KANTECH

WinPASS™

System Reference Manual & KT-300 controllers

Version 2

SPECIFIER'S CHOICE
AWARD
NEW YORK 1997

DSC
GROUP OF COMPANIES

Part of the DSC group, Kantech Systems Inc. embraces the group's corporate philosophy