tyco | Kantech

KT-2 Two-Door Controller Installation Guide

Johnson Controls

End User License Agreement (EULA)

➤ **Important:** READ THIS END-USER LICENSE AGREEMENT ("EULA") CAREFULLY BEFORE OPENING THE DISK PACKAGE, DOWNLOADING THE SOFTWARE OR INSTALLING, COPYING OR OTHERWISE USING THE SOFTWARE.

THIS EULA IS A LEGAL AGREEMENT BETWEEN YOU AND TYCO SAFETY PRODUCTS CANADA LTD ("TYCO"), AND GOVERNS YOUR USE OF THE SOFTWARE AND/OR FIRMWARE ACCOMPANYING THIS EULA WHICH SOFTWARE MAY BE INCLUDED IN AN ASSOCIATED PRODUCT AND INCLUDES COMPUTER SOFTWARE AND MAY INCLUDE MEDIA, PRINTED MATERIALS, AND "ON-LINE" OR ELECTRONIC DOCUMENTATION (COLLECTIVELY, THE "SOFTWARE"). BY BREAKING THE SEAL ON THIS PACKAGE, DOWNLOADING THE SOFTWARE OR INSTALLING, COPYING OR OTHERWISE USING THE SOFTWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS EULA. IF YOU DO NOT AGREE TO ALL OF THE TERMS AND CONDITIONS OF THIS EULA, DO NOT OPEN, DOWNLOAD, INSTALL, COPY OR OTHERWISE USE THE SOFTWARE.

1. SCOPE OF LICENSE. The Software may include computer code, program files and any associated media, hardware or software keys, printed material and electronic documentation. The Software may be provided to you pre-installed in a product or on a storage device (the media) as part of a computer system or other hardware or device ("System"). The Software is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. All title and intellectual property rights in and to the Software (including but not limited to any images, photographs, and text incorporated into the Software), the accompanying printed materials, and any copies of the Software, are owned by Tyco and/or its suppliers. The Software is licensed, not sold. All rights not expressly granted under this EULA are reserved by Tyco and its suppliers.

2. GRANT OF LICENSE. This EULA grants you the following rights on a non-exclusive basis:

    a. General. This EULA permits you to use the Software for which you have purchased this EULA. If the Software is protected by a software or hardware key or other device, the Software may be used on any computer on which the key is installed. If the key locks the Software to a particular System, the Software may only be used on that System.

    b. Locally Stored Components. The Software may include a software code component that may be stored and operated locally on one or more devices. Once you have paid the required license fees for these devices (as determined by Tyco in its sole discretion), you may install and/or use one copy of such component of the Software on each of the devices as licensed by Tyco. You may then use, access, display, run or otherwise interact with ("use") such component of the Software in connection with operating the device on which it is installed solely in the manner set forth in any accompanying documentation or, in the absence of such, solely in the manner contemplated by the nature of the Software.

    c. Remotely Stored Components. The Software may also include a software code component for operating one or more devices remotely. You may install and/or use one copy of such component of the Software on a remote storage device on an internal network with all of the devices and may operate such component with each device over the internal network solely in the manner set forth in any accompanying documentation or, in the absence of such, solely in the manner contemplated by the nature of the Software; provided however, you must still acquire the required number of licenses for each of the devices with which such component is to be operated.

    d. Embedded Software/Firmware. The Software may also include a software code component that is resident in a device as provided by Tyco for operating that device. You may use such component of the Software solely in connection with the use of that device, but may not retrieve, copy or otherwise transfer that software component to any other media or device without Tyco's express prior written authorization.

    e. Backup Copy. You may make a back-up copy of the Software (other than embedded software) solely for archival purposes, which copy may only be used to replace a component of the Software for which you have current valid license. Except as expressly provided in this EULA, you may not otherwise make copies of the Software, including the printed materials.

3. OTHER RIGHTS AND LIMITATIONS. Your use of the Software is subject to the following additional limitations. Failure to comply with any of these restrictions will result in automatic termination of this EULA and will make available to Tyco other legal remedies.

   a. Limitations on Reverse Engineering and Derivative Works. You may not reverse engineer, decompile, or disassemble the Software, and any attempt to do so shall immediately terminate this EULA - except and only to the extent that such activity may be expressly permitted, notwithstanding this limitation, either by applicable law or, in the case of open source software, the applicable open source license. You may not make any changes or modifications to any portion of the Software, or create any derivative works, without the written permission of an officer of Tyco (except as provided in Section 3(f) of this EULA with respect to "open source" software). You may not remove any proprietary notices, marks or labels from the Software. You shall institute reasonable measures to ensure compliance with the terms and conditions of this EULA by your personnel and agents.

   b. Copyright Notices. You must maintain all copyright notices on all copies of the Software.

   c. Transfer. You may only transfer your rights under this EULA (i) as part of a permanent sale or transfer of all of the devices for which the Software is licensed as applicable; (ii) if you transfer all of the Software (including all component parts, the media and printed materials, any upgrades and this EULA); (iii) if you do not retain any copies of any portion of the Software; (iv) if the recipient agrees to the terms of this EULA; and (v) if the Software is an upgrade, such transfer must also include all prior versions of the Software. You agree that failure to meet all of these conditions renders such transfer null and void.

   d. Termination. Without prejudice to any other rights, Tyco may terminate this EULA if you fail to comply with the terms and conditions herein. In such event, you must immediately destroy all copies of the Software and all of its component parts. To the extent the Software is embedded in hardware or firmware, you will provide prompt access to Tyco or its representative to remove or lock Software features or functionality as Tyco determines.

   e. Subsequent EULA. Tyco may also supersede this EULA with a subsequent EULA pursuant to providing you with any future component, release, upgrade or other modification or addition to the Software. Similarly, to the extent that the terms of this EULA conflict with any prior EULA or other agreement between you and Tyco regarding the Software, the terms of this EULA shall prevail.

   f. Incorporation of "Open Source" and other Third Party Software. Portions of the Software may be subject to certain third party license agreements governing the use, copying, modification, redistribution and warranty of those portions of the Software, including what is commonly known as "open source" software. Such portions of the Software are governed solely by the terms of such other license, and no warranty is provided under this License for open source software. By using the Software you are also agreeing to be bound to the terms of such third party licenses. If provided for in the applicable third party license, you may have a right to reverse engineer such software or receive source code for such software for use and distribution in any program that you create, so long as you in turn agree to be bound to the terms of the applicable third party license, and your programs are distributed under the terms of that license. If applicable, a copy of such source code may be obtained free of charge by contacting your Tyco representative.

   g. Trademarks. This EULA does not grant you any rights in connection with any trademarks or service marks of Tyco, its affiliates or its suppliers.

   h. Rental. You may not sublicense, rent, lease or lend the Software. You may not make it available to others or post it on a server or web site or otherwise distribute it.

   i. Software Keys. The hardware/software key, where applicable, is your proof of license to exercise the rights granted herein and must be retained by you. Lost or stolen keys will not be replaced.

   j. Demonstration and Evaluation Copies. A demonstration or evaluation copy of the Software is covered by this EULA; provided that the licenses contained herein shall expire at the end of the demonstration or evaluation period.

   k. Registration of Software. The Software may require registration with Tyco prior to use. If you do not register the Software, this EULA is automatically terminated and you may not use the Software.

   l. Additional Restrictions. The Software may be subject to additional restrictions and conditions on use as specified in the documentation accompanying such Software, which additional restrictions and conditions are hereby incorporated into and made a part of this EULA.

m. Upgrades and Updates. To the extent Tyco makes them available, Software upgrades and updates may only be used to replace all or part of the original Software that you are licensed to use. Software upgrades and updates do not increase the number of copies licensed to you. If the Software is an upgrade of a component of a package of Software programs that you licensed as a single product, the Software may be used and transferred only as part of that single product package and may not be separated for use on more than one computer or System. Software upgrades and updates downloaded free of charge via a Tyco authorized World Wide Web or FTP site may be used to upgrade multiple Systems provided that you are licensed to use the original Software on those Systems.

n. Tools and Utilities. Software distributed via a Tyco-authorized World Wide Web or FTP site (or similar Tyco-authorized distribution means) as a tool or utility may be copied and installed without limitation provided that the Software is not distributed or sold and the Software is only used for the intended purpose of the tool or utility and in conjunction with Tyco products. All other terms and conditions of this EULA continue to apply.

4. EXPORT RESTRICTIONS. You agree that you will not export, re-export or transfer any portion of the Software, or any direct product thereof (the foregoing collectively referred to as the "Restricted Components"), to IRAN, NORTH KOREA, SYRIA, CUBA and SUDAN, including any entities or persons in those countries, either directly or indirectly ("Tyco's Position"). You also agree that you will not export, re-export or transfer the Restricted Components to any other countries except in full compliance with all applicable governmental requirements, including but not limited to applicable economic sanctions and constraints administered by the U.S. Treasury Department and applicable export control measures administered by the U.S. Department of Commerce and U.S. Department of State, any other U.S. government agencies, and measures administered by the European Union or the government agencies of any other countries. Any violation by you of the applicable laws or regulations of the U.S. or any other government, or where you breach Tyco's Position notwithstanding whether or not this is contrary to any aforementioned applicable laws or regulations, will result in automatic termination of this EULA.

5. U.S. GOVERNMENT RESTRICTED RIGHTS. The Software is Commercial Computer Software provided with "restricted rights" under Federal Acquisition Regulations and agency supplements to them. Any use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFAR 255.227-7013 et. seq. or 252.211-7015, or subparagraphs (a) through (d) of the Commercial Computer Software Restricted Rights at FAR 52.227-19, as applicable, or similar clauses in the NASA FAR Supplement. Contractor/manufacturer is Sensormatic Electronics, LLC, 6 Technology Park Drive, Westford, MA 01886.

6. LIMITED WARRANTY.

a. Warranty. Tyco warrants that the recording medium on which the Software is recorded, hardware key, and the documentation provided with it, will be free of defects in materials and workmanship under normal use for a period of ninety (90) days from the date of delivery to the first user. Tyco further warrants that for the same period, the Software provided on the recording medium under this license will substantially perform as described in the user documentation provided with the product when used with specified hardware. THE FOREGOING EXPRESS WARRANTY REPLACES AND IS IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING BUT NOT LIMITED TO, ANY IMPLIED OR OTHER WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT OR NON-MISAPPROPRIATION OF INTELLECTUAL PROPERTY RIGHTS OF A THIRD PARTY, CUSTOM, TRADE, QUIET ENJOYMENT, ACCURACY OF INFORMATIONAL CONTENT, OR SYSTEM INTEGRATION. TYCO MAKES NO WARRANTY THAT ANY PORTION OF THE SOFTWARE WILL OPERATE ERROR-FREE, FREE OF ANY SECURITY DEFECTS OR IN AN UNINTERRUPTED MANNER. TYCO SHALL NOT BE RESPONSIBLE FOR PROBLEMS CAUSED BY CHANGES IN THE OPERATING CHARACTERISTICS OF THE DEVICE(S) UPON WHICH THE SOFTWARE IS OPERATING, OR FOR PROBLEMS IN THE INTERACTION OF THE SOFTWARE WITH NON-TYCO SOFTWARE OR HARDWARE PRODUCTS. TYCO 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. THE WARRANTY MADE BY TYCO MAY BE VOIDED BY ABUSE OR MISUSE. THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS UNDER MANDATORY LAW THAT VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

b. Exclusive Remedy. Tyco's entire liability and your exclusive remedy under the warranty set forth in this Section 6 will be, at Tyco's option, to (i) attempt to correct Software errors with efforts Tyco believes suitable to the problem, (ii) replace at no cost the recording medium, Software or documentation with functional equivalents as applicable, or (iii) refund a pro-rated portion of the license fee paid for such Software (less depreciation based on a five-year life expectancy) and terminate this EULA, provided, in each case, that Tyco is notified in writing of all warranty problems during the applicable warranty period. Any replacement item will be warranted for the remainder of the original warranty period. No remedy is provided for failure of the Software if such failure is the result of accident, abuse, alteration or misapplication with respect to the Software or any hardware on which it is loaded. Warranty service or assistance is provided at the original point of purchase.

