and the key is installed within 30 seconds of power on. This mode makes it difficult to snoop the communications unless the attacker has access to the communication line from the power startup. Communications lost for more than 8 seconds will cancel secure setup.

3. Custom key installed. Power up or communication restored. The secure channel must be setup using the CHLNG and CCYRPT commands. This is done in unsecured mode. No other commands are available. After the secure channel is setup, the communication moves to item 4 below.

4. Custom key installed and security enabled. All commands are available except the install custom key command is only available when the install mode jumper is installed and the key is installed within 30 seconds of power on. This is not vulnerable to attackers even with access to the communications line at powerup. Security with the default key is not allowed if a custom key is installed.

Note: If the custom key is lost, the custom key cannot be changed without factory assistance

Installation of Mobile access key.

Using the mobile access key, is purchased or obtained from HID Global. This should be card part number SEC9X-CRD-E-MKYD ordered with your customer's mobile access key as maintained by HID Global's ORIGO page.

On powering up the reader, within 30 seconds, present the key card to the reader and wait for the reader to accept and configure itself to that key.

Any mobile access enabled phone, with BLE capacity, and with an assigned mobile access credential may now present to the reader, with a “tap” which will send the credential to the reader BLE receiver, which will send this credential to the system to release the turnstile for entry.

We recommend that the installer and/or user become familiar with HID Global’s Mobile Access usage.

https://www.hidglobal.com/solutions/mobile-access-solutions

https://www.hidglobal.com/documents/hid-mobile-access-solutions-datasheet

https://www.hidglobal.com/mobile-access-compatible-devices