

# ioSmart Card Reader Installation Guide



Building Technologies & Solutions  
[www.kantech.com](http://www.kantech.com)  
2020-07-21

D29008984R004  
DN2187-2007



# Contents

TYCO INTERNATIONAL LTD END-USER LICENSE AGREEMENT.....	5
Technical support.....	8
United States and Canada.....	8
Latin America and Caribbean.....	8
Europe, Middle East, and Africa.....	9
Asia Pacific.....	9
Copyright information.....	11
Safety instructions.....	12
System overview.....	13
Unpacking the ioSmart card reader.....	14
ioSmart mobile smart keys.....	15
Changing the ioSmart card reader from standard to panel-less mode.....	16
Changing the ioSmart card reader from panel-less to standard mode.....	16
Upgrading the ioSmart card reader.....	17
ioSmart card reader models.....	18
Mullion ioSmart card reader.....	18
Single Gang ioSmart card reader.....	20
Technical features.....	21
Wiegand mode.....	21
RS-485 mode.....	21
BLE mode.....	21
RFID technologies.....	21
Capacitive touch keypad.....	21
Auto-detection.....	21
LED status bar.....	22
Optical tamper.....	22
Technical specifications.....	23
Mounting.....	25
Mounting the ioSmart card reader.....	25
Wiring.....	27
Wiring distance.....	27
Six pole screwless terminal block.....	29
RS-485 mode.....	29
Wiegand mode.....	29
RS-485 wiring.....	30
RS-485 CAT5 wiring.....	31
RS-485 lock output wiring.....	32
BLE lock output wiring for panel-less mode.....	33
Wiegand wiring.....	34
Wiegand CAT5 wiring.....	35

Connecting multiple readers to a controller.....	35
Daisy chain wiring.....	36
Star wiring.....	37
Configuring the reader.....	38
Configuring the reader using the terminals.....	38
Factory default (SSF transmission format).....	38
Hard reset (SSF transmission format).....	39
34-bit transmission format.....	40
26-bit transmission format.....	41
Sending the unique identifier (UID).....	42
Configuring the reader using a Kantech smartcard.....	43
Compliance specifications.....	44
FCC.....	44
CE compliance.....	44
UL Standards compliance.....	44
NIST (National Institute of Standards and Technology).....	45
RoHS (Restriction on Hazardous Substances).....	45
WEEE (Waste Electrical and Electronic Equipment).....	45

# TYCO INTERNATIONAL LTD END-USER LICENSE AGREEMENT

FOR KANTECH Software provided with or without products or components

## **IMPORTANT - READ CAREFULLY**

**KANTECH Software purchased with or without Products and Components is copyrighted and is purchased under the following license terms:**

- This End-User License Agreement (“EULA”) is a legal agreement between You (the company, individual or entity who acquired the Software and any related Hardware) and KANTECH, the manufacturer of the integrated security systems and the developer of the software and any related products or components (“HARDWARE”) which You acquired.
- If the KANTECH software product (“SOFTWARE PRODUCT” or “SOFTWARE”) is intended to be accompanied by HARDWARE, and is NOT accompanied by new HARDWARE, You may not use, copy or install the SOFTWARE PRODUCT. The SOFTWARE PRODUCT includes computer software, and may include associated media, printed materials, and “online” or electronic documentation.
- Any software provided along with the SOFTWARE PRODUCT that is associated with a separate end-user license agreement is licensed to You under the terms of that license agreement.
- By installing, copying, downloading, storing, accessing or otherwise using the SOFTWARE PRODUCT, You agree unconditionally to be bound by the terms of this EULA, even if this EULA is deemed to be a modification of any previous arrangement or contract. If You do not agree to the terms of this EULA, KANTECH is unwilling to license the SOFTWARE PRODUCT to You, and You have no right to use it.

## **SOFTWARE PRODUCT LICENSE**

**a** - The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed, not sold.

### **1 - GRANT OF LICENSE - This EULA grants You the following rights:**

**a** - Software Installation and Use - For each license You acquire, You may have only one copy of the SOFTWARE PRODUCT installed.

**b** - Storage/Network Use - The SOFTWARE PRODUCT may not be installed, accessed, displayed, run, shared or used concurrently on or from different computers, including a workstation, terminal or other digital electronic device (“Device”). In other words, if You have several workstations, You will have to acquire a license for each workstation where the SOFTWARE will be used.

**c** - Backup Copy - You may make back-up copies of the SOFTWARE PRODUCT, but You may only have one copy per license installed at any given time. You may use the back-up copy solely for archival purposes. Except as expressly provided in this EULA, You may not otherwise make copies of the SOFTWARE PRODUCT, including the printed materials accompanying the SOFTWARE.

### **2 - DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS**

**a** - Limitations on Reverse Engineering, Decompilation and Disassembly - You may not reverse engineer, decompile, or disassemble the SOFTWARE PRODUCT, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation. You may not make any changes or modifications to the Software, without the written permission of an officer of KANTECH. You may not remove any proprietary notices, marks or labels from the Software Product. You shall institute reasonable measures to ensure compliance with the terms and conditions of this EULA.

**b** - Separation of Components - The SOFTWARE PRODUCT is licensed as a single product. Its component parts may not be separated for use on more than one HARDWARE unit.

**c** - Single INTEGRATED PRODUCT - If You acquired this SOFTWARE with HARDWARE, then the SOFTWARE PRODUCT is licensed with the HARDWARE as a single integrated product. In this case, the SOFTWARE PRODUCT may only be used with the HARDWARE as set forth in this EULA.

**d** - Rental - You may not rent, lease or lend the SOFTWARE PRODUCT. You may not make it available to others or post it on a server or web site.

**e** - Software Product Transfer - You may transfer all of Your rights under this EULA only as part of a permanent sale or transfer of the HARDWARE, provided You retain no copies, You transfer all of the SOFTWARE PRODUCT (including all component parts, the media and printed materials, any upgrades and this EULA), and provided the recipient agrees to the terms of this EULA. If the SOFTWARE PRODUCT is an upgrade, any transfer must also include all prior versions of the SOFTWARE PRODUCT.

**f** - Termination - Without prejudice to any other rights, KANTECH may terminate this EULA if You fail to comply with the terms and conditions of this EULA. In such event, You must destroy all copies of the SOFTWARE PRODUCT and all of its component parts.

**g** - Trademarks - This EULA does not grant You any rights in connection with any trademarks or service marks of KANTECH or its suppliers.

### **3 - COPYRIGHT**

All title and intellectual property rights in and to the SOFTWARE PRODUCT (including but not limited to any images, photographs, and text incorporated into the SOFTWARE PRODUCT), the accompanying printed materials, and any copies of the SOFTWARE PRODUCT, are owned by KANTECH or its suppliers. You may not copy the printed materials accompanying the SOFTWARE PRODUCT. All title and intellectual property rights in and to the content, which may be accessed through use of the SOFTWARE PRODUCT, are the property of the respective content owner and may be protected by applicable copyright or other intellectual property laws and treaties. This EULA grants You no rights to use such content. All rights not expressly granted under this EULA are reserved by KANTECH and its suppliers.

### **4 - EXPORT RESTRICTIONS**

You agree that You will not export or re-export the SOFTWARE PRODUCT to any country, person, or entity subject to US export restrictions.

### **5 - CHOICE OF LAW**

This Software License Agreement is governed by the laws of the State of New York.

### **6 - LIMITED WARRANTY**

#### **a - NO WARRANTY**

KANTECH PROVIDES THE SOFTWARE "AS IS" WITHOUT WARRANTY. KANTECH DOES NOT WARRANT THAT THE SOFTWARE WILL MEET YOUR REQUIREMENTS OR THAT OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE.

#### **b - CHANGES IN OPERATING ENVIRONMENT**

KANTECH shall not be responsible for problems caused by changes in the operating characteristics of the HARDWARE, or for problems in the interaction of the SOFTWARE PRODUCT with non-KANTECH SOFTWARE or HARDWARE PRODUCTS.

#### **c - LIMITATION OF LIABILITY; WARRANTY REFLECTS ALLOCATION OF RISK**

IN ANY EVENT, IF ANY STATUTE IMPLIES WARRANTIES OR CONDITIONS NOT IN THIS LICENSE AGREEMENT, KANTECH'S ENTIRE LIABILITY UNDER ANY PROVISION OF THIS LICENSE AGREEMENT SHALL BE LIMITED TO THE GREATER OF THE AMOUNT ACTUALLY PAID BY YOU TO LICENSE THE SOFTWARE PRODUCT AND FIVE US DOLLARS (USD\$5.00). BECAUSE SOME JURISDICTIONS DO

NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

**d - DISCLAIMER OF WARRANTIES**

THIS WARRANTY CONTAINS THE ENTIRE WARRANTY AND SHALL BE IN LIEU OF ANY AND ALL OTHER WARRANTIES, WHETHER EXPRESSED OR IMPLIED (INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE) AND OF ALL OTHER OBLIGATIONS OR LIABILITIES ON THE PART OF KANTECH. KANTECH MAKES NO OTHER WARRANTIES. KANTECH NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON PURPORTING TO ACT ON ITS BEHALF TO MODIFY OR TO CHANGE THIS WARRANTY, NOR TO ASSUME FOR IT ANY OTHER WARRANTY OR LIABILITY CONCERNING THIS SOFTWARE PRODUCT.

**e - EXCLUSIVE REMEDY AND LIMITATION OF WARRANTY**

UNDER NO CIRCUMSTANCES SHALL KANTECH BE LIABLE FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL OR INDIRECT DAMAGES BASED UPON BREACH OF WARRANTY, BREACH OF CONTRACT, NEGLIGENCE, STRICT LIABILITY, OR ANY OTHER LEGAL THEORY. SUCH DAMAGES INCLUDE, BUT ARE NOT LIMITED TO, LOSS OF PROFITS, LOSS OF THE SOFTWARE PRODUCT OR ANY ASSOCIATED EQUIPMENT, COST OF CAPITAL, COST OF SUBSTITUTE OR REPLACEMENT EQUIPMENT, FACILITIES OR SERVICES, DOWN TIME, PURCHASERS TIME, THE CLAIMS OF THIRD PARTIES, INCLUDING CUSTOMERS, AND INJURY TO PROPERTY.

**⚠ WARNING: KANTECH recommends that the entire system be completely tested on a regular basis. However, despite frequent testing, and due to, but not limited to, criminal tampering or electrical disruption, it is possible for this SOFTWARE PRODUCT to fail to perform as expected.**

# Technical support

See the following technical support contact details and opening hours in your region.

## United States and Canada

For technical support, use the phone number for your area or go to:

[https://kantech.com/Support/Contact\\_Technical\\_Support\\_Advanced.aspx](https://kantech.com/Support/Contact_Technical_Support_Advanced.aspx).

**Table 1: United States and Canada telephone numbers**

Area	Call type	Opening times: 08:00 to 20:00 (EST)
United States and Canada	Toll free	+1 888 222 1560
United States and Canada	Toll free	+1 800 507 6268 option 4

## Latin America and Caribbean

For technical support, contact us at one of the following email addresses or use the phone number for your area.

- For access technical support, email [access-support@jci.com](mailto:access-support@jci.com).
- For video technical support, email [video-support@jci.com](mailto:video-support@jci.com).
- For technical training inquiries, email [latam.certificaciones@jci.com](mailto:latam.certificaciones@jci.com).