7. LIMITATION OF LIABILITY & EXCLUSION OF DAMAGES.

a. LIMITATION OF LIABILITY. IN NO EVENT WILL TYCO'S AGGREGATE LIABILITY (INCLUDING, BUT NOT LIMITED TO, LIABILITY FOR NEGLIGENCE, STRICT LIABILITY, BREACH OF CONTRACT, MISREPRESENTATION AND OTHER CONTRACT OR TORT CLAIMS) ARISING FROM OR RELATED TO THIS EULA, OR THE USE OF THE SOFTWARE, EXCEED THE GREATER OF USD$5.00 OR THE AMOUNT OF FEES YOU PAID TO TYCO OR ITS RESELLER FOR THE SOFTWARE THAT GIVES RISE TO SUCH LIABILITY. BECAUSE AND TO THE EXTENT THAT SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSIONS OR LIMITATIONS OF LIABILITY ABOVE, THESE MAY NOT APPLY TO YOU.
b. EXCLUSION OF OTHER DAMAGES. UNDER NO CIRCUMSTANCES SHALL TYCO OR ANY OF ITS RESELLERS OR LICENSORS BE LIABLE FOR ANY OF THE FOLLOWING: (I) THIRD PARTY CLAIMS; (II) LOSS OR DAMAGE TO ANY SYSTEMS, RECORDS OR DATA, OR LIABILITIES RELATED TO A VIOLATION OF AN INDIVIDUAL'S PRIVACY RIGHTS; OR (III) INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, PUNITIVE, RELIANCE, OR COVER DAMAGES (INCLUDING LOST PROFITS AND LOST SAVINGS), IN EACH CASE EVEN IF TYCO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. YOU ARE SOLELY RESPONSIBLE AND LIABLE FOR VERIFYING THE SECURITY, ACCURACY AND ADEQUACY OF ANY OUTPUT FROM THE SOFTWARE, AND FOR ANY RELIANCE THEREON. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, OR THE LIMITATION ON HOW LONG AN IMPLIED WARRANTY LASTS, SO SOME OF THE ABOVE LIMITATIONS MAY APPLY TO YOU ONLY TO THE EXTENT PERMITTED BY THOSE LAWS.

8. GENERAL. If any provision of this EULA is found to be unlawful, void, or for any reason unenforceable, then that provision shall be severed from this EULA and shall not affect the validity and enforceability of the remaining provisions. You should retain proof of the license fee paid, including model number, serial number and date of payment, and present such proof of payment when seeking service or assistance covered by the warranty set forth in this EULA. This EULA is governed by the laws of the State of New York, without regards to its conflicts of law principles. The parties hereby irrevocably agree that they submit themselves to the personal jurisdiction of the state and federal courts of New York for purposes of resolving any and all disputes arising under or related to these terms and conditions. The parties specifically exclude the application of the provisions of the United Nations Convention on Contracts for the International Sale of Goods.

Copyright

Safety information

➤ **Important:** Never install the equipment during an electrical storm.

➤ **Important:** The KT-2-EU-MET is to be protected by a branch overcurrent protective device not exceeding 7A as part of the installation.

⚠ **WARNING:** Do not look directly at LEDs with unshielded eyes, or damage to retina may occur.

The KT-2 Two-Door Controller shall be installed and used within an environment that provides a maximum pollution degree of 2, and over voltages category II NON HAZARDOUS LOCATIONS, INDOOR only. The equipment is FIXED and PERMANENTLY CONNECTED. The

KT-2 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). The equipment is installed in a metallic cabinet that meets the applicable requirements for a FIRE ENCLOSURE.

ⓘ **Note:** When installed on the North American Market, powered via the UL, cUL Listed 40VA Transformer, the KT-2 shall be connected to the mains by a LICENSED ELECTRICIAN in accordance with the applicable rules of the National Electrical Code or Canadian Electrical Code regarding this type of connection.

1. The connection to the mains supply must be made as per the local authorities' rules and regulations. An appropriate disconnect device must be provided as part of the building installation. Where it is not possible to rely on the identification of the NEUTRAL in the AC MAINS SUPPLY, the disconnecting device must disconnect both poles simultaneously (LINE and NEUTRAL).

2. AVOID setting up the equipment near heaters, air conditioners, ventilators, and/or refrigerators; DO NOT select a place that exposes your controller to direct sunlight, excessive heat, moisture, vapors, chemicals or dust.

3. If during the installation a knockout on the cabinet is removed, it is the installer's responsibility to ensure that the same degree of protection for the cabinet is provided by the use of bushings, fittings, adequate sealant, etc.

4. The metallic cabinet must be secured to the building structure before operation. Use four (4) stainless steel tapping screws #8, 32 mm (1.25 in.) to mount the cabinet.

5. The ground connection must be as shown within the included diagram, or equivalent.

6. Internal wiring must be routed in a manner that prevents:

    - Excessive strain on wire and on terminal connections
    - Loosening of terminal; connections
    - Damage of conductor insulation
    - Reducing the clearance between SELV (Safety Extra Low Voltage) circuits and NON-POWER Limited Circuits (Battery wires)
    - Route the battery wires away from the rest of the SELV circuits.

7. It is the end-user and/or installer's responsibility to ensure that the disposal of the used batteries is made according to the waste recovery and recycling regulations applicable to the intended market.

8. There are no serviceable parts within the equipment; For any issues regarding the equipment please contact your installer.

9. Before leaving the premises, if Ethernet communication lines are being used, they must first be connected to an approved (acceptable to local authorities) type Network Interface Device (NID), (UL installations, UL 60950 or 62368 listed NID, for ULC installations CAN/CSA C22.2, No. 60950-1 or 62368-1 Certified NID). All wiring shall be performed according to the local electrical codes.

10. DISCONNECT POWER BEFORE SERVICING.

11. DO NOT OPEN the enclosure! Hazardous voltages may become accessible!

Replacing or discarding batteries

➤ **Important:** Only qualified service technicians should perform maintenance recommendations.

The KT-2 includes a lithium CR2032 primary battery. To avoid risk of explosion, the battery must be replaced by a qualified service technician only. Do not crush, puncture, open, disassemble or otherwise mechanically interfere with the battery. Do not try to recharge the battery. If you need to dispose of the PCB and/or the lithium battery, wrap them in non-conductive tape. Check with your local authorities for battery disposal regulations.

⚠ **WARNING:** Do not store the batteries in such a way that they come into contact with each other or with any piece of metal. Explosion or fire may occur. Should fire occur, use only dry chemical fire extinguishers. Do not use water to put out the fire. Do not heat the batteries. Do not dispose of the batteries or PCB in a fire. Do not disassemble the batteries. Do not apply pressure to deform the batteries. Ensure that the above precautions are strictly observed by related departments, including, but not limited to, production, sales and outside contractors.

⚠️ **WARNING:** There is a risk of fire, explosion, and burns. Do not recharge, disassemble, heat above 100°C or incinerate.

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.

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.
- For video technical support, email video-support@jci.com.
- For technical training inquiries, email 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.
- For technical training inquiries, email emea.training@tycoint.com.
- For all licensing inquiries, email 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.
- For technical training inquiries, email apac.training@jci.com.
- For all licensing inquiries, email sp-licensing-support@jci.com.

Table 4: Asia Pacific telephone numbers

Area	Call type	Opening times: 09:00 to 18:00 (CST China Standard Time) and 09:00 to 19:00 (India Time)
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

Introduction

The KT-2 Two-Door Controller offers a simple access control and point monitoring solution. The following figure shows the KT-2 installation with a back plate.

Figure 1: KT-2-BP

Figure 2: Example of a KT-2 setup with a T.REX
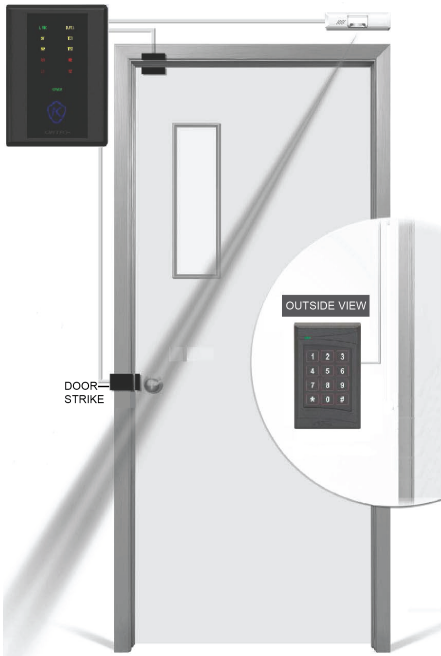
Features

The KT-2 controller includes the following features.

Operating modes

Use the KT-2 controller in one of the following modes:

- Stand-alone mode: use as a stand-alone access controller with an Ethernet configuration for direct configuration.

  ⓘ **Note:** Wi-Fi communication is not available in stand-alone mode.

- EntraPass mode: connect to EntraPass access control management software to add additional doors and controllers using an Ethernet, RS-485, or Wi-Fi connection.

For information about how to configure each mode, see Configuration.

Compatibility with EntraPass

The KT-2 is compatible with the following EntraPass editions, 8.40 and later:

- EntraPass Special Edition
- EntraPass Corporate Edition
- EntraPass Global Edition with a multi-site gateway, a global gateway, or a KT-NCC Network Communications Controller

Configuring IP communication

To configure the controller's IP settings, use one of the following options:

- KT Registration web page
- KT-Finder

For more information, see Configuration.

Communication ports

The following table lists the KT-2 controller's communication ports.

Table 5: Communication ports

Port	Quantity	Use
Wired Ethernet 10/100 Base-T (ETHERNET), with or without PoE/PoE+	1	For the Ethernet connection
RS-232	1	To communicate and integrate with third party systems ⓘ **Note:** For UL listed installations, this is only for supplementary use.
RS-485 (COM1)	1	To communicate with EntraPass or a loop of controllers
RS-485 (COM2)	1	To communicate with ioSmart card readers or expansion modules such as the KT-MOD-IO16 Input/Output Module

IP connectivity: WiFi or wired, and optional PoE or PoE+

When you use the KT-2 with EntraPass Special Edition, Global Edition, or Corporate Edition software, it can gather its configuration through an IP connection over a local area network (LAN) or over a wide area network (WAN).

ⓘ **Note:** Do not use a WAN configuration with EntraPass Global Edition.

When you use the KT-2 with any EntraPass edition, the first controller becomes a master controller and can poll up to 31 controllers. The KT-2 asynchronously polls the KT-1, KT-300, or KT-400 controllers, and communicates with the EntraPass gateway only when it is necessary. This reduces the amount of bandwidth that the security system requires to operate on the network.

PoE provides up to 13 W power to the unit. PoE+ provides up to 25.5 W power to the unit. For more information, see Powering the KT-2.

ⓘ **Note:** Do not use the Ethernet port when the controller is connected to Wi-Fi. If you plug in an Ethernet cable, PoE or PoE+, you may experience connectivity issues.

AES encryption 128-bit

When you use the KT-2 over Ethernet, the controller uses 128-bit AES encryption to communicate with the gateway.

AES encryption: NIST CAVP validation number AES 3092, key length 128.

Inputs

Use the KT-2 controller's eight onboard inputs for any of the following functions:

- Door contact
- REX: Request to Exit detector such as T.REX
- Second REX
- Interlock
- External alarm system status: armed/disarmed
- External alarm system alarm: alarm/secure
- External alarm system zones
- Input actions: relays # to activate on each input in alarm, tamper, or trouble events.
- Zone shunt: shunt a single zone or group of zones, permanently or temporarily, to a secure state on the same controller, or on any other controller if it is operating in NCC mode. For a description of the different shunt methods, see the following list:

  - Manual shunt: the operator can manually shunt a zone into a secure state.
  - Disarmed door shunt: when the alarm system is dayside (disarmed), some zones may be shunted to a secure state.

- Entry/exit delay shunt: when a user disarms or arms the alarm system and an entry or exit delay prevails, some zones may be shunted to a secure state.
- Zone shunt by another zone: when a zone in alarm is programmed to shunt another zone or group of zones.
- Zone shunt on unlock: the zone freezes temporarily to its actual state (alarm or secured) after an access is granted. This is also called no report. See access application.

- Arming/disarming request: the zone is defined as an arming request input.
- Postpone arming request: the zone is defined as a postpone arming request input.

Tamper input

The tamper input is a non-programmable, fixed-function input that identifies cover tampering. You can set up a tamper schedule so that the tamper is supervised only at certain times. You can set up a tamper action to define the relays # to activate the tamper switch in an alarm event.

Lock outputs

The KT-2 has two onboard lock outputs. You can configure any onboard or expansion module to perform the locking function. Lock outputs are supervised for open circuit or short to ground fault detection.

Relay outputs

The KT-2 has two onboard relays. The two relays on the KT-2 board and any relays on optional extension boards that attach through RS-485 are defined as local relay outputs.

ioSmart card readers

The KT-2 is compatible with ioSmart card readers, which provide security by using end-to-end encryption between the ID badge credentials and the EntraPass software.

Reader outputs

The KT-2 has two LED and two buzzer open-collector, switch-to-ground reader outputs. Use these outputs for readers 1 and 2 to give the user visual and audible feedback on access events.

Reader interfaces

The KT-2 has two onboard 12 VDC reader interfaces. You can configure each of the reader interfaces to operate in the following ways:

- Wiegand data over Wiegand
- ABA data over Wiegand
- ABA data over ABA clock and data

ⓘ **Note:** For UL listed installations, use only Wiegand or Kantech XSF/SSF, or Kantech ioSmart smart card readers.

Integration interface

The KT-2 supports alarm panel interfacing when you make the appropriate connections between zone inputs, relay outputs, and the alarm system panel.

Detecting ports automatically

The KT-2 automatically detects the site communication speed set by EntraPass.
To detect the communication port automatically, in EntraPass, select WiFi, wired Ethernet, or RS-485 (COM1).

Downloading firmware

To download firmware updates, log on to http://www.kantech.com. Click the **Support** tab, click **Software Downloads**, and download the appropriate firmware version.

Trouble and reporting

The KT-2 monitors its power continuously and reports low and critical power issues. The controller monitors the power outputs and electronically protects them against short-circuits and surges. The controller monitors locking devices to detect open circuit or short to ground faults.

Technical specifications

The following table lists the technical specifications of the KT-2 controller.
Table 6: Technical specifications

Type	Description
DC power input	11.3 VDC to 14.0 VDC, 1.5 A
PoE	13 W in, 0.9 A/13 VDC out
PoE+	25.5 W in, 1.2 A/13 VDC out
Operating temperatures	For UL listed installations: 0°C to 49°C (32°F to 120°F) indoor use only. For European compliant installations: -10°C to 55°C (14°F to 131°F) Environmental Class II.
Humidity level	85% relative humidity non-condensing.
Cabinet dimensions	11.3 in. x 11.7 in. x 3.1 in. (28.702 cm x 29.718 cm x 7.874 cm)
Weight of the controller	4.75 lb (2.16 kg)
Reader types	Wiegand, proximity, ABA Clock and Data, bar code, magnetic, integrated keypad, smartcard and others.
Reader power output	12 VDC 500 mA maximum, protected and supervised.
Monitored points (zone inputs)	8 monitored points (Z1 to Z8), NO/NC without EOL (DRY), single EOL, double EOL and 1 fixed-function tamper input.
Points maximum wiring	AWG #22-600 m (2000 ft) For the relevant reader's maximum wiring specifications, refer to the reader's installation manual.
Door strike power supervised	750 mA for one output or 1.0 A total (in PoE 13 W, 375 mA each or 750 mA total). Lock outputs are supervised for open circuit or short to ground fault detection.
Auxiliary reader outputs	LEDs and buzzer (BUZ), 25 mA maximum each, open collector outputs
Relay controlled outputs	2 onboard Form C relays, 30 VDC, 3 Amps each, 0.6 power factor
Communication ports	1 x RS-232 with RJ-12, 2 x RS-485, 1 x Ethernet 10/100 Base-T with RJ-45, WiFi. ⓘ **Note:** Use the RS-232 for integrations, with a maximum cable length of 3 m (10 ft).
Wi-Fi specifications	Station mode wireless 802.11 b/g/n (2.4 GHz only). Access point wireless 802.11 n (2.4 GHz only).
Auxiliary power	1.0 A maximum. This is shared with door strike power.

Table 6: Technical specifications

Type	Description
Communication speed	1200 to 115200 Bauds (automatic detection) over RS-485. 10/100 Mb/s BaseT over Ethernet. 1 Mb/s over Wi-Fi.
Flash memory	256 MB NAND flash for application, storage and standalone event buffer holding 60,000 events.
Network type	IEEE 802.00 b/g/n (Wireless LAN)
Frequency/ Max. E.I.R.P.	2412-2471 MHz / ETSI 100 mW, FCC 1 W
RF channels	US/Canada: 1-11 Others: 1-13 Antenna gain at 2.4 GHz: 2.5 dBi (maximum)
RAM memory	128 MB DDR2 for application loading and running.
Network autonomy	Distributed data and processing.
Certifications/ Listing	United States: Transmission complies with FCC Part 15.247 Regulations for Low Power Unlicensed Transmitters. Transmitter FCC identification: YOPGS2101M FCC compliant to CFR 47, Part 15, Subpart B, Class A; KT-2-M: UL 294 and UL 1076 listed equipment. Canada: Industry Canada IC: 9154-GS2101M. ICES-003 (A)/NMB-003 (A)
AES Encryption	NIST CAVP validation number AES 3092, key length 128.

ⓘ **Note:** The KT-2 restarts automatically after total power loss and keeps its programming after an unlimited time of power interruption. The design uses flash memory to save access rules. For PoE-powered KT-2 and Class B installations, use a ferrite on the Ethernet cable.

ⓘ **Note:** The KT-2 Wi-Fi performance level depends on the type of router that you use and on the installation environment. The KT-2 Wi-Fi access point mode is used for configuration: it requires a mobile, tablet, or laptop that has Wi-Fi capability and a web browser.

ⓘ **Note:** Total power for readers, door strikes, outputs, and auxiliary power must not exceed 1.5A at 14VDC.

Front cover LEDs

The LEDs on the front cover of the KT-2 indicate the controller's network activity, power status, and outputs. The following table describes the status that each LED indicates when it turns on.

Table 7: LED status indicators

Name	LED color	Status
LINK	Green	The LED is steady on if there is an Ethernet network connection. The LED is off if is no Ethernet network connection or the cable is disconnected.
DATA	Yellow	The LED is steady on if there is network activity.
RX1	Yellow	The LED is steady on if the RS-485 serial port is receiving activity from the gateway.
TX1	Yellow	The LED is steady on if the RS-485 serial port is transmitting activity to the gateway.
RX2	Yellow	The LED is steady on if the RS-485 serial port is receiving activity from the backplane, ioSmart readers, or expansion modules.
TX2	Yellow	The LED is steady on if the RS-485 serial port is transmitting activity to the backplane, ioSmart readers, or expansion modules.
R1	Red	The LED is steady on if Relay 1 is activated.
R2	Red	The LED is steady on if Relay 2 is activated.

Table 7: LED status indicators

Name	LED color	Status
L1	Red	The LED is steady on if Lock output 1 is activated.
L2	Red	The LED is steady on if Lock output 2 is activated.
POWER	Green or yellow	The LED is steady on if the DC level is sufficient for all DC terminals, such as the 12 V AUX.
Kantech shield (One Button)	Blue	The LED is steady on if the controller is communicating with EntraPass or the controller's IP mode is activated. For more information, see Kantech shield LED.
RS-232 Rx	Yellow	The LED is steady on if the RS-232 serial port is receiving activity from an integrated device.
RS-232 Tx	Yellow	The LED is steady on if the RS-232 serial port is transmitting activity to an integrated device.
Wi-Fi Link	Green	The LED is steady on when the router is associated with the KT-2.
KT-2 backplane vital	Red	The LED is off when everything is okay. The LED is steady on when there is a communication problem between the backplane and the top board. The LED flashes quickly when the MCU firmware is updating.
COM2 Rx backplane	Yellow	The LED is steady on if the COM2 backplane is receiving activity from the main boards, or the main boards are receiving activity from ioSmart card readers or expansion modules over COM2.
COM2 Tx backplane	Yellow	The LED is on if the COM2 backplane is transmitting activity to the main boards.

Kantech shield LED

The LED on the Kantech shield shows the controller's communication status and other conditions. Use this information when you connect the controller to the EntraPass system. The following tables describes all possible conditions.

Table 8: Kantech shield LED patterns
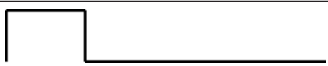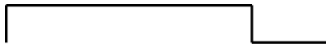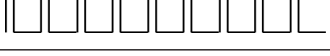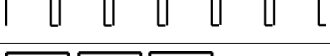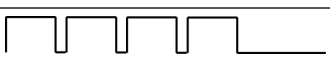
Condition	LED color	Flashing pattern	
Starting up	Blue	Steady	
Corporate/ Multi-site Gateway	Blue	3 short flashes	
Global Gateway	Blue	1 short flash	
Restarting	Blue	10 flashes every second at 50% duty cycle	
Card read or swipe	Blue	One 0.5 second flash, then it resumes previous flash	
Enrolling	White	1 long flash every 2 seconds	

KT-2 Two-Door Controller Installation Guide

Table 8: Kantech shield LED patterns

Condition	LED color	Flashing pattern	
Acknowledge enrollment	Pink	One 2.5 second flash	
Updating firmware	Green	5 flashes every second at 50% duty cycle	
Receiving broadcast	Green	One 2.5 second flash	
Fail soft	Yellow	Continuous short flashes	
Factory default DHCP	Yellow	Continuous long flashes	
Forced default STATIC	Yellow	3 long flashes	
Hard reset	Red	4 short flashes	
Unable to resolve DNS	Red	2 long flashes	
DHCP server failed	Red	4 long flashes	

ⓘ **Note:** To reset or change the KT-2 controller's communication mode, see Resetting the KT-2.

Wiring diagrams

The KT-2 monitors its power continuously, and reports low and critical power issues. Power outputs are monitored and are protected electronically against short-circuits and surges. Locking devices are monitored to detect open circuit or short to ground faults.