**Table 2: Latin America and Caribbean telephone numbers**

Area	Call type	Opening times: 08:00 to 20:00 (EST)
Latin America and Caribbean	Toll free	+1 800 507 6268
Latin America and Caribbean	Toll free	+1 800 392 2873
Argentina, Buenos Aires	Direct	+54 11 5199 3104
Brazil, Sao Paolo	Direct	+55 11 3181 7377
Chile, Santiago	Direct	+56 2 3210 9662
Colombia, Cali	Direct	+57 2 891 2476
Colombia, Medellin	Direct	+57 4 204 0519
Costa Rica, National VOIP	Direct	+506 4 000 1655
Dominican Republic, Santo Domingo	Direct	+1 829 235 3047
El Salvador, San Salvador	Direct	+503 2 136 8703
Guatemala, Guatemala City	Direct	+502 2 268 1206
Mexico, Mexico City	Direct	+52 55 8526 1801
Panama, Panama City	Direct	+507 836 6265
Peru, Lima	Direct	+51 1 642 9707
Venezuela, Caracas	Direct	+58 212 720 2340



## Europe, Middle East, and Africa

For technical support, contact us at one of the following email addresses or use the phone number for your area.

- For technical post-sales inquiries, email [video-support@jci.com](mailto:video-support@jci.com).
- For technical training inquiries, email [emea.training@tycoint.com](mailto:emea.training@tycoint.com).
- For all licensing inquiries, email [sp-licensing-support@jci.com](mailto:sp-licensing-support@jci.com).

**Table 3: Europe, Middle East, and Africa telephone numbers**

Area	Call type	Opening times: 08:00 to 18:00 (CET)
Europe, Middle East, and Africa	Toll free	+800 2255 8926
Europe, Middle East, and Africa	Direct	+31 475 352 722
Bahrain	Direct	(0)800 04127
Belgium	Direct	+0800 76 452
Denmark	Direct	+45 4494 9001
France	Direct	+0800 90 79 72
Germany	Direct	+0800 1806 757
Greece	Direct	00800 312 294 53
Ireland	Direct	+1800 94 3570
Israel	Direct	+972 772 201 350
Italy	Direct	+39 0230 510 112
KSA	Direct	+96 6800 8500 509
Kuwait	Direct	(0)22062915
Lebanon	Direct	01 426 801, new dial tone and then dial 8552 3436 77
Nordic Countries	Direct	04494 9001
Oman	Direct	(00) 8007 4364
Qatar	Direct	(00) 800100841
Russia	Direct	81 0800 2052 1031
South Africa	Direct	+27 (0) 10 100 3292
Spain	Direct	+900 99 31 61
Turkey	Direct	+00800 3192 3007
United Arab Emirates	Direct	(0)800 0310 7123
United Kingdom	Direct	+44 330 777 1300

## Asia Pacific

For technical support, contact us at one of the following email addresses or use the phone number for your area.

- For video technical support, email [video-support@jci.com](mailto:video-support@jci.com).
- For technical training inquiries, email [apac.training@jci.com](mailto:apac.training@jci.com).
- For all licensing inquiries, email [sp-licensing-support@jci.com](mailto:sp-licensing-support@jci.com).

**Table 4: Asia Pacific telephone numbers**

<b>Area</b>	<b>Call type</b>	<b>Opening times: 09:00 to 18:00 (CST China Standard Time) and 09:00 to 19:00 (India Time)</b>
Asia Pacific	Toll free	+ 800 2255 8926
Australia	Direct	+1 800 580 946
China	Direct	+86 21 6163 8644
India	Direct	+91 80 4199 0994
Oceania and New Zealand	Direct	+64 9942 4004

## Copyright information

© 2020 Johnson Controls. All rights reserved. JOHNSON CONTROLS, TYCO and KANTECH are trademarks of Johnson Controls.

## Safety instructions

This equipment, RS-485 ioSmart Card Reader, shall be installed and used within an environment that provides the pollution degree max 2 and overvoltages category II, in NON HAZARDOUS LOCATIONS only. The equipment is FIXED and is powered from a Limited Power Source from the controller to which it is connected; it is designed to be installed by Service Persons only; [Service Person is defined as a person having the appropriate technical training and experience necessary to be aware of hazards to which that person may be exposed in performing a task and of measures to minimize the risks to that person or other persons].

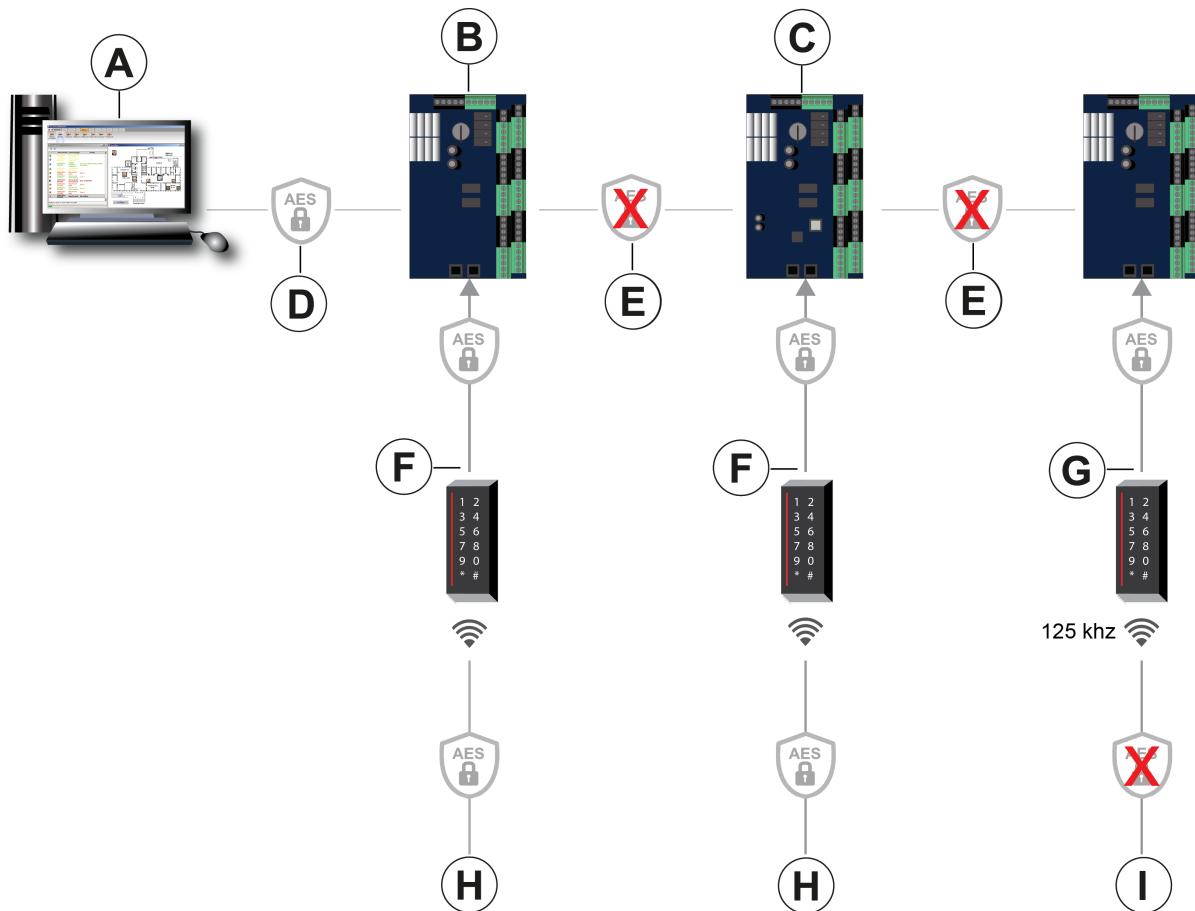
# System overview

Kantech ioSmart card readers in RS-485 mode provide end-to-end encryption when they are used with other products such as Kantech controllers and EntraPass access control management software.

The ioSmart card readers in RS-485 mode use AES 128-bit (U.S. NIST encryption specification) between the following:

- The ioSmart card reader and the ID badge credentials.
- The ioSmart card reader and the Kantech controller.
- The Kantech controller and the EntraPass software. An IP or RS-485 connection is required.

**Figure 1: ioSmart card reader encryption overview**



**Table 5: ioSmart card reader encryption overview**

Callout	Description
A	EntraPass
B	Master
C	Subordinate
D	IP (AES 128-bit encrypted)
E	Standard RS-485

**Table 5: ioSmart card reader encryption overview**

Callout	Description
F	RS-485 (AES 128-bit encrypted)
G	RS-485 Protocol M (AES 128-bit encrypted)
H	MIFARE PLUS EV1 (AES 128-bit encrypted)
I	HID Prox, ioProx, HID Iclass CSN

The ioSmart card readers support the transmission of card numbers using Wiegand protocol.

The ioSmart card readers support the following formats:

- Standard 34-bit format
- Standard 26-bit format
- Most common HID formats
- Other Kantech proprietary formats including eXtended Secure Format (XSF) and Smartcard Secure Format (SSF)

You can install ioSmart card readers inside or outside. For PIN entry and other functions, some models integrate a backlit, capacitive touch keypad. For security purposes, you must install panel-less (no controller) readers on the secure side of the door.

To upgrade easily, some models support both ioSmart card technology and Kantech ioProx proximity technology.

- ① **Note:** For information about the available models and the supported credentials for each model, see [Technical specifications](#).

## Unpacking the ioSmart card reader

Before you install the reader, check that the product box contains the following items:

- One ioSmart card reader
- Two 11.1K  $\Omega$  resistors
- Four 5.6K  $\Omega$  resistors
- One Phillips head screw, #6-32
- One *ioSmart Card Reader Installation Sheet*

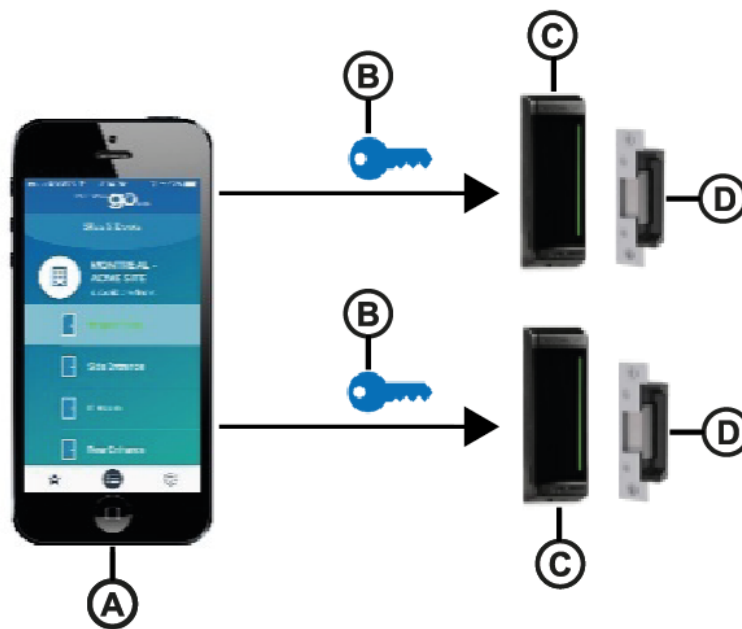
## ioSmart mobile smart keys

Using the ioSmart card reader Bluetooth low energy (BLE) mobile technology, smart keys provide panel-less, managed access to offline doors, or other powered, lock-controlled openings. Administrators can create, edit, issue, and revoke smart keys for personnel, remotely and on demand, without access to physical cards.

In panel-less mode, ioSmart card readers do not require any local network connectivity and provide cloud-managed access control for mobile users even when the mobile device hosting the EntraPass mobile application is disconnected from the internet. Tyco Cloud services manage the smart keys and deliver them to the EntraPass go Pass mobile application.

**⚠ WARNING:** Controlled door locks may be governed by regulatory bodies and must always be installed according to local regulations. In most instances, there are strict limitations to installing fail-secure devices and fail-safe locking devices such as magnetic locks or other similar locking devices on doors that are used as emergency exits.