Figure 3: KT-2 inputs and outputs (North American model)

Table 9: KT-2 inputs and outputs (North American model)

Callout	Description
A	2.4GHz Antenna
B	RF cable with U.FL connector
C	Door locking device: 12 VDC 750 mA maximum
D	Connect a 1K Ohms resistor between LK- and +12 V if you are not using a locking device.
E	Kantech smart card reader with an integrated keypad in Wiegand mode.
F	Optional RS-485 expansion module
G	Connect the RS-485 main network to other KT-2 or KT-1 controllers or to the gateway using a USB-485 interface.
H	Tighten the nut to break the paint and ensure a secure connection to the cabinet.
I	Tamper switch, 1/4 A 30 VDC, UL Recognized
J	Battery 12 VDC/7 AH

Table 9: KT-2 inputs and outputs (North American model)

Callout	Description
K	Connect the ACT (AC trouble) output from the KT-PS4085 to one input on the KT-2 to transmit AC loss events to the monitoring console.
L	Class 2 power limited adapters, model PTC1640UG
M	Transformer 16 VAC/40 VA
N	Optional power supply: KT-PS4085 12 VDC/1.5 A ⓘ **Note:** To power the KT-2, use a PoE or PoE+ power source connected to a RJ45 socket, or a UL listed external power supply connected to a terminal block +/- rated 12 VDC/1.5 A.
O	RJ45 Ethernet network. Optional PoE or PoE+ powered.
P	Door 1 request to exit device
Q	Door 1 contact
R	Relay 1: 30 VDC, 3 Amps, Form C
S	RJ12 RS232C port: integration

Power supply (North American model)

The mains input ratings are 120 VAC/60 Hz 16 V/40 VA.

ⓘ **Note:** Do not connect to a receptacle controlled by a switch.

Figure 4: KT-2 inputs and outputs (European model)

Table 10: KT-2 inputs and outputs (European model)

Callout	Description
A	2.4GHz Antenna
B	RF cable with U.FL connector
C	Door locking device: 12 VDC 750 mA maximum
D	Connect a 1K Ohms resistor between LK- and +12 V if you are not using a locking device.
E	Kantech smart card reader with an integrated keypad in Wiegand mode
F	Optional RS-485 expansion module and Kantech ioSmart reader
G	Connect the RS-485 main network to other KT-2 or KT-1 controllers or to the gateway using a USB-485 interface.
H	Tamper switch
I	Connect the normally open EPS FAULT ouput (mains failure) from the KT-2-CAB-PSU to one input on the KT-2 to transmit an AC loss event to the monitoring console.

Table 10: KT-2 inputs and outputs (European model)

Callout	Description
J	Tighten the nut to break the paint and ensure a secure connection to the cabinet.
K	Battery 12 VDC/7 AH
L	Neutral
M	Ground wire from building installation
N	Line
O	Optional RJ45 Ethernet network
P	Door 1 request to exit device
Q	Door 1 contact
R	Relay 1: 30 VDC, 3 Amps, Form C
S	Optional RJ12 RS232C port: integration

Power supply (European model)

The mains input ratings are 230 VAC/50 Hz.

System setup with EntraPass

You can configure the KT-2 with EntraPass Special Edition, Corporate Edition, or Global Edition software in a number of ways.
When you use the KT-2 with EntraPass Special Edition, Corporate multi-site gateway, or Global Edition gateway, you can configure the setup in the following ways:

- Over Wi-Fi
- Over Ethernet
- Over the RS-485 with a USB-485 or VC-485

When you use the KT-2 with EntraPass Global Edition and a KT-NCC, you can configure the setup in the following ways:

- Over the local area network (LAN)
- Over the RS-485 with a USB-485 or VC-485

Security hardening guide

The security hardening guide provides information about the following areas:

- Assuring compliance with the cybersecurity criteria that govern the target environment
- Designing safe and secure deployment architecture
- Providing a reference for settings that you configure during deployment

To ensure the safe and secure deployment of the KT-2 controller, complete the following steps:

1. Ensure that you understand and plan your controller architecture. For more information, see Architecture.
2. After you complete your architectural plan, install the controller and make application-specific configuration changes. For more information, see Deployment.

Architecture

The KT-2 architecture includes the following components:

- The KT-2 controller that you can configure in one of two modes:

    - Stand-alone mode: use as a stand-alone access device with an Ethernet connection for direct configuration.
    - EntraPass mode:

        - Wired: use the Ethernet or RS-485 port to connect the controller to the network with access to the EntraPass gateway to establish communication with the EntraPass software.
        - Wi-Fi: use the built-in access point (AP) to connect the controller to a Wi-Fi network with access to the EntraPass gateway to establish communication with the EntraPass software.

- The controller commonly has at least one reader connected to it. You can connect multiple readers and input/output modules to the controller.

See the following guidelines that relate to your chosen controller architecture.

Connecting to EntraPass using RS-485

If you connect the controller to EntraPass using an RS-485 bus, the connection is not encrypted or authenticated.

- Ensure that you isolate and secure the connection wires inside the walls of the installation in a safe area.
- Ensure that you cannot access wires from an exterior wall.

Connecting to EntraPass using Ethernet

- To connect the controller to EntraPass in TCP mode, even if the link is encrypted and secure, use a LAN or VLAN.

ⓘ **Note:** The controller does not support the direct use of a VPN. Connect a VPN through a router.

Connecting to EntraPass using Wi-Fi

- Ensure that the Wi-Fi connection is encrypted.
- Use a strong Wi-Fi password.

Connecting a stand-alone controller using Ethernet

- To connect a stand-alone controller, configure your username and password. Use these details to access the secure Kantech registration web pages to configure the controller.

    ⓘ **Note:** Complete this process during the initial setup.

Connecting readers and modules using Wiegand and an SPI

The Wiegand connections and SPI connection are not encrypted or authenticated. If you connect readers and modules, complete the following steps:

- Ensure that you isolate and secure the connection wires inside the walls of the installation in a safe area.
- Ensure that you cannot access wires from an exterior wall.
- Use a tamper contact to signal an alarm if someone tries to breach security.

Connecting readers and modules using an RS-485 bus (with encrypted protocol)

- Connect readers and modules, such as the ioSmart card reader, that interconnect with an encrypted and secure 485 link. These devices include a mechanical or optical contact alarm that does not require additional wires.

Updating to the latest firmware

The latest security features are included in firmware 3.xx and higher. To ensure your controller has up-to-date security features, use the latest available firmware version.

Security configuration

You can view, monitor, and access the controller in one of three modes: stand-alone, with EntraPass, or with the cloud service.
If it is required, as you complete the installation wizard, you are prompted to reconfigure your user account, activate additional password security measures, or disable the access point mode.

Connecting to the internet

Depending on your configuration and deployment architecture, you may require internet access. To access cloud services, you require an internet connection. For a convenient stand-alone deployment, you can configure the KT-2 over the internet.

- When you connect to the internet, use a private LAN.

Managing users

Follow best practice guidelines for managing user accounts, credentials, and permissions. Best practice guidelines include the following:

- Do not share accounts.
- Change passwords every 90 days.
- Create strong passwords. Passwords must contain at least eight characters, and include one lowercase, one uppercase, one number, and one special character.
- Give users access only to what they need.
- Set temporay accounts to expire after a set amount of time.

Protecting the network

- When the trust deviation is beyond the risk tolerance, control the flow of data between trusted and untrusted networks by using a switch or a router with data flow control capabilities, such as a firewall.
- Isolate the KT-2 system from networks of lower trust.

Deployment

To ensure the safe and secure deployment of the KT-2, see the following guidelines:

- Restricting physical access to the controller
- Logging on during the initial startup
- Resetting to factory default
- Knowledge level

Restricting physical access to the controller

If you install the controller in an area that is easily accessible, this enables actions that cannot be authenticated or logged electronically, and therefore, impact the controller's cybersecurity capabilities.
To restrict unauthorized access to the controller, complete the following steps:

- Install the controller in a room, cabinet, or enclosure that you can restrict access to, for example, by using a mechanical lock or other physical access control.

- Configure the controller's mechanical tamper switch to send and log alerts if the device is tampered with.
- Use protective electric wire conduits when communication wires pass through areas of lower trust.

For more information about installing the KT-2, see Installation.

Logging on during the initial startup

To facilitate common commissioning tasks when you first start up the controller, the following functions are enabled: KT Registration web page and controller discovery. There is no default user account to access these functions.

- To log on to the controller during the initial startup, use the secure account activation process.

Resetting to factory default

- If the controller was used previously as part of another installation or test environment, reset it to factory default before you use it in the current installation. To reset the controller, see Resetting the KT-2.

Knowledge level

- To execute the proper hardening steps, you must have experience with KT-2 administration and networking technologies. To gain the required competencies, complete the basic and advanced Kantech installation courses. For more information, refer to http://www.kantech.com.

Installation

Use this section to prepare for the installation, to install the controller, and to connect all of the components.

Preparing to install the KT-2

Before you install the KT-2, follow these guidelines:

- Install the KT-2 indoors in a secure location with normal temperature and humidity levels.
- Install the KT-2 away from electrical and communication devices.
- When you mount the KT-2, ensure that there is 9 in. (23 cm) of clear space around all sides of the unit and a minimum of 13 in. (33 cm) of clear space in front of the unit.
- If you use WiFi connectivity, avoid metallic surfaces near the antenna location.
- Locate the controllers close to the controlled doors.
- Do not locate the controller within 6.5 ft (2 m) of any high voltage equipment or wiring or any electrical equipment susceptible to generating electrical interference, within 3 ft (1 m) of any telephone equipment or lines, and within 26 ft (8 m) of any third party transmitting equipment.
- Locate the controller so that it is easily accessible to service the equipment. Provide physical access by using keys on controlled doors.

Installing the KT-2

⚠️ **WARNING:** Route and secure all internal wiring using tie wraps or equivalent means to ensure that the cables do not come into contact with the front cover of the metal enclosure. Failure to do so may result in risk of physical injury to persons, or damage to or destruction of property.

1. Before you wire the terminal connections, disconnect the power supply.
2. Connect the devices that you require, for example, door locking devices, card readers, and inputs. For more information, see the following sections.
3. Connect the KT-PS4085 12 VDC power supply, or if powered by Ethernet, connect the PoE or PoE+ to the RJ-45 connection.

Figure 5: KT-2 exploded view
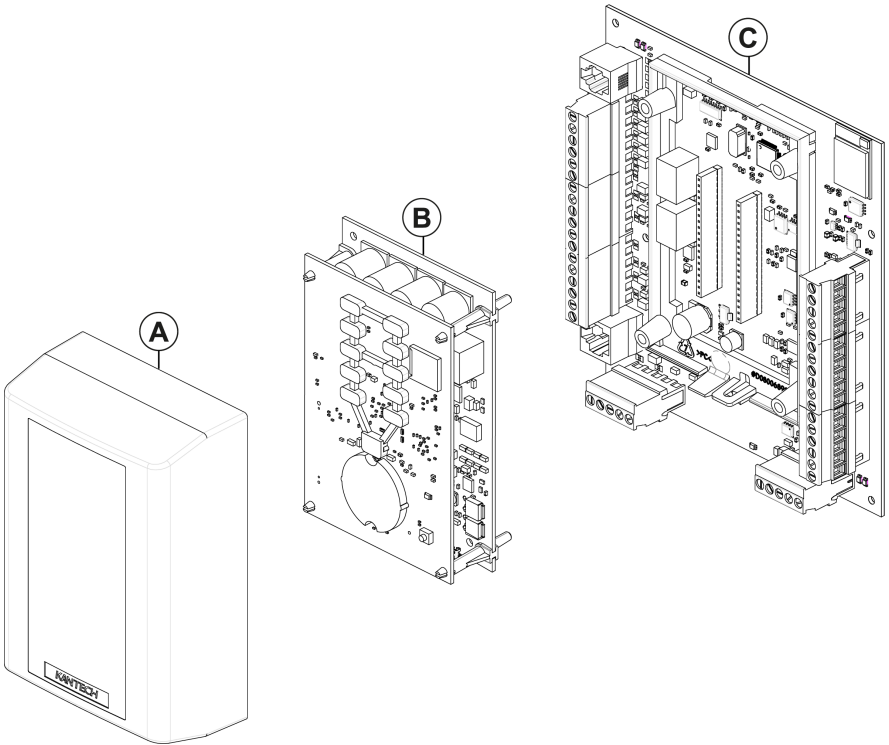
Table 11: KT-2 exploded view

Callout	Description
A	Front cover
B	Main boards
C	Backplane

Mounting the cabinet

This guide does not provide exact mounting instructions because applications and facilities vary. The surface on which you mount the cabinet at your site determines the type of hardware that you require to fasten the cabinet into position. Use wall anchors that are appropriate for the wall surface.
When you mount the cabinet, follow these guidelines:

- Mount the cabinet on a wall or other surface in a restricted-access area.
- Mount the cabinet flat against a vertical surface with the hinge to the left.
- Locate the cabinet in a position that allows the door to swing open fully to the left.
- Locate the cabinet in a position that allows air to flow over the exposed surfaces.
- Follow the environmental requirements, as Table 6 outlines.