**Figure 2: ioSmart mobile smart keys**



**Table 6: ioSmart mobile smart keys**

Callout	Description
A	Smartphone with the EntraPass go Pass application
B	Smart key
C	ioSmart card reader
D	Door strike

## Changing the ioSmart card reader from standard to panel-less mode

To change the ioSmart card reader from standard mode to panel-less mode, complete the following steps:

1. If the reader is connected to a controller and authenticated, you must factory default it before you can configure it as a panel-less reader. To factory default the reader, see [Factory default \(SSF transmission format\)](#).
2. To define the reader as panel-less, log on to Tyco Cloud: <https://cloudvue.com/login>.
  - a. On the **Live** page, on the **Access** tab, find the reader and click the **Edit** icon.
  - b. On the **Settings** page, in the **General** pane, from the **Function Mode** list, select **Panelless (Mobile Smart Key Door)**.
3. From the EntraPass go Pass application, send three valid unlock requests in panel-less mode.

When an ioSmart card reader is in panel-less mode, it does not generate Wiegand code and it cannot be connected over RS-485 to a controller.

## Changing the ioSmart card reader from panel-less to standard mode

To change the ioSmart card reader from panel-less mode to standard mode, factory default or perform a hard reset on the reader.

- **Important:** Forcing the reader to factory default deletes all custom settings from the reader, and you may need to contact technical support to reset it. Therefore, it is highly recommended not to factory default a panel-less reader but to perform a hard reset instead. To perform a hard reset, see [Hard reset \(SSF transmission format\)](#).



## Upgrading the ioSmart card reader

The ioSmart card readers are field upgradable with future firmware releases and can be upgraded using RS-485 communication with a KT-1 or KT-400 controller through EntraPass or through the KT-Standalone connection.

If you use a Kantech controller with EntraPass, perform upgrades on the **Operation** tab.

If you use the KT-Standalone connection, perform upgrades under **Admin > Firmware > Update ioSmart**.

① **Note:** You cannot perform field upgrades in panel-less mode.

## ioSmart card reader models

There are two ioSmart card reader sizes, the Mullion and the Single Gang. The Mullion has three models and the Single Gang has three models.

### Mullion ioSmart card reader

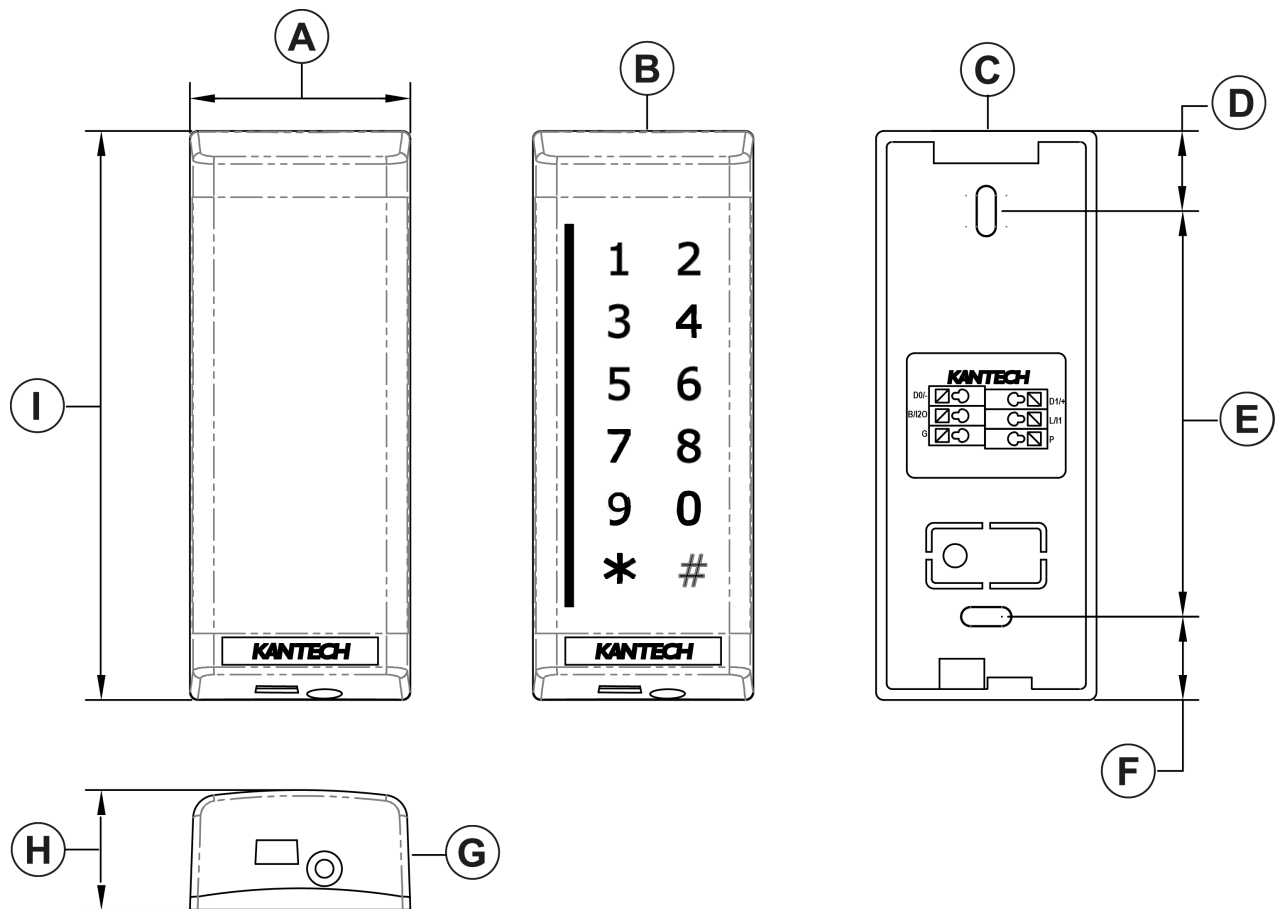
The following table lists the Mullion ioSmart card reader models.

**Table 7: Mullion ioSmart card reader models**

Model	Type	RFID
KT-MUL-SC	Mullion	13.56 MHz
KT-MUL-MT	Multi-technology Mullion	13.56 MHz + 125 kHz
KT-MUL-MT-KP	Multi-technology Mullion with a keypad	13.56 MHz + 125 kHz

The following figure shows the dimensions of the Mullion ioSmart card reader.

**Figure 3: Mullion ioSmart card reader dimensions**



**Table 8: Mullion ioSmart card reader dimensions**

Callout	Description
A	1.770 in. (44.96 mm)
B	Reader with a keypad
C	Rear view of the reader

**Table 8: Mullion ioSmart card reader dimensions**

<b>Callout</b>	<b>Description</b>
D	0.643 in. (16.32 mm)
E	3.254 in. (82.65 mm)
F	0.669 in. (16.99 mm)
G	Elevation
H	0.964 in. (24.48 mm)
I	4.565 in. (115.95 mm)

# Single Gang ioSmart card reader

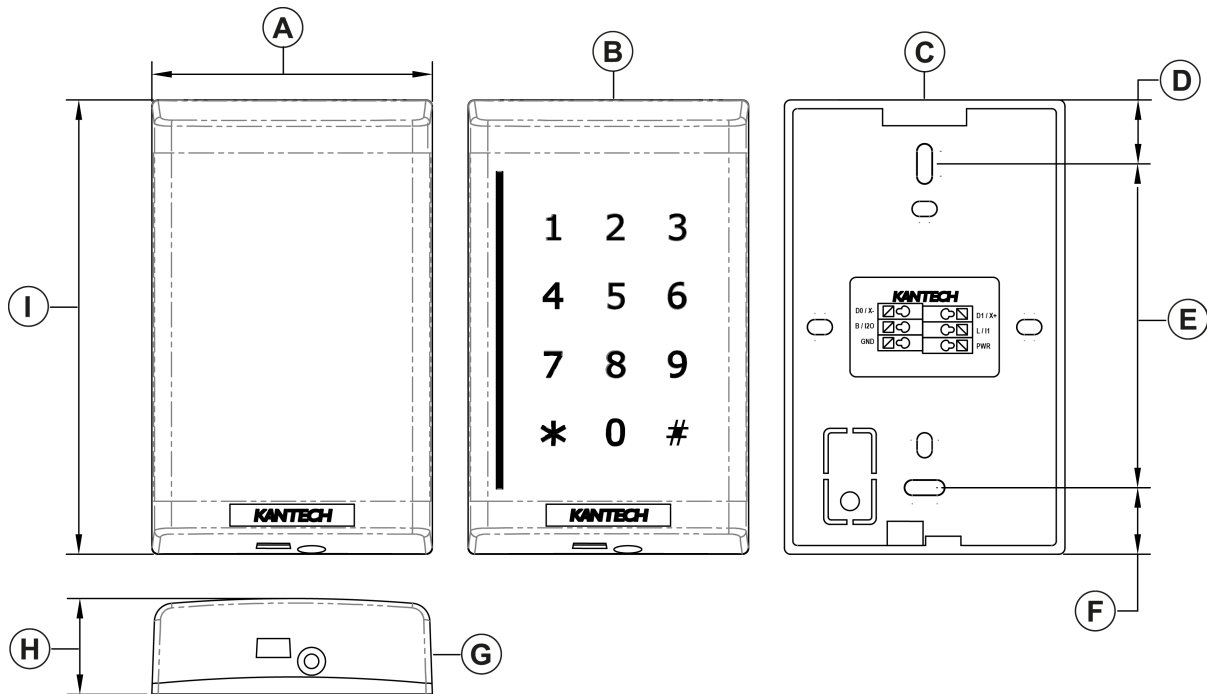
The following table lists the Single Gang ioSmart card reader models.

**Table 9: Single Gang card reader models**

Model	Type	RFID
KT-SG-SC	Single Gang	13.56 MHz
KT-SG-MT	Multi-technology Single Gang	13.56 MHz + 125 kHz
KT-SG-MT-KP	Multi-technology Single Gang with a keypad	13.56 MHz + 125 kHz

The following figure shows the dimensions of the Single Gang ioSmart card reader.

**Figure 4: Single Gang ioSmart card reader dimensions**



**Table 10: Single Gang ioSmart card reader dimensions**

Callout	Description
A	2.820 in. (71.63 mm)
B	Reader with a keypad
C	Rear view of the reader
D	0.643 in. (16.32 mm)
E	3.254 in. (82.65 mm)
F	0.669 in. (16.99 mm)
G	Elevation
H	0.964 in. (24.48 mm)
I	4.565 in. (115.95 mm)

## Technical features

Use this section to find out about the technical features of the ioSmart card reader.

### Wiegand mode

The ioSmart card reader is compatible with all Kantech controllers through the Wiegand communication interface and with all third party access controllers supporting Wiegand 26-bit or 34-bit standard.

### RS-485 mode

The RS-485 mode supports KT-400 and KT-1 access controllers.

### BLE mode

In BLE mode, you can configure the ioSmart card reader in the following two ways:

- **Panel mode:** connected to a controller Wiegand or RS-485. The ioSmart card reader supports standard reading using cards and keypads, and accepts BLE access requests from the EntraPass go Pass application.
- **Panel-less mode:** no controller required. The ioSmart card reader supports only BLE access requests from the EntraPass go Pass application and acts as a lock controller with a supervised lock output and two optional door inputs. For more information, see [BLE lock output wiring for panel-less mode](#).

### RFID technologies

Wire loop antennas are used to generate the radio frequency identification (RFID) signals and are compatible with ioSmart, ioProx, and HID proximity cards.

### Capacitive touch keypad

On the reader keypad, the 12 capacitive touch keys are backlit with light-emitting diodes (LEDs). By default, the backlighting illuminates in the following situations:

- When you tap the keypad. The first tap is not considered an entry.
- When you swipe a card.

After the backlighting illuminates, you can enter digits.

The reader dims and turns off to save energy if there is no interaction for a set amount of time. Configure the no interaction time in EntraPass. The default time is 10 seconds.

❗ **Note:** Panel-less mode does not support the capacitive touch keypad.

### Auto-detection

After installation, you do not have to configure the reader. The reader defaults to Wiegand automatically. To detect RS-485, it switches format automatically.

❗ **Note:** Auto-detection does not work in panel-less mode.

## LED status bar

The LED status bar indicates various access conditions to the user. The following table lists the default LED colors and the statuses that they indicate.

**Table 11: LED status bar**

LED color	Status
Red	Locked
Green	Unlocked
Blue	Keypad press
Yellow	Warning: tamper alarm, low power, or locking device issue.

- ① **Note:** In RS-485 mode, the reader supports up to eight status colors that you can customize in EntraPass.

## Optical tamper

For tamper security, a light reflective sensor on the reader detects a reflective part on the mounting plate. Tamper detection initiates if the reader separates from the mounting plate by more than 5 mm. To mount directly to a wall, use a detachable bracket. In this position, tamper detection initiates if the whole assembly separates from the wall.

The security-enhancing optical tamper is available in RS-485 mode and in Wiegand mode. In Wiegand mode, for firmware 1.04 and higher, you must activate the optical tamper feature for the KT-400 and the KT-1 controllers to support it. To activate the optical tamper feature, see mode 8 in Table 22.

## Technical specifications

The following table outlines the technical specifications for the Mullion and the Single Gang ioSmart card readers.

**Table 12: Technical specifications**

Specification	Mullion			Single Gang		
<b>Model</b>	KT-MUL-MT-KP	KT-MUL-MT	KT-MUL-SC	KT-SG-MT-KP	KT-SG-MT	KT-SG-SC
<b>RF technologies</b>	13.56 MHz 125 kHz	13.56 MHz 125 kHz	13.56 MHz	13.56 MHz 125 kHz	13.56 MHz 125 kHz	13.56 MHz
<b>Power consumption (mA) at 12 VDC peak /average</b>	200 mA / 80 mA	120 mA / 70 mA	120 mA / 70 mA	200 mA / 80 mA	120 mA / 70 mA	120 mA / 70 mA
<b>Weight</b>	110 g (0.24 lb)	110 g (0.24 lb)	105 g (0.23 lb)	175 g (0.40 lb)	170 g (0.37 lb)	165 g (0.36 lb)
<b>Capacitive touch keypad with backlighting</b>	Yes	No	No	Yes	No	No
<b>Typical read range 125 kHz ioProx ID-1 credentials (cards)</b>	Up to 5.1 cm (2 in.)			Up to 6.8 cm (2.7 in.)		
<b>Typical read range 13.56 MHz MIFARE Plus EV1, encrypted sector, ID-1 credentials (cards)</b>	Up to 3.8 cm (1.5 in.)			Up to 4.3 cm (1.7 in.)		
<b>Mounting</b>	Mullion			Single Gang, North America/Europe		
<b>Dimension (H x W x D)</b>	115.8 x 44.6 x 24.7 mm (4.56 x 1.75 x 0.97 in.)			115.8 x 71.5 x 24.7 mm (4.56 x 2.81 x 0.97 in.)		
<b>Supported credentials 125 kHz</b>	ioProx and HID			ioProx and HID		
<b>Supported credentials 13.56 MHz</b>	MIFARE Plus EV1 and ISO/IEC 14443A and 14443B					
<b>Supported credentials BLE (Bluetooth low energy) 2.4 GHz</b>	ioSmart mobile credentials and smart keys					
<b>Wiring terminal</b>	6 screwless poles					
<b>Tamper</b>	Optical					
<b>Wiegand communication formats</b>	Kantech SSF, Kantech XSF, 34-bit, 26-bit					
<b>Sounder</b>	Integrated					

**Table 12: Technical specifications**

<b>Specification</b>	<b>Mullion</b>	<b>Single Gang</b>
<b>AES 128-bit Security</b>	From the ioSmart card to the reader. From the reader to the access control unit over RS-485. From the smartphone application to the reader.	
<b>Output</b>	RS-485 or BLE panel-less: 1 supervised open-drain, up to 750 mA	
<b>Operating temperature</b>	-40°C to +70°C (-40°F to +158°F) -35°C to +66°C (-31°F to +151°F) for a UL listed product	
<b>Operating humidity</b>	0 to 95% non-condensing	
<b>LED indicator</b>	Multi-color bar: red, green, yellow, blue. Configurable.	
<b>Inputs in Wiegand</b>	LED and buzzer	
<b>Inputs in RS-485</b>	2 to 4, configurable	
<b>Inputs in BLE panel-less</b>	2 configurable	
<b>Input voltage</b>	8.5 VDC to 16 VDC (provided by UL 294 or UL 603 listed, power limited power source)	
<b>Housing</b>	Polycarbonate, smoked black	
<b>Flammability rating</b>	UL94 V-2	
<b>Firmware</b>	Fully upgradable using RS-485	
<b>Ingress protection rating</b>	IP55 (not verified by UL)	
<b>Communication</b>	RS-485 (AES 128-bit), Wiegand or BLE (AES 128-bit)	
<b>Cabling</b>	3 twisted pairs AWG 22 unshielded or CAT5, up to 150 m (500 ft)	
<b>Warranty</b>	Limited lifetime	
<b>Certifications</b>	FCC, IC, CE, UL 294, FIPS 197, RoHS, WEEE.  For RS-485, NIST CAVP validation number AES 3667, key length 128.	



# Mounting

Use this section to find out how to mount the ioSmart card reader in an appropriate location and how to set up the tamper detection.

There are two levels of tamper detection: the first is if an intruder pulls the front cover from the back panel, and the second is if an intruder pulls the entire panel from the wall.

ⓘ **Note:** To guarantee the correct setup, a trained installation technician must install the reader and follow the instructions in this guide.

## Mounting the ioSmart card reader

### About this task:

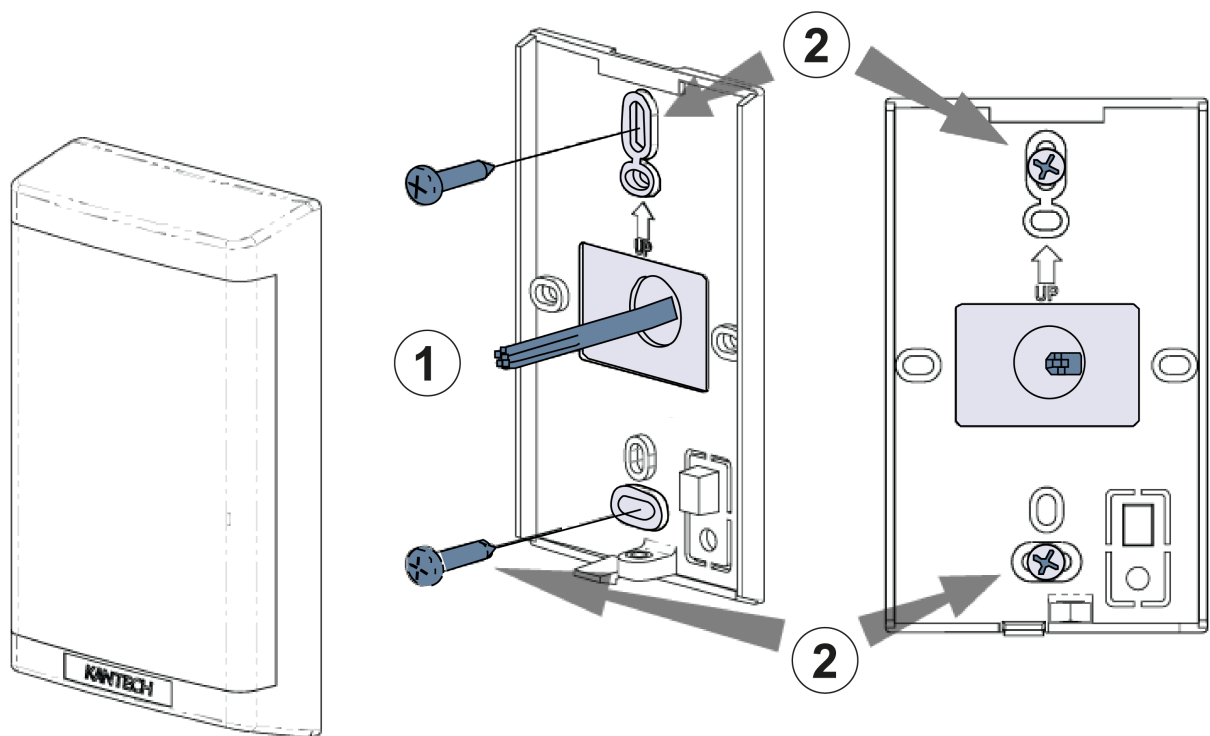
Mount the Single Gang reader on a wall or on an electrical box. Mount the Mullion reader on a doorframe.

To mount the reader, complete the following steps:

1. Pull the controller's wires from the wall and put them through the hole in the mounting plate.
2. Attach the mounting plate to a flat wall using two screws. The screws are not included.

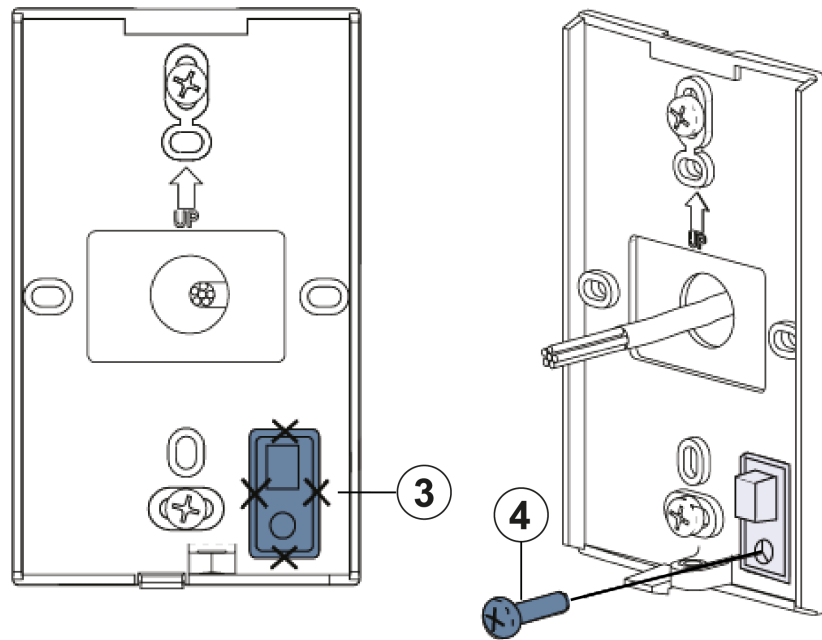
ⓘ **Note:** Do not over tighten the screws, especially if mounting on an uneven wall.