Mounting the KT-2-M cabinet

- To mount the cabinet, use the four mounting holes as Figure 6 shows.

Figure 6: KT-2-M cabinet dimensions

9.8 in. (24.9 cm)

9.8 in. (24.9 cm)
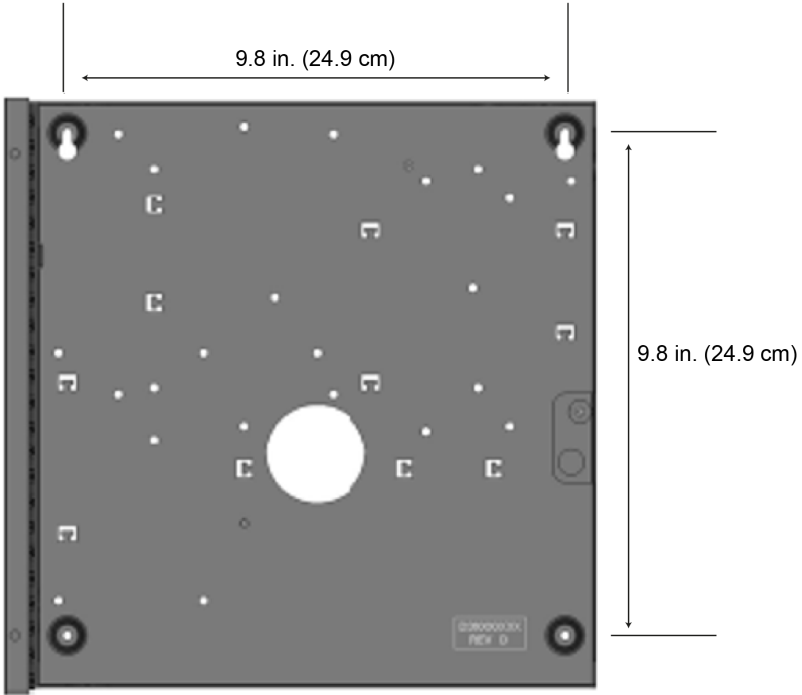
Mounting the KT-2-EU-MET cabinet

- Use 45 mm (minimum) long by 6 mm diameter screws (for example, M6).
- To mount the cabinet, use the five mounting holes, as Figure 7 shows.

Figure 7: KT-2-EU-MET cabinet dimensions
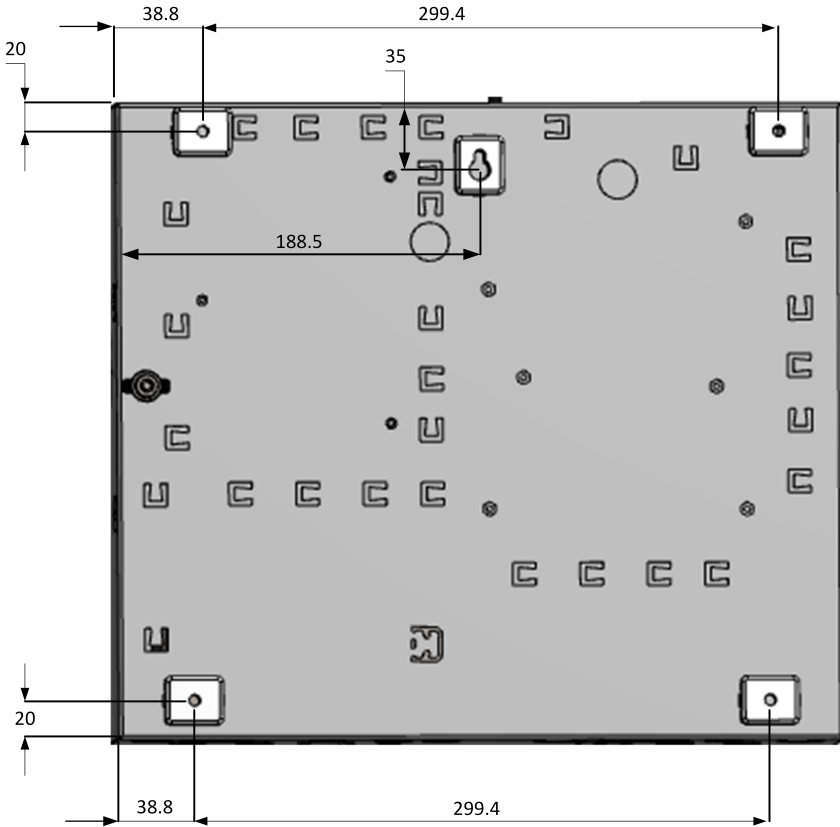
ⓘ **Note:** Dimensions in mm.

Earth grounding

To ensure that the KT-2 controller operates effectively, provide earth grounding.

1. Connect the ground wire to the corresponding earth ground terminal.
2. Make an earth ground connection to the cabinet of the controller.

   ⓘ **Note:** Follow the requirements of your local electrical code.

3. Wire the E-GND terminal on the controller's printed circuit board directly to the earth ground connection point.

Connecting door locking devices

➤ **Important:** Controlled door locking devices may be governed by regulatory bodies. Always install controlled door locking devices according to local regulations. In most instances, there are strict limitations for emergency exit doors when installing fail-secure and fail-safe locking devices, such as magnetic locks or other similar locking devices.

Note: The door locking device outputs can operate DC-powered locking devices such as electromechanical strikes and can be configured to operate in fail-safe or fail-secure mode (normal or reverse action.

Note: If required, you can program any of the controller relays to provide galvanically-isolated outputs.

1. Connect the negative wire from the door strike to the LK1- output.
2. **Optional:** Connect the door magnetic lock to the LK2- output.
3. Connect the positive wire to the +12 VDC output.
4. Program the schedules and access levels for the door locking device.

Figure 8: Door lock setup
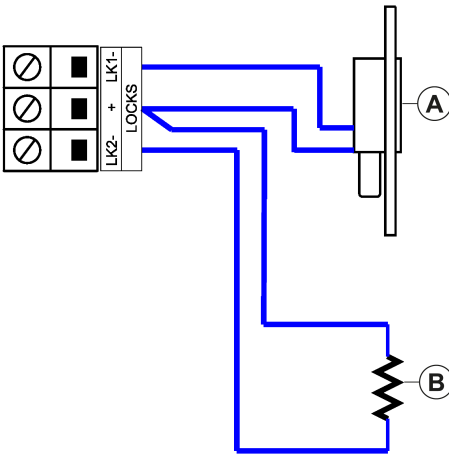
Table 12: Door lock setup

Callout	Description
A	Door locking device: 12 VDC 750 mA maximum.
B	Connect a 1000 Ohms resistor between LK- and +12 V if you do not connect a door locking device

Connecting inputs

The KT-2 controller can monitor eight inputs. Each onboard input is supervised with or without 5.6K ohm end-of-line (EOL) resistors. The maximum distance of one line is 2,000 ft (600 m) with AWG #22 in a single or double EOL configuration.

1. Connect devices to inputs 1 to 4.
2. Define onboard inputs with none, single, or double EOL resistors.
   Note: For UL listed installations, you must use supervised EOL resistors.

Inputs 1 and 2 are automatically reserved for controller door number 1. Inputs 5 and 6 are automatically reserved for controller door number 2.

Table 13: Automatic input assignments

Door	Door contact	Request to exit detector
1	Input 1	Input 2
2	Input 5	Input 6

Note: You do not have to follow this convention but it facilitates servicing.

KT-2 Two-Door Controller Installation Guide

Figure 9: KT-2 inputs
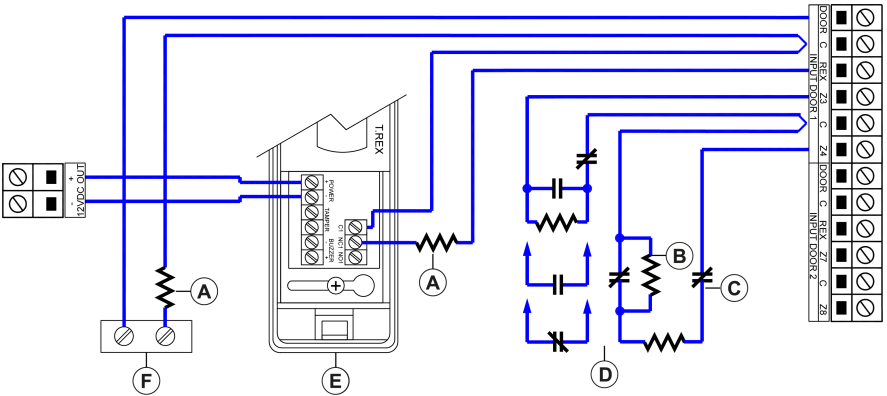
Table 14: KT-2 inputs

Callout	Description
A	Optional end-of-line resistor
B	Alarm
C	Tamper
D	Individually programmable zone termination: NC, NO, NEOL, single or double EOL termination.
E	Door 1 request to exit device
F	Door 1 door contact

Connecting card readers

You can connect up to two readers to a KT-2 controller. The controller provides 12 VDC power for card readers. The maximum distance between the readers and the controller varies by reader type. For more information, refer to the card reader Installation Guide.

- Install one reader to control the entry of a single door.
- Install two readers to control the entry and the exit of a single door.

Figure 10 shows how to connect two readers using a Wiegand configuration. Figure 11 shows how to connect two readers using a daisy-chain RS-485 configuration.