**Figure 5: Front cover, mounting plate wire, and screw holes**

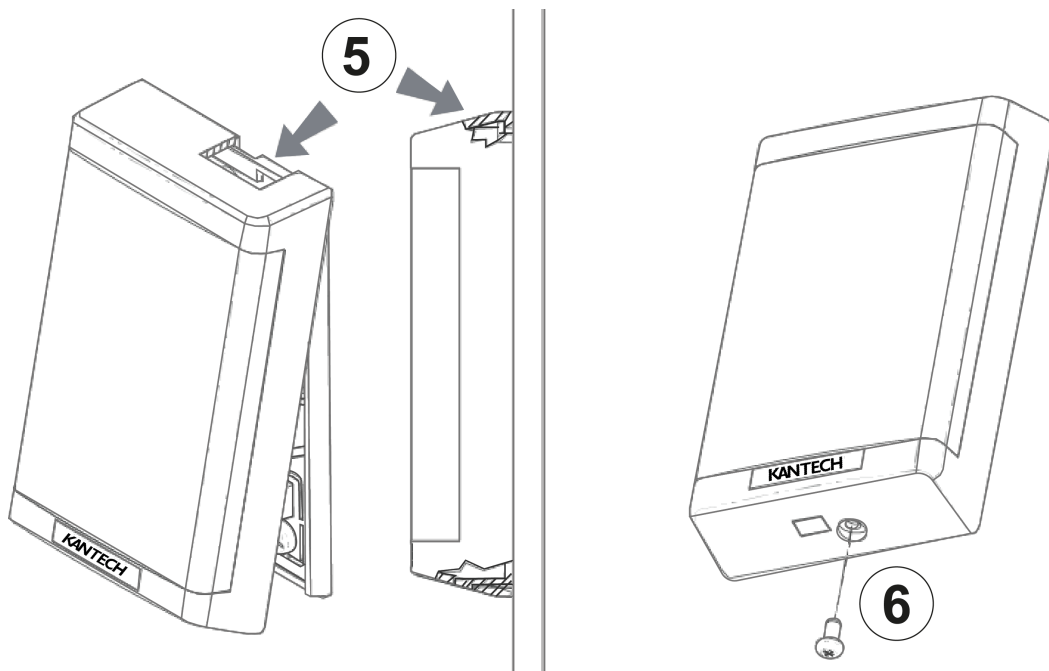


3. For a high level of tamper detection, cut the plastic tamper tab from the mounting plate.
4. Fasten the white reflector tab into the mounting plate hole using a screw. The screw is not included. Use a wall anchor if necessary.

**Figure 6: Mounting plate tamper tab and screw hole**



**Figure 7: Cover securing hook and screw**



5. After wiring the reader, insert the hook at the top of the cover into the mounting plate tab and press the bottom of the cover until the bottom hook snaps into place.
  - ⓘ **Note:** For instructions about how to wire the reader, see [Wiring](#).
6. Use the provided Phillips head screw, #6-32, to secure the bottom of the reader. The mounting position is successful if you hear a click when you attach the front cover to the mounting plate. If the mounting plate bends, consider positioning the reader in a new location.

## Wiring

To connect the reader to the controller, use 3 twisted pairs, 22 AWG (American wire gauge) or CAT5 cable. If you use the CAT5 cable, use two wires for GND and two wires for PWR. The recommended maximum distance between the reader and its power source is 150 m (500 ft).

### Wiring distance

The following table outlines the maximum cable distances between the reader and the controller. The results are based on using a KT-400 rev1 or a KT-1. To obtain results for a KT-400 with heat sinks, divide the distance by half.

**Table 13: Wiring distance**

Protocol	Maximum cable distance at 12 VDC	Wiring per line (1 door)	Equipment per wiring line (1 door)	Example of total equipment (based on KT-400)
RS-485	152 m (500 ft)	Home run	2 x reader 1 x door contacts 1 x T.REX-xxx	8 x reader 4 x door contacts 4 x T.REX-xxx
RS-485	152 m (500 ft)	Home run	1 x reader with keypad 1 x door contacts 1 x T.REX-xxx	4 x reader with keypad 4 x door contacts 4 x T.REX-xxx
Wiegand	152 m (500 ft)	Weigand, Reverse Wiegand*	2 x reader	8 x reader
Wiegand	76 m (250 ft)	Weigand, Reverse Wiegand*	1 x reader 1 x reader with keypad	4 x reader 4 x reader with keypad

① **Note:** \*Reverse Wiegand is available only with ioSmart SSF and ioProx XSF readers and cards on the KT-400 controller.

Figure 8: Example of a home run RS-485 connection

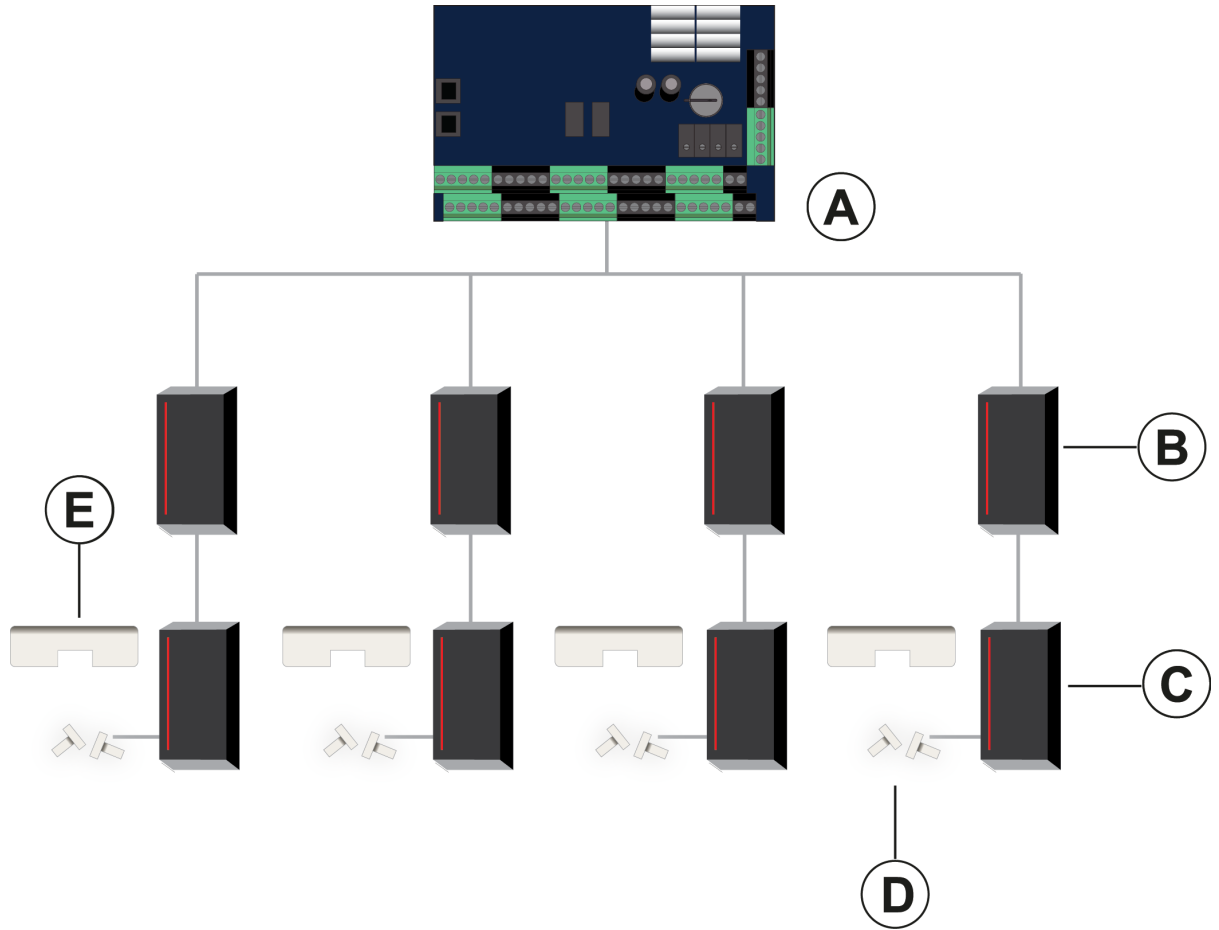


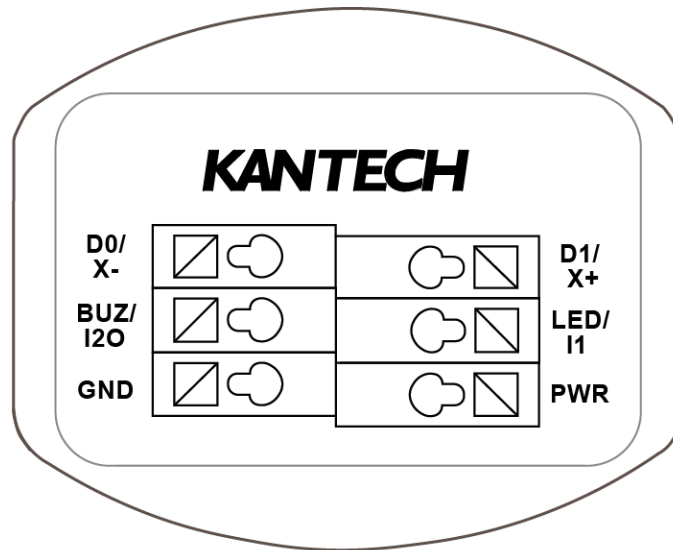
Table 14: Example of a home run RS-485 connection

Callout	Description
A	RS-485 (COM2) 500 ft for each line
B	IN readers
C	OUT readers
D	Door contacts
E	T.REX (request to exit) detectors

## Six pole screwless terminal block

The following diagram shows the ioSmart card reader six pole screwless terminal block.

**Figure 9: Six pole screwless terminal block**



The six pole screwless terminal block consists of the following input and output terminals.

**Table 15: Terminal block inputs and outputs**

Inputs and outputs	Description
D0 and D1 outputs	Wiegand mode outputs open collector 1K pull-up through 5 VDC with 22 $\Omega$ resistor at 50 mA maximum
LED and BUZ input terminals	2.2K pull-ups to +3.3 VDC
GND terminal	Ground
PWR terminal	8.5 VDC to 16 VDC

### RS-485 mode

In RS-485 mode, the LED and BUZ inputs are not required so you can configure them for other purposes. For example, configure the BUZ input as an open-collector supervised output and use it as a standard output or as a lock output. You could also use the input as a door contact input or as a request to exit (REX).

### Wiegand mode

In Wiegand mode, the Wiegand terminals share the RS-485 port terminals. The BUZ and LED inputs are standard BUZ and LED terminals and not inputs.

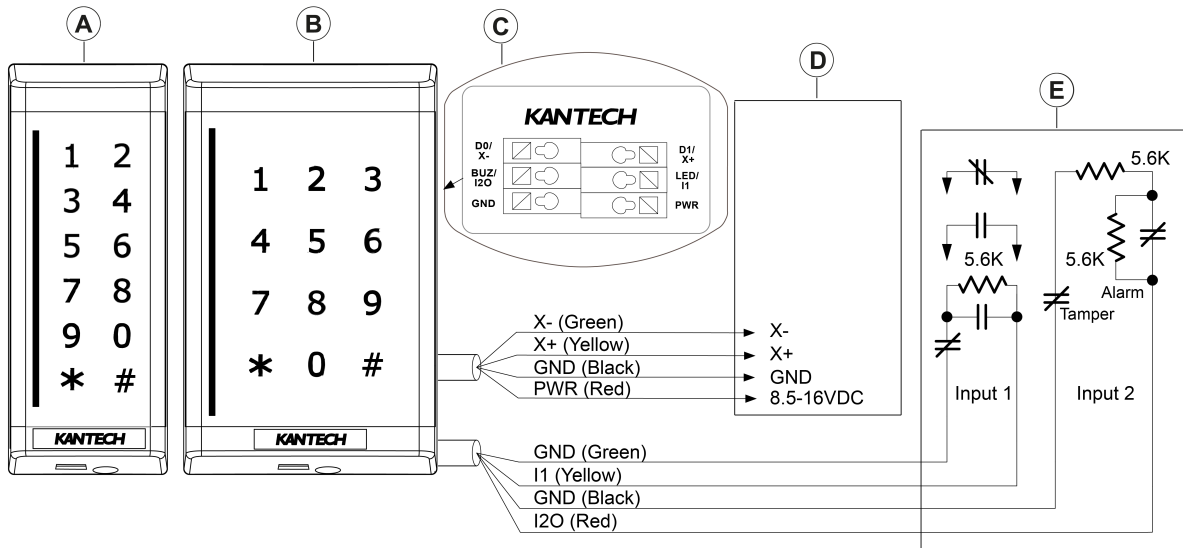
The Wiegand mode output formats are as follows:

- Kantech Smartcard Secure Format (SSF) is the default transmission
- Kantech eXtended Secure Format (XSF) transmission
- 34-bit transmission
- 26-bit transmission

## RS-485 wiring

The following wiring diagram shows how to connect the reader to the controller in RS-485 (COM2) mode.