Figure 10: Wiegand configuration

| (BUZ) Blue |
| (LED) Brown |
| (GND) Black |
| (PWR) Red |
| (D1) White |
| (D0) Green |
| (BUZ) Blue |
| (LED) Brown |
| (GND) Black |
| (PWR) Red |
| (D1) White |
| (D0) Green |
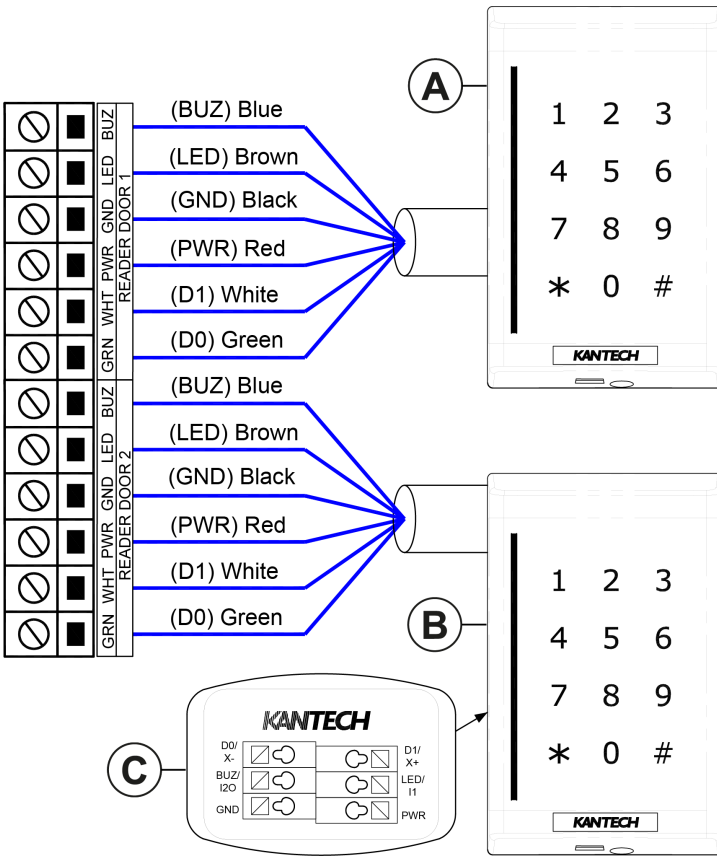
Table 15: Wiegand configuration

Callout	Description
A	Reader door 1
B	Reader door 2
C	Rear view of the reader

Figure 11: RS-485 configuration
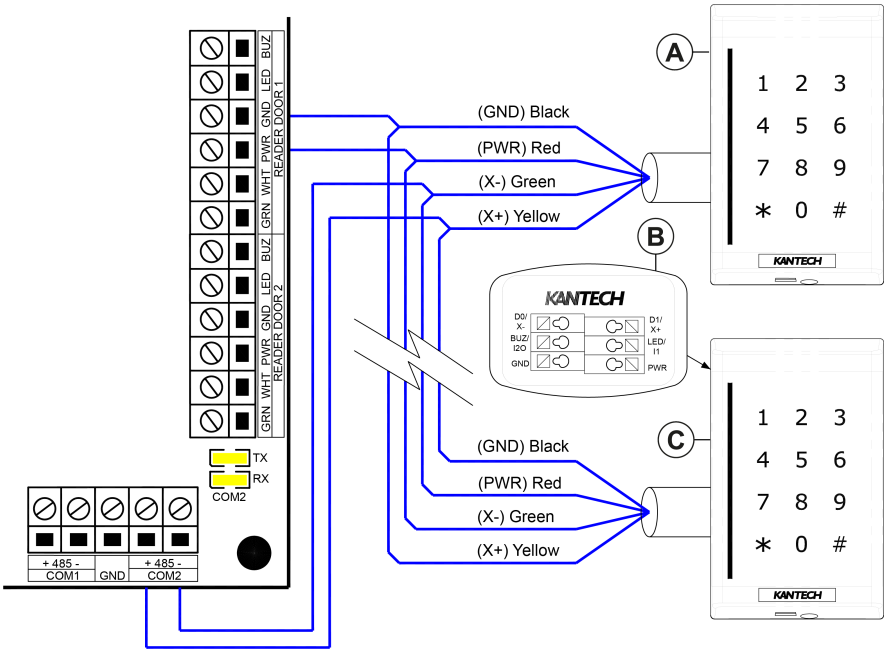
Table 16: RS-485 configuration

Callout	Description
A	Reader door 1
B	Rear view of the reader
C	Reader door 2

Connecting relay controlled outputs

The KT-2 controller provides two Form C relays that are rated at 3 Amps, 30 VDC, 0.6 power factor.

Figure 12: KT-2 relay controlled outputs
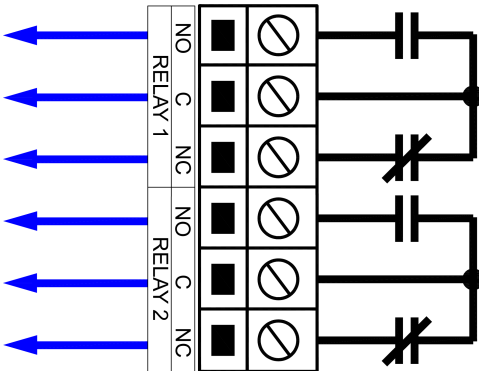
Connecting auxiliary outputs

LEDs provide visual feedback for access operations. Audible warning devices, such as the T-REX or reader buzzer, signal door alarms.

- To provide visual and audio signals of access operations, connect auxiliary outputs to card readers and to local warning devices.

  (i) **Note:** Auxiliary outputs activate according to input conditions, events, and local alarms.

Connecting the KT-2 over RS-485

⚠ **CAUTION:** Do not connect several KT-2 controllers at a single point. Do not use splitters or spider web networks at a single point.

(i) **Note:** On the last KT-2 controller of a loop, there is no end-of-line resistor to install on the RS-485 COM1 terminals.

1. Connect the RS-485 cable to (COM1) X+, X-. The RS-485 terminals link the controllers together.

   (i) **Note:** The maximum communication loop length is 4,000 ft (1.2 km) using the appropriate cabling.

2. Wire the RS-485 communication loop with an Ethernet Category 3 double twisted pair (unshielded) network cable or better.

   (i) **Note:** The RS-485 loop can operate from 1200 to 115200 Bauds under normal conditions.

3. **Optional:** If you experience intermittent communication problems or erratic operation, drop your network speed to a Baud rate of 9600 or 19200. If you vary the network speed, the operating speed of the system does not change noticeably.

Figure 13: Connecting the KT-2
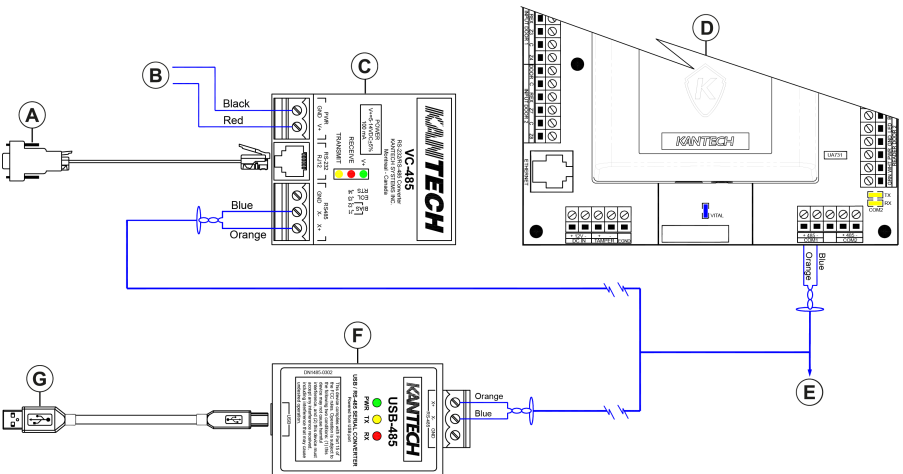
Table 17: Connecting the KT-2

Callout	Description
A	DB9F: Gateway serial port. The maximum length of the cable is 100 ft (33 m).
B	External power supply: 5 to 14 VDC 100 mA
C	VC-485: RS-232 to RS-485 serial communication interface.
D	KT-2 controller

Table 17: Connecting the KT-2

Callout	Description
E	Connect the RS-485 main network to other KT-2 controllers using the RS-485 interface.
F	USB-485: USB to RS-485 serial communication interface.
G	Gateway USB port. The maximum length of the cable is 3.3 ft (1 m).

Making an RS-232 cable with an RJ-12 connector

To make your own RS-232 cable with an RJ-12 connector, see the following figure which shows an example of the configuration.

Figure 14: RJ-12 pin-out
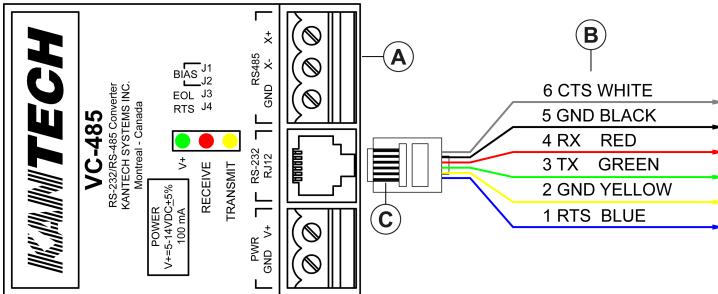
Table 18: RJ-12 pin-out

Callout	Description
A	VC-485
B	RJ-12 male connector (clip down)
C	PIN 1

Powering the KT-2

➤ **Important:** Do not apply power to the KT-2 controller until after you complete and test all connections, and after you fix the unit to the wall.

ⓘ **Note:** Do not connect the KT-2 controller to the PoE or PoE+ injector and to an external 12 VDC power supply at the same time.

To power the controller, complete one of the following procedures:

Powering the KT-2 using PoE or PoE+

- During the installation, connect the Ethernet wire to the RJ-45 connector.
    - ⓘ **Note:** Use PoE or PoE+ Phihong models POE125U-4-HP-R or POE36U-1AT-R.
    - ⓘ **Note:** Do not use PoE or PoE+ if you intend to use the KT-2 as a wireless controller.

Powering the KT-2 using a KT-PS4085 power supply

- Connect a KT-PS4085 power supply to the 12 VDC input terminals.
    - ⓘ **Note:** To ensure the KT-PS4085 operates correctly, use a 12 VDC 7 AH battery.

Powering the KT-2 in a KT-2-CAB-M

1. Connect a KT-PS4085 power supply, a PTC 1640UG plug-in adapter, and a battery rated 12V/7Ah. In this configuration, the KT-2 has four hours of standby power.
2. Connect the AC trouble output from the KT-PS4085 to one of the available inputs on the KT-2 to transmit AC loss events to the monitoring console.

Reset options

The KT-2 has four reset options:

- Soft reset
- Hard reset
- Forced default static
- Factory default DHCP

To reset the controller, see Resetting the KT-2.

Soft reset

If you perform a soft reset on a KT-2, the following occurs:

- If all of the controller's memory definitions and parameters are valid, they are verified and kept intact. If they are not valid, the controller goes into a hard reset.
- If it is valid, the internal event buffer is maintained.
- If it is defined, the previous IP address is kept.
- You see one of the following messages: **Power ON Soft Reset**, **Manual Pushbutton Soft Reset**, or **Operator Soft Reset**.
- The input alarm status is maintained unless it was changed during the restart.
- Relay energizing (physical) state is maintained even if the relay LED goes off.
- The LED pattern does not change during the reset.

Table 19: Soft reset LED pattern

EntraPass Edition	Communication state	LED pattern
All editions	Offline	Fast flashes
Global Edition	Online	1 flash every second
Corporate Edition	Online	3 flashes every second

Hard reset

If you perform a hard reset on a KT-2, the following occurs:

- All of the controller's memory definitions reset to their default values.
- The internal event buffer clears.
- If they are used, the IP address and WiFi configuration are kept.
- The LED pattern is in a hard reset state: 4 flashes every second, if it is not in a factory default or forced default static state.
- You see the following message: **Controller Hard Reset**.
- The internal real time clock (RTC) and clock reset to the default time an date values of January 1st 2014, 00:00:00, Wednesday.

Forced default static

If you perform a forced default on a KT-2, the following occurs:

- If all of the controller's memory definitions and parameters are valid, they are verified and kept intact. If they are not valid, the controller goes into a hard reset.
- If it is valid, the internal event buffer is maintained.
- The IP address resets to the default static IP: 192.168.1.2 Subnet mask: 255.255.255.0.
- You see one of the following messages: **Power ON Soft Reset**, **Manual Pushbutton Soft Reset**, or **Operator Soft Reset**.

KT-2 Two-Door Controller Installation Guide

- The LED pattern remains in forced default static mode: a flashing beat of 3 reversed flashes, until the controller resets to another mode.
  - ⓘ **Note:** When the LED is normally on and flashes off, it is a reversed flash.

Factory default DHCP

The KT-2 default DHCP is completed by Kantech. Reset the controller to factory default DHCP only for the following reasons:

- To configure the KT-2 with the KT-Finder. For more information, see Configuring the KT-2 using the KT-Finder.
- To change the KT-2 communication port.

If you perform a factory default on a KT-2, the following occurs:

- All of the controller's memory definitions reset to their default values.
- The internal event buffer clears.
- The LED pattern is a reversed flash continuous beat.
- You see the following message: **Controller Factory Default Reset**.
- The internal RTC and clock reset to the default time and date values of January 1st 2014, 00:00:00, Wednesday.
- EntraPass configures the controller by communicating through an Ethernet or RS-485 communication port. Over WiFi, the controller automatically performs an antenna calibration, reverts to access point mode, and waits for its configuration from the default web page. For more information, see Enabling WiFi connectivity.

Resetting the KT-2

1. Remove the front cover of the KT-2 controller by unlocking the clip at the bottom.
2. In the lower right of the main board, locate the **Reset** button. See Figure 15.
3. Complete one of the following reset options:

Table 20: Steps for each reset option

Step	Soft reset	Hard reset	Forced default static	Factory default DHCP
a	Press **Reset** for less than 2 seconds.	Press **Reset** for 3 seconds until you hear 5 beeps.		
b	-	Press **Reset** once.	Press **Reset** twice.	Press **Reset** three times.
c	-	Press **Reset** for 3 seconds until you hear 5 beeps.		

ⓘ **Note:** For a description of the Kantech shield LED during each reset option, see Table 8.

Figure 15: KT-2 main board
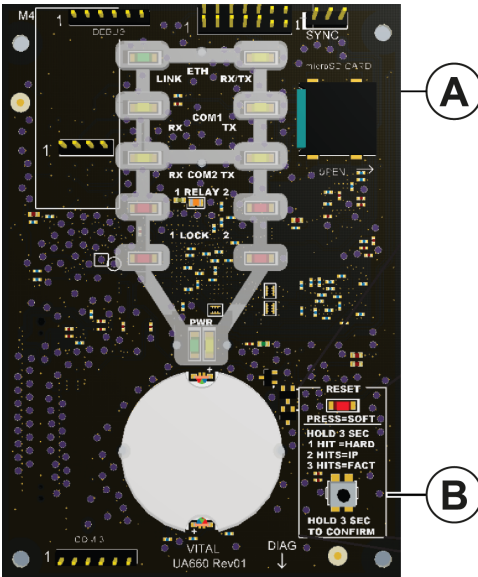
Callout	Description
A	KT-2 controller main board
B	Reset button

Using the One Button on the Kantech shield

The One Button is located on the Kantech shield. Press the One Button to configure some of the controller's functions.

ⓘ **Note:** When you replace the controller's front cover, there is a 20-second delay before the One Button responds.

Turning on the Kantech shield LED

• Press the button for three seconds. The status LED activates for 10 minutes. To deactivate this function, press the button for three seconds again.

Enrolling to EntraPass

• Press the button for six seconds to trigger enrollment to EntraPass for ten minutes and to activate the status LED. To turn off these functions, press the button for six seconds again.

ⓘ **Note:** This function is available only when the KT-2 controller is connected over Ethernet.

Configuration

To configure a wired controller, complete the steps in one of the following procedures:

- To configure standalone mode, complete Configuring the KT-2 using the registration page.
- To configure EntraPass mode, complete one of the following procedures:

    - Configuring the KT-2 using the registration page
    - Configuring the KT-2 using the KT-Finder

To configure a wireless controller, complete Connecting and configuring a wireless controller.

Configuring the KT-2 using the registration page

1. Connect the controller to your preferred network using the Ethernet port.
2. On your computer or mobile device, open a web browser.

ⓘ **Note:** If you use a mobile device, connect it to a wireless network that has access to the wired network subnet.

3. In the address bar, type one of the following options:

    - Type the IP address of the KT-2 controller. This is the preferred option. To find the controller's IP address, you can use the KT-Finder.
    - Type `KT-XX-XX-XX` where XX-XX-XX is the last six digits of the controller's Ethernet MAC address.

ⓘ **Note:** The KT-2 controller and the device you use to access the registration page must be on the same network. If either of the devices are behind a bridged network, even if they have the same subnet, this cannot work.

4. On the **KT-2 REGISTRATION** page, in the upper right of the window, select your preferred language. English is selected by default.
5. To configure the correct mode, complete the steps in one of the following procedures:

    - To configure the controller in stand-alone mode, complete one of the following options:

        - Configuring stand-alone mode using the activate now option
        - Configuring stand-alone mode using an activation code

    - To configure the controller in EntraPass mode, complete Configuring EntraPass mode for a wired controller.

Configuring stand-alone mode using the activate now option

1. On the **KT-2 REGISTRATION** page, click **Activate now**.
2. On the **Activate now** tab, in the **Customer information** and **Installer information** fields, type the relevant information.
3. Click **Activate now**.

Configuring stand-alone mode using an activation code

1. Go to http://www.kantech.com.
2. Click **Support** and click **Kantech Registration**.
3. In the **KT Standalone Registration** area, click **Click here**.
4. On the **KTWeb - Registration** page, type the relevant information and click **Register**. You receive an activation code by email. Alternatively, contact Kantech technical support in your region to get an activation code.
5. Go to the **KT-2 REGISTRATION** page and click **Other ways to activate**.

6.   In the **Activation code** field, type the activation code, and click **Activate now**.

Configuring EntraPass mode for a wired controller

1. On the **KT-2 REGISTRATION** page, click **EntraPass**.
2. In the **EntraPass gateway** pane, in the **IP address** field, type the IP address, or in the **Domain name** field, type the domain name.
3. From the **Protocol** list, select **TCP** or **UDP**.
4. **Optional:** If you select **UDP**, in the **Port** field, type the port number.
5. Click **Submit**.

Configuring the KT-2 using the KT-Finder

Download the KT-Finder for free from http://www.kantech.com. Use the KT-Finder application to configure the controller over the LAN or the WAN.

   ⓘ   **Note:** If you connect to Wi-Fi, use the STA MAC address not the AP.

1. Exit all EntraPass applications and services.
2. Reset the KT-2 to factory default DHCP mode. For more information, see Resetting the KT-2
3. To open the KT-Finder, go to ***Start >All Programs>EntraPass Edition>Server>KT-Finder***.

      ⓘ   **Note:** If you try to open the KT-Finder when EntraPass is open, an error message appears.

4. In the **KT-Finder Wizard** window, from the **Device** list, click **KT-2**.
5. In the **MAC address** field, type the MAC address of the KT-2, and click **Connect**. When the KT-Finder finds the controller, the following message appears: **Configuring the KT-2 with the KT-Finder**.
6. In the **EntraPass Gateway** pane, in the **EntraPass IP Address** field, type the IP address. For more information, refer to the *EntraPass Administrative Guide*.
7. In the **Ethernet configuration** pane, from the **Protocol** list, select **UDP** or **TCP**.
8. **Optional:** If you select **UDP**, in the **Port** field, type the port number.

      ⓘ   **Note:** Change the port number only if you have more than one KT-2 controller at the same remote site.

9. Click **OK**.
10. Repeat the steps for each controller at the site.

Connecting and configuring a wireless controller

You can connect the KT-2 over Wi-Fi only when you use the controller in EntraPass mode and power it with a KT-PS4085 power supply.

1. On a laptop or mobile device, go to the Wi-Fi settings.
2. From the list of available wireless networks, select the access point (AP) name (SSID) of the controller. The AP name of the controller appears as **KT2-XX-XX-XX**. XX-XX-XX represents the last six digits of the AP MAC address printed on the KT-2 backplane label.
3. Clear the **Connect automatically** check box and click **Connect**.
4. In the **Enter the network security key** field, type the password. The default password is `TYCO1234`.
5. Click **Next** and check your connection status.
6. On a web browser address bar, type the following IP address: `192.168.240.1/jciprov.html`. Press Enter.
7. On the **Web Provisioning** page, from the **Please Select Country** list, select a country.

   ⓘ   **Note:** To change the selected country after you complete the configuration, you must factory default the controller. All saved settings and data are lost when you factory default the controller.

   ⓘ   **Note:** The list of supported countries may vary depending on regulatory and standards updates.

8. In the **Wireless Network** pane, click **Select Network from List** and select the appropriate network, or click **Manually** and type the name of the network if it is hidden.

9. In the **Password** field, type the network password.
10. In the **EntraPass gateway** pane, click **EntraPass IP address**, and type the direct IP address. Alternatively, leave the IP address as **0.0.0.0** if you want to enroll the controller using the KT-Finder or the One Button.

ⓘ **Note:** To avoid connectivity issues, ensure that the controller and the gateway are on the same subnet, and that all the required ports are open in the firewall.

11. From the **Protocol** list, select **TCP** or **UDP**. Before you configure the protocol, ask your network administrator about the firewall rules for communicating over your selected protocol.
12. **Optional:** If you select **UDP**, in the **Port** field, type the port number. Before you configure the port, ask your network administrator about the firewall rules for ports.
13. Click **Submit**.

Result

- If the controller succeeds in joining the selected wireless network, the Wi-Fi LED turns on and is solid yellow.
- If the controller fails to connect, the Wi-Fi LED stays off. The controller attempts to connect three times before returning to AP mode (factory default).
- If static IP mode is not supported in Wi-Fi, the Wi-Fi LED turns off.

KT-2 models, expansion kits, and related items

The following table lists all of the KT-2 controller models, expansion kits, and miscellaneous, related items.

Table 21: KT-2 models, expansion kits, and related items

Part number	Description
KT-2-M	One KT-2-BP, IP controller with metal cabinet (No P/S, no BAT)
KT-2-BP	Two-Door IP Controller Back-Plate
KT-2-CVR	Black replacement cover for a KT-2 controller including a back box
KT-2-CAB-M	Metal enclosure only for the KT-2-BP
KT-2-MP	KT-300 back plate cabinet adapter
KT-2-ANT	WiFi antenna with knockout plug kit
USB-485	USB-485 interface, USB cable 0.9 m (3 ft) and USB drivers on CD-ROM
VC-485	VC-485 interface, RS-232 cable 3 m (10 ft) with RJ-12 connectors, 740-1012 (DB25F to RJ-12) adapter, 740-1022 (DB9F to RJ-12) adapter and 740-1033 (DB25M to RJ-12) adapter
KT-PTC1640UG	Plug-in wall transformer, 120 V/16 VAC 40 VA (US only)
KT-PTC1640CG	Plug-in wall transformer, 120 V/16 VAC 40 VA (Canada only)
KT-PS4085	12 VDC, 1.5 A power supply, optional
KT-BATT-12	Rechargeable battery, 12 VDC, 7 AH, optional
KT-MOD-IO16	RS-485 Input/Output Module
KT-MOD-INP16	Expansion module 16-zone input with SPI cable (KT-MOD-SPI-16)
KT-MOD-OUT16	Expansion module 16-output with SPI cable (KT-MOD-SPI-16)
KT-MOD-REL8	Expansion module 8-relay with SPI cable (KT-MOD-SPI-16)

Compliance specifications

United States and Canada

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 this 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 may cause harmful interference, in which case users will be required to correct the interference at their own expense.

RF Transmitters: Compliance Statement (Part 15. 19)

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.
2. This device must accept any interference received, including interference that may cause undesired operation.

Warning (Part 15. 21)

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

RF Exposure (OET Bulletin 65)

To comply with FCC RF exposure requirements for mobile transmitting devices, this transmitter should only be used or installed at locations where there is at least 20 cm separation distance between the antenna and all persons.