**Figure 10: RS-485 wiring diagram**



ⓘ **Note:** Only use copper conductors.

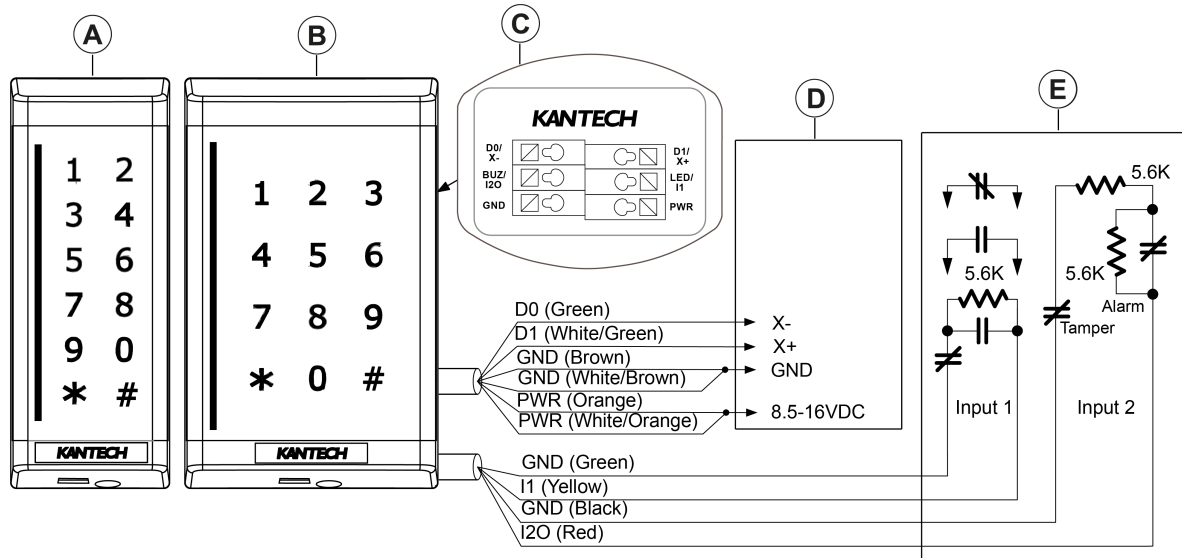
**Table 16: RS-485 wiring diagram**

Callout	Description
A	Mullion reader
B	Single Gang reader
C	Rear view of the reader
D	Host controller RS-485 (COM2) interface
E	Optional zone inputs 1 and 2. Individually programmable. Zone termination: NC, NO, NEOL, SEOL or DEOL termination.

## RS-485 CAT5 wiring

The following wiring diagram shows how to connect the reader to the controller in RS-485 mode using CAT5 cable.

**Figure 11: RS-485 wiring diagram using CAT5 cable**



① **Note:** With CAT5 cabling, use 2 wires for GND and 2 wires for PWR.

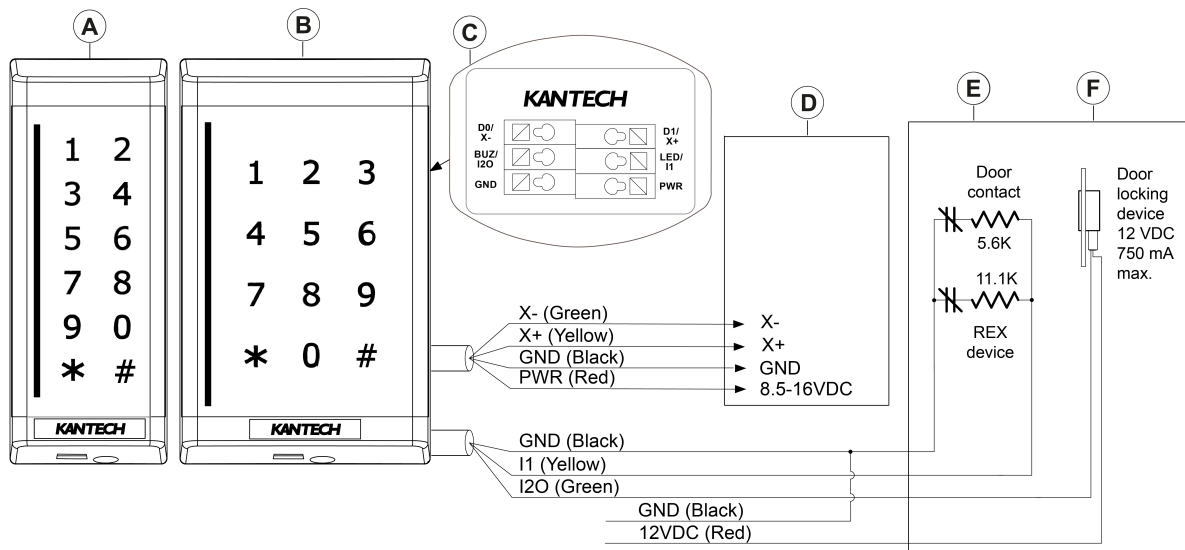
**Table 17: RS-485 wiring diagram using CAT5 cable**

Callout	Description
A	Mullion reader
B	Single Gang reader
C	Rear view of the reader
D	Host controller RS-485 (COM2) interface
E	Optional zone inputs 1 and 2. Individually programmable. Zone termination: NC, NO, NEOL, SEOL or DEOL termination.

## RS-485 lock output wiring

The following wiring diagram shows how to connect the BUZ input to a lock output in RS-485 mode.

**Figure 12: RS-485 lock output wiring diagram**



- ① **Note:** Only use copper conductors.
- ① **Note:** Use external power supply 12 VDC (750 mA minimum).

**Table 18: RS-485 lock output wiring**

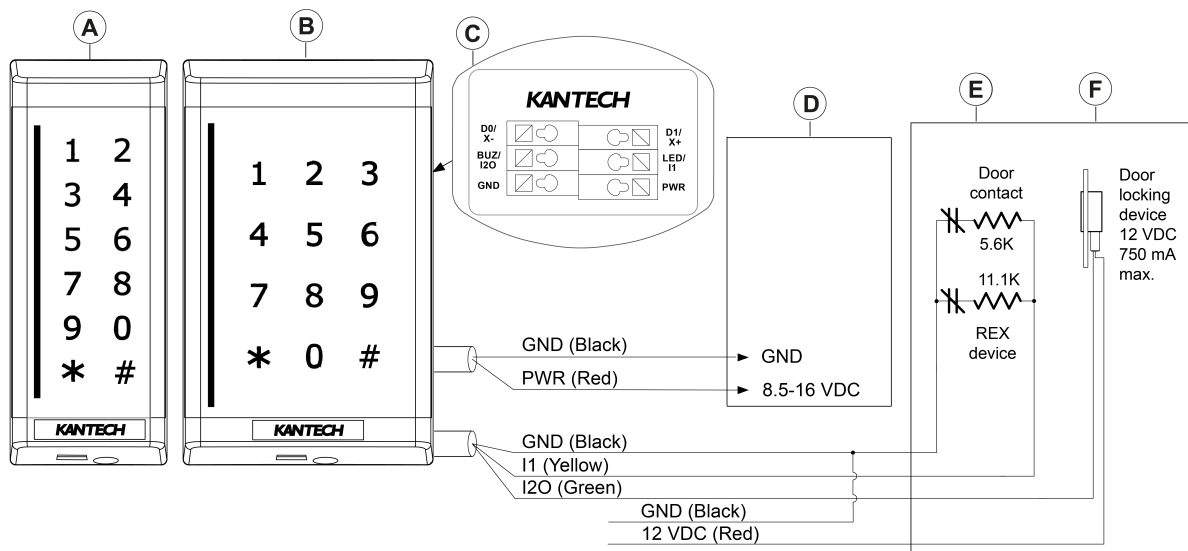
Callout	Description
A	Mullion reader
B	Single Gang reader
C	Rear view of the reader
D	Host controller RS-485 (COM2) interface
E	Input 1 programmed as dual input configuration
F	Input 2 programmed as output device configuration



## BLE lock output wiring for panel-less mode

The following wiring diagram shows how to connect the BUZ input to a lock output in BLE panel-less mode, with optional input contact.

**Figure 13: BLE lock output wiring diagram**



- ① **Note:** Only use copper conductors.
- ① **Note:** Use external power supply 12 VDC (750 mA minimum).

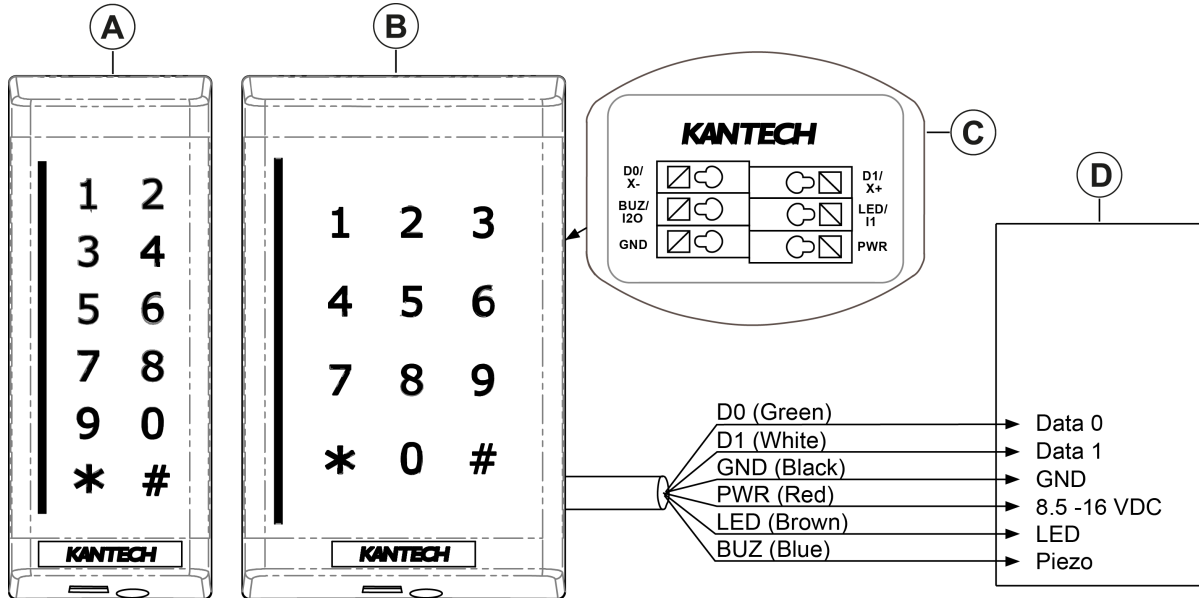
**Table 19: BLE lock output wiring**

Callout	Description
A	Mullion reader
B	Single Gang reader
C	Rear view of the reader
D	External 12 VDC power supply
E	Input 1 programmed as dual input configuration (door contact and REX)
F	Input 2 programmed as output device configuration

## Wiegand wiring

The Wiegand interface uses three wires, one common ground (GND) and two data transmissions (D0 and D1). The following wiring diagram shows how to connect the reader to the controller in Wiegand mode.

**Figure 14: Wiegand wiring diagram**



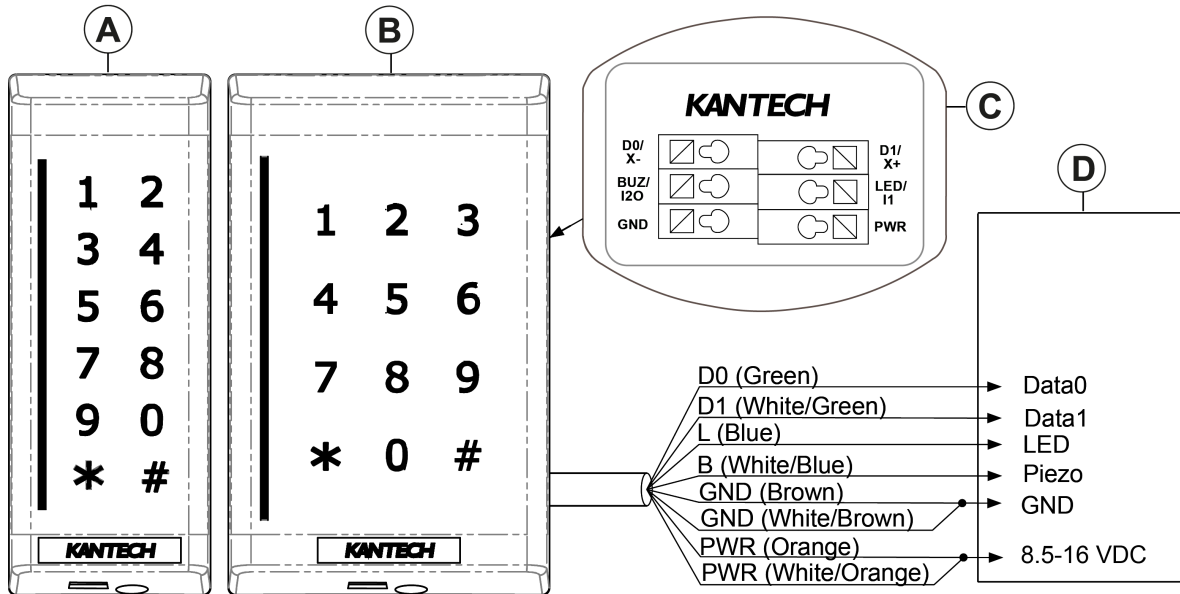
**Table 20: Wiegand wiring diagram**

Callout	Description
A	Mullion reader
B	Single Gang reader
C	Rear view of the reader
D	Host controller Wiegand interface

## Wiegand CAT5 wiring

The following wiring diagram shows how to connect the reader to the controller in Wiegand mode using the CAT5 cable.

**Figure 15: Wiegand wiring diagram using CAT5 cable**



① **Note:** With CAT5 cabling, use 2 wires for GND and 2 wires for PWR.

**Table 21: Wiegand wiring diagram using CAT5 cable**

Callout	Description
A	Mullion reader
B	Single Gang reader
C	Rear view of the reader
D	Host controller Wiegand interface

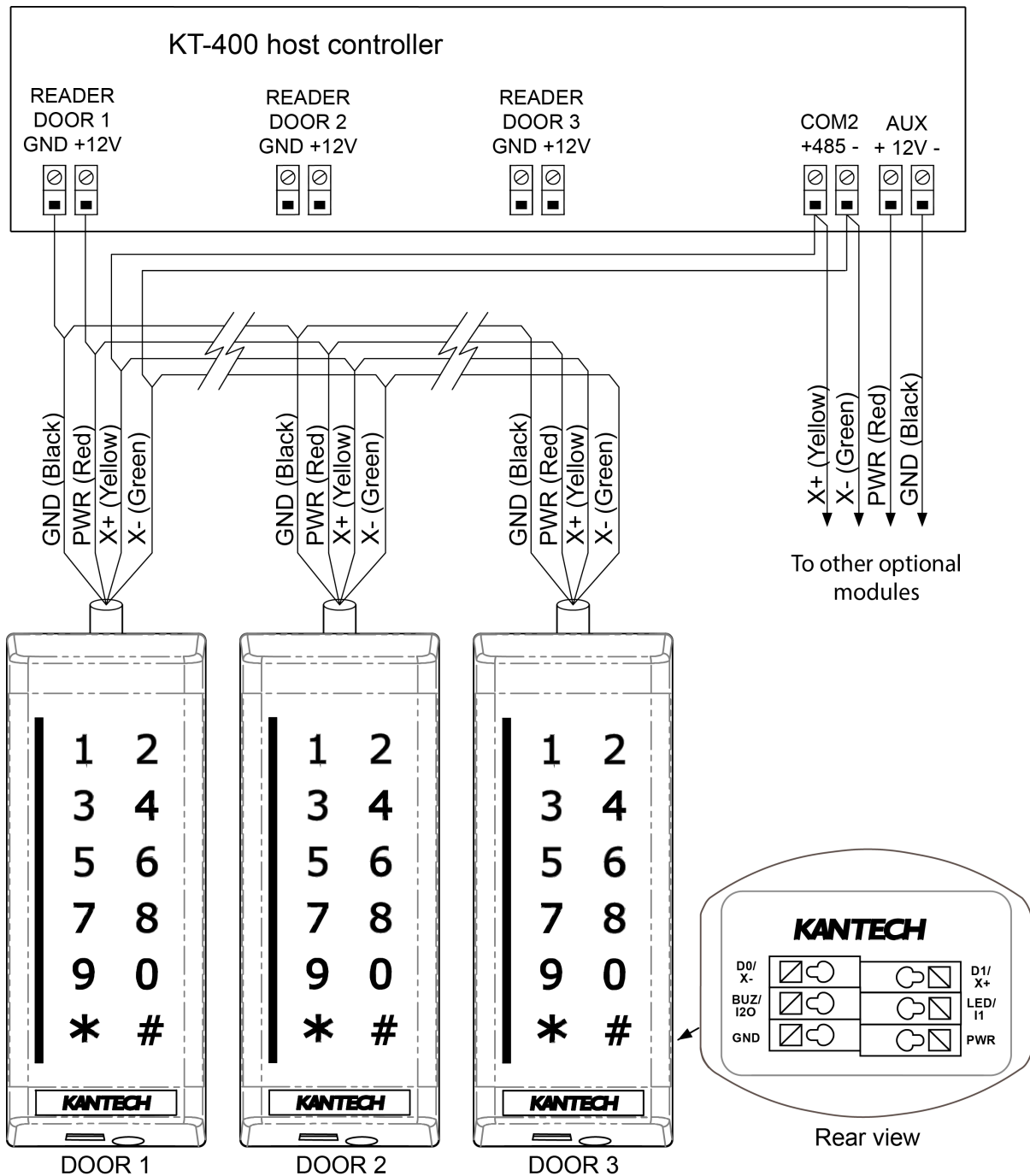
## Connecting multiple readers to a controller

Use this section to find out how to connect multiple readers to a controller using the daisy chain or the star wiring methods.

## Daisy chain wiring

The following diagram shows the daisy chain wiring method to connect multiple readers to a controller.

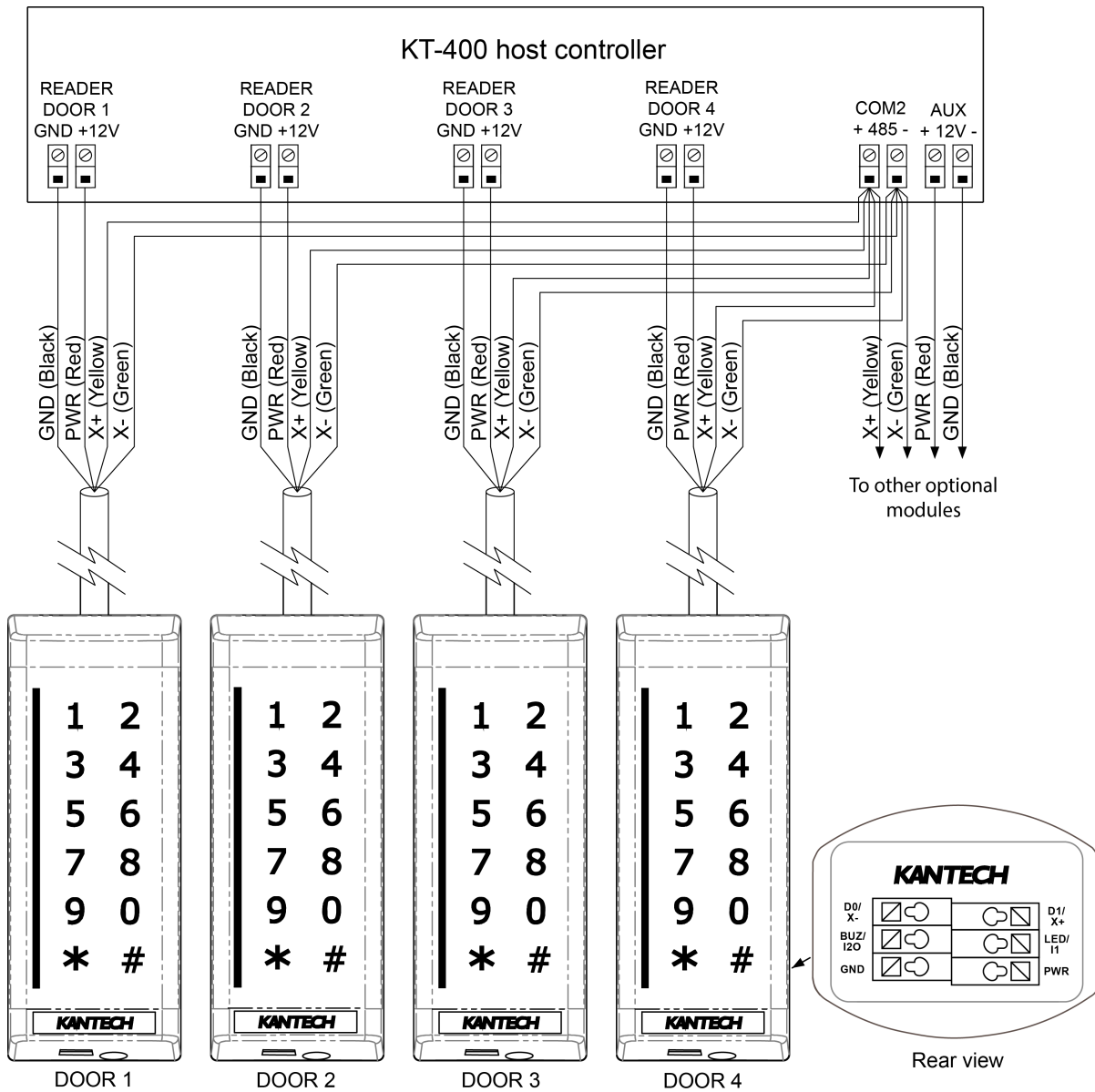
**Figure 16: Daisy chain wiring diagram**



## Star wiring

The following diagram shows the star wiring method to connect multiple readers to a controller.

**Figure 17: Star wiring diagram**



## Configuring the reader

This section describes how to configure the reader by short circuiting the wires on the terminal, and how to configure the reader using your Kantech smart card.