Canada

This class A digital apparatus meets all requirements of the Canadian Interference Causing Equipment Regulations. CAN ICES-3 (A) / NMB-3 (A).
This radio transmitter 9154-GS2101M has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with the KT-2.
Table 22: Antenna type

Antenna type	Antenna gain at 2.4 GHz
Dipole with I-PEX connector	2.5 dBi (maximum)

CE, RCM, & UKCA

Australia/New Zealand: RCM Compliance.
European Union: KT-2-EU-MET complies with Radio Equipment Directive.
United Kingdom: KT-2-EU-MET complies with Radio Equipment Regulations.

UL

When a KT-2 is enclosed in the metal cabinet model KT-2-CAB-M and powered by the power supply model KT-PS4085 in conjunction with the external adapter PTC1640UG the following performance levels are defined for the access control unit as per UL 294:
Destructive attack: Level I (no attack test)
Endurance: Level IV (100,000 cycles)
Standby power: Level 1 (when no standby power is provided) and Level IV (4 hours, when using KT-PS4085)

ⓘ **Note:** If KT-2 is used in a single gang configuration, powered by an external, separately listed power supply or PoE/PoE+ switch the performance levels remain the same with the exception of the standby time that will be rated Level I (no secondary power source).

Line Security: Level II (Standard line security, RS-485, Ethernet, or Wi-Fi) and Level III (encrypted line security 128 bit, Ethernet only)

ⓘ **Note:** Line Security Level II requires an audible **or** visual signal at the monitoring station (EntraPass) and at the protected premises (KT-2 controller).

(i) **Note:** Line Security Level III requires an audible **and** visual signal at the monitoring station (EntraPass) and at the protected premises (KT-2 controller).

To set up audible and/or visual signals in EntraPass, complete the following procedures:

Creating a task builder action for audible and visual signals in EntraPass

1. On the EntraPass main menu, click the **Definition** tab, and click **Task Builder**.
2. In the **Task Builder** window, click the **New** icon.
3. In the **English** field, enter a name for the task.
4. Click **Command**.
5. To set up an audible signal, complete the following steps:

     a. In the **SmartLink Task Builder** window, from the **Component Type** list, select **Relay**.
     b. From the **Command** list, select a relay action, for example **Toggle relay activation**.
     c. From the **Component** List, select a relay on the KT-2 controller.

6. To set up a visual signal, complete the following steps:

     a. In the **SmartLink Task Builder** window, from the **Component Type** list, select **Relay**.
     b. From the **Command** list, select a relay action, for example **Toggle relay activation**.
     c. From the **Component** List, select a relay on the KT-2 controller.

7. Click **OK**.
8. Click **Save** and close the window.

(i) **Note:** Audible and visual signaling devices must be connected to the KT-2 relays and located near to the KT-2 controller. Depending on the audible or visual device you use, you may require an external power supply.

Creating a trigger and alarm sound in EntraPass

1. On the EntraPass main menu, click the **Devices** tab and click **Controller**.
2. From the **Controller** list, select the controller.
3. Click the **Trigger and Alarm** tab.
4. Right-click and select **New trigger**.
5. In the **Trigger and Alarm** window, in the **English** field, enter a name for the trigger.
6. On the **General** tab, from the **Component Type** list, select **Controller**.
7. From the **Controller** list, select the controller.
8. From the **Trigger schedule** list, select **Always valid**.
9. From the **Task Builder** list, select the task that you created in Creating a task builder action for audible and visual signals in EntraPass.
10. On the **Events** tab, click **Controller communication failed**.
11. On the **Alarm notification** tab, from the **Alarm schedule** list, select **Always valid**.
12. From the **Desktop alarm** list, select **Always valid**, and click the **Save** icon.
13. To create an alarm sound, complete the following steps:

     a. On the EntraPass main menu, click the **Options** tab and click **Multimedia Device**.
     b. On the **Sound** tab, from the **Priority** list, select the priority level associated with the event **Controller communication failed**. The default is priority level 3.
     c. Click **Assign alarm sound** and select an alarm sound from the list.
     d. Click **OK**.

14. On the EntraPass main menu, click the **Desktops** tab, right-click one of the eight desktop views and select **Properties**.
15. In the **Desktop properties** window, in the **Alarms Desktop** pane, select **Messages screen** and click **OK**.

When a controller's communication fails, a message displays in the desktop view and an alarm sounds.

To comply with UL listings, the following requirements must be met:

- Installation locations and wiring methods shall be in accordance with the National Electrical Code, ANSI/NFPA 70.
- Do not connect to a receptacle controlled by a switch.
- Use of a UL listed computer.
- Use of UL listed readers (Wiegand 26 and 34 bits, stripe 26 and 34 bits, XSF 39 bits have been tested and found to comply).
- Kantech XSF 39 bits have been tested and found to comply.
- Use of a UL recognized tamper switch on every housing cabinet for the KT-2 Two-Door Controller.
- Do not use the SmartLink option.
- Do not use a 230 VAC transformer (not UL listed).
- Use only UL listed cables.
- Use only UL listed adaptors.
- Use only a UL listed power supply such as Kantech part number KT-PS4085 (available through Kantech distributors or dealers, please refer to the Technical Support contact information at the beginning of this guide to obtain the specific transformer).
- The KT-2-EU-MET has not been validated as a UL Listed system.
- The PTC1640UG and 12V/7Ah battery are used for 4 hours of standby power.
- Security hardening guide has not been evaluated by UL.

ⓘ **Note:** All circuits are power limited with the exception of battery connection. Separation of 3/4 in. shall be maintained between power limited and non-power limited wiring.

ⓘ **Note:** Replace battery with Changzho Jintan Chaochuang Battery Co Ltd., Pansonic or Energizer Part No. CR2032 Only. Use of another battery may present a risk of fire or explosion.

UL 294 Compliance Notice

- Use only UL 294 or UL 1076 listed power supply.
- Connect Kantech part number KT-ACPW-LED status indicator to the AC terminals of the KT-PS4085.
- Use Kantech part number KT-BATT-12 battery.

    ⓘ **Note:** Using a 12V/7Ah battery, backup battery provides a minimum of 4 hours standby time.

- For UL listed installations, use only in conjunction with compatible PoE/PoE+ devices that are UL 294 listed. These devices shall be used in conjunction with UL listed transient protectors.
- The following Kantech readers have been validated by UL for the UL 294 Standard: P225W26, P225KPW26, P225XSF, P225KPXSF, P325W26, P325KPW26, P325XSF, P325KPXSF, P600, KT-MUL-SC, KT-MUL-SC-KP, KT-SG-SC, KT-SG-SC-KP, KT-MUL-MT, KT-MUL-MT-KP, KT-SG-MT, and KT-SG-MT-KP.
- Communication between EntraPass and the KT-2 shall use a secure network to guard against such threats as: Denial of Service (DoS), spoofing, sniffing, hijacking, Trojans, viruses/worms, and malware.

UL 1076 Compliance Notice

- The KT-2 is UL 1076 Listed as a Commercial Proprietary Control Unit Accessory and Proprietary Burglar Alarm Unit (Section 83.2), with EntraPass and Redundant Server, alarm system features, KT-300, KT-400 Controllers, Kantech ioProx Proximity readers, and TRex request to exit devices – other sensor devices (temperature, water level, etc.) may be used as long as they are also UL 1076 Listed.
- The EntraPass and Redundant Server shall be running at all time, and manned 24 hours a day, 365 days a year – The EntraPass and Redundant Server will each have their own operator workstation.
- Data processing equipment and office appliance and business equipment used as central supervisory equipment station shall be listed to Information Technology Equipment - Safety-Part 1: General Requirements - UL 60950-1 or UL 62368-1.

- Should the EntraPass and/or Redundant Server be replaced, a UL 60950-1 or UL 62368-1 listed computer must be used.
- The following recommended system requirements apply to the EntraPass Server, Redundant Server, Video Vault, Card Gateway, SmartLink, and Workstation:

  - Operating Systems: Windows® 2008/Windows 2012/Windows 7 Standard/Enterprise Server Editions/Windows 8/Windows 10
  - Processor: Dual Core
  - 4 GB RAM
  - Minimum free hard disk space: 20 GB
  - Color depth: 24-bit (16 million colors), required for Video Integration only
  - Screen resolution: 1024 x 768
  - AGP or PCI Express 8X graphics card with 64 MB memory and DirectX 9.0 support
  - Network Interface card: 10/100 Base-T network adaptor

  ⓘ **Note:** Actual requirements may vary based on your operating system and configuration.
- The Central Supervisory Equipment shall employ supply line transient protection complying with the Standard for Transient Voltage Surge Suppressors, UL 1449, with a maximum marked rating of 330 V.
- The Central Supervisory Equipment shall employ signal line Transient protection complying with the Standard for Protectors for Data Communications and Fire Alarm Circuits, UL 497B, with a maximum marked rating of 50 V.
- The Central Supervisory Equipment shall employ that communication circuits and network components connected to the telecommunications network shall be protected by secondary protectors for communication circuits. These protectors shall comply with the Standard for Secondary Protectors for Communications Circuits, UL 497A. These protectors shall be used only in the protected site of the telecommunications network.
- The Central Supervisory Equipment shall be installed in a temperature controlled environment. A temperature controlled environment is defined as one that can be maintained between 13° - 35°C (55° - 95°F) by HVAC system. Twenty-four hours on standby power shall be provided for the HVAC system. The standby power system for the HVAC system may be supplied by an engine driven generator alone. A standby battery is not required to be used.
- A marking to identify the application and signaling function of the product is located on the inside of the unit (inner door sticker).
- For certified commercial proprietary control unit accessory applications, the requirements of UL 1076, Commercial Proprietary Control Unit Accessory also apply.
- The reader(s), that is(are) designated to arm or disarm the alarm system, must be within the secured side of the customer premises.
- The following Kantech readers have been validated by UL for the UL 1076 Standard: P225W26, P225KPW26, P225XSF, P225KPXSF, P325W26, P325KPW26, P325XSF, P325KPXSF and P600.
- All alarms shall be reported and acknowledged in the following priority:
  ⓘ **Note:** To set these priorities, please adjust the Event Parameters, found in EntraPass System.

  - Fire alarm and industrial supervision where a risk of injury to persons, or damage or destruction of property may be involved.
  - Hold-up or panic alarm.
  - Burglar alarm.
  - Watchman tour (Guard tour).
  - Fire-alarm supervision.
  - Burglar-alarm supervision.
  - Industrial supervision where a risk of injury to persons, or damage or destruction of property will not be involved.

- If multiplex system signals are transmitted directly from the protected systems to the central supervising station and the loss of the channel prevents the receipt of signals from protective circuits beyond the fault, the number of separate signals on a single channel shall be limited to 1000.

- Minimum 4 hours of stand-by power provided by a standby rechargeable battery, rated 12V, 7Ah. Loss of AC signal is transmitted immediately to the central station. Required use of Reader's LED (flashing) as acknowledgment signal indicator.
- Use EntraPass and under Definition/Alarm System/Door enable the option "Supervised door when armed" when using the Reader's flashing LED to indicate the acknowledgment signal. POE/POE+ feature is not permitted for UL 1076.
- The supervision of the IP network connection between a KT-2 and EntraPass is controlled by the network pulse time. You can program the network pulse time in EntraPass from 15 seconds up to 10 minutes. The default times are 1 minute for EntraPass Corporate Edition and 15 seconds for EntraPass Global Edition. For UL listed installations, the allowed range for the network pulse time is from 15 seconds up to 140 seconds. The loss of communication notification will occur when the network pulse time has elapsed twice plus 15 seconds.
- Acknowledgment signal (closing signal) is indicated at the user interface reader via a flashing red/green LED.