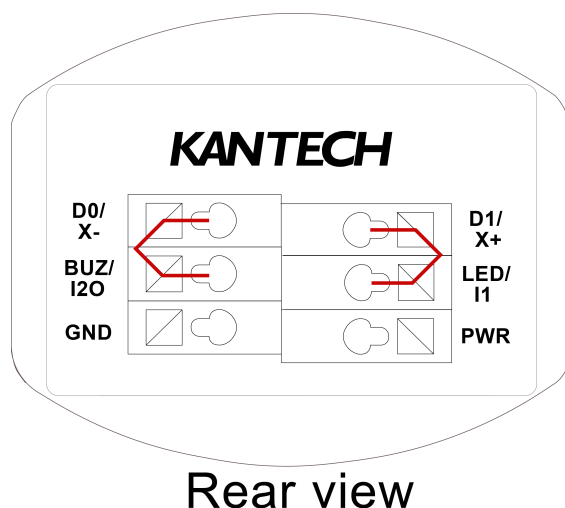
### Configuring the reader using the terminals

Use this section to configure the reader using the terminals.

- ① **Note:** If RS-485 communication is not detected when you turn on the reader, it transmits Wiegand format according to its configuration.

Factory default (SSF transmission format)

**Figure 18: Factory default terminal block shorting diagram**



SSF is the factory default configuration.

- **Important:** Forcing the reader to factory default deletes all custom settings from the reader and defaults BLE credential data. If you factory default a panel-less reader, you may need to contact technical support to reset it.

To return the reader to the factory default configuration, complete the following steps:

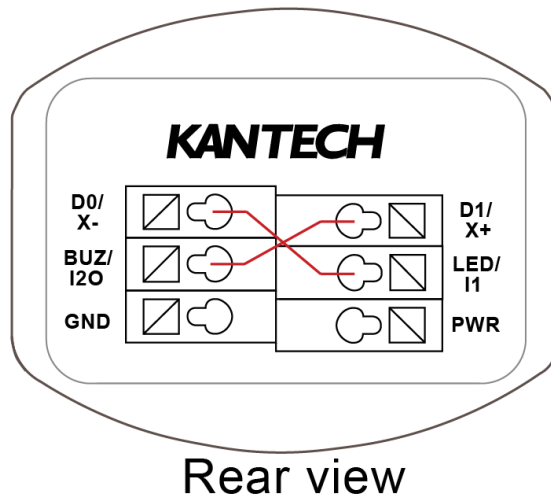
1. Short circuit together the D0 and BUZ terminals.
2. Short circuit together the D1 and LED terminals.
3. Apply power to the reader.

A simultaneous sequence of four beeps and flashes, four times, indicates a successful return to the SSF transmission format.

A sequence of rapid beeps and flashes for 4 seconds indicates that the device has not returned to the SSF transmission format.

Hard reset (SSF transmission format)

**Figure 19: Hard reset terminal block shorting diagram**



- **Important:** Forcing a hard reset deletes all custom settings from the reader except certain BLE credential data. Perform a hard reset instead of a factory default to keep the reader in panel-less mode. This option is available in firmware 1.06.19 and higher.

To return the reader to the default configuration, excluding certain BLE credential data, complete the following steps:

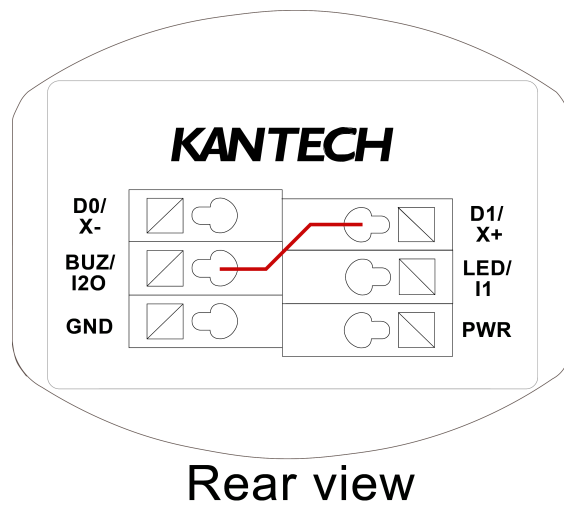
1. Short circuit together the D0 and BUZ terminals.
2. Short circuit together the D1 and BUZ terminals.
3. Apply power to the reader.

A simultaneous sequence of six beeps and flashes, four times, indicates a successful return to default configuration data.

A sequence of rapid beeps and flashes for 4 seconds indicates that the device has not returned to default configuration data.

## 34-bit transmission format

**Figure 20: 34-bit terminal block shorting diagram**



To configure Wiegand 34-bit format transmission, complete the following steps:

1. Short circuit together the D1 and BUZ terminals.
2. Apply power to the reader.

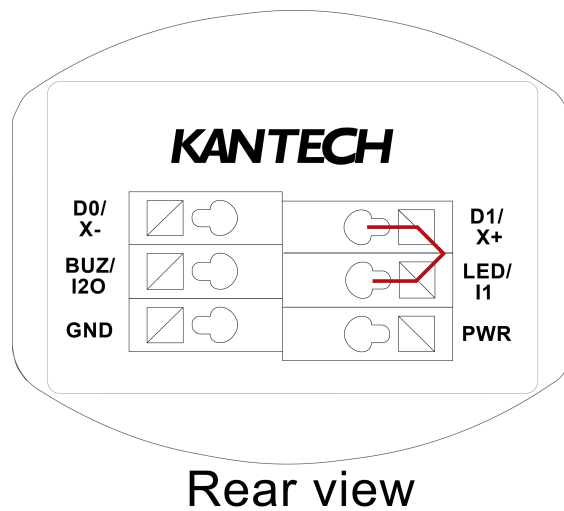
A simultaneous sequence of one beep and one flash, four times, indicates a successful configuration to the 34-bit transmission format.

A sequence of rapid beeps and flashes for 4 seconds indicates that the device is not configured to the 34-bit transmission format.



## 26-bit transmission format

**Figure 21: 26-bit terminal block shorting diagram**



To configure Wiegand 26-bit format transmission, complete the following steps:

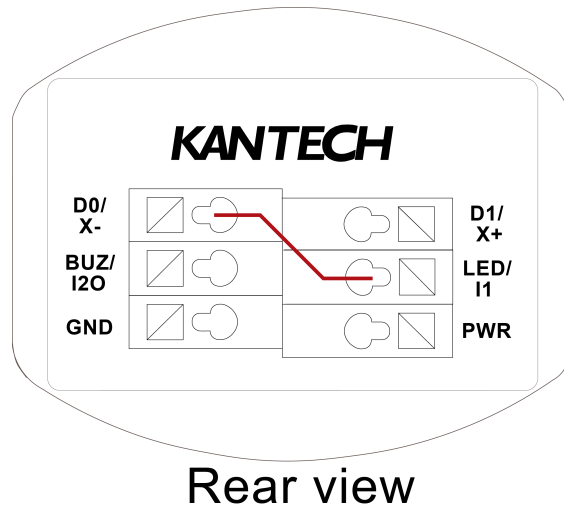
1. Short circuit together the D1 and LED terminals.
2. Apply power to the reader.

A simultaneous sequence of two beeps and flashes, four times, indicates a successful configuration to the 26-bit transmission format.

A sequence of rapid beeps and flashes for 4 seconds indicates that the device is not configured to the 26-bit transmission format.

## Sending the unique identifier (UID)

**Figure 22: UID terminal block shorting diagram**



If RS-485 communication is not detected when you turn on the reader, configure the reader to send the UID with supported 13.56 credentials.

To configure the reader to send the UID, complete the following steps:

1. Short circuit together the D0 and LED terminals.
2. Apply power to the reader.

A simultaneous sequence of five beeps and flashes, four times, indicates a successful configuration to the UID option.

A sequence of rapid beeps and flashes for 4 seconds indicates that the device is not configured to the UID format.

# Configuring the reader using a Kantech smartcard

## About this task:

As an alternative method to using the terminal block to short together two or more outputs, you can configure the reader using a Kantech smartcard.

You can configure up to eight different modes. The following steps describe how to configure the first two modes. For other modes, follow the same steps, but substitute the appropriate values from Table 22.

1. Reset the reader to factory default mode and present the card within the first 10 seconds. Maintain contact for at least 4 seconds. The reader beeps once and the LED flashes once.
2. **Optional:** To configure Wiegand 34-bit format transmission, present the card to the reader once. Five seconds later, the reader beeps once and the LED flashes once to confirm mode 1.
3. **Optional:** To configure Wiegand 26-bit format transmission, present the card to the reader twice. Five seconds after the last card presentation, the reader beeps twice and the LED flashes twice to confirm mode 2.
4. Present the card one final time to confirm the configuration. The reader acknowledges the new configuration with a 1-second continuous beep and LED activation.

The following table outlines the amount of card presentations that are required for each mode.

**Table 22: Card configuration modes**

Mode	Card presentations	Functions
1	Once	34-bit Wiegand transmission
2	Twice	26-bit Wiegand transmission
3	Three times	XSF transmission format
4	Four times	SSF transmission format
5	Five times	Send UID only
6	Six times	14443 Type B enabled
7	Seven times	HID Prox disabled
8*	Eight times	Enable Wiegand mode tamper reporting

- ① **Note:** \*Configuration mode 8 is supported for firmware 1.04 and higher. Wiegand mode tamper reporting is configured by default for firmware 1.03 and lower.
- ① **Note:** If you select a nonexistent mode, the error mode is triggered; this is a 4-second sequence of beeps and a flashing LED.

After the configuration is confirmed, the reader can accept another configuration within 10 seconds. If you want to use the card to reconfigure the reader, return the reader to factory default mode.

# Compliance specifications

The ioSmart card reader complies to the following standards approvals.

## FCC

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

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 provide reasonable protection against harmful interference in a residential installation. This equipment generates and uses radio frequency energy and if the user fails to install and use it in accordance with the instructions, it may cause harmful interference to radio communication. 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.

## CE compliance

- **EN60950**: Information technology equipment. Safety. General requirements.
- **EN55022, Class B**: Information technology equipment. Radio disturbance characteristics.
- **EN300 330-1**: Electromagnetic compatibility and radio spectrum matters (ERM); short range devices (SRD); radio equipment in the frequency range 9 kHz to 25 MHz and inductive loop systems in the frequency range 9 kHz to 30 MHz; part 1: technical characteristics and test methods.
- **EN300 330-2**: Electromagnetic compatibility and radio spectrum matters (ERM); short range devices (SRD); radio equipment in the frequency range 9 kHz to 25 MHz and inductive loop systems in the frequency range 9 kHz to 30 MHz; part 2: harmonized EN under article 3.2 of the R&TTE directive.
- **EN301 489-1**: Electromagnetic compatibility and radio spectrum matters (ERM); electromagnetic compatibility (EMC) standard for radio equipment and services; part 1: common technical requirements.
- **EN301 489-3**: Electromagnetic compatibility and radio spectrum matters (ERM); electromagnetic compatibility (EMC) standard for radio equipment and services; part 3: specific conditions for short-range devices (SRD) operating on frequencies between 9 kHz and 40 GHz.

## UL Standards compliance

- **UL-294** (UL standard for access control equipment, USA).
  - ① **Note:** Use only a UL 294 or UL 1076 listed power supply.

## NIST (National Institute of Standards and Technology)

An approved laboratory has validated the encryption algorithm used in this product. It is compliant with the NIST algorithm validation suite.

## RoHS (Restriction on Hazardous Substances)

This standard restricts the use of the following substances: lead, cadmium, mercury, chromium IV, polybrominated biphenyl (PBB), and polybrominated diphenyl ether (PBDE) in electrical and electronic equipment.

## WEEE (Waste Electrical and Electronic Equipment)

This regulation is used for waste electrical and electronic equipment, and addresses the disposal and the environmental handling of these products.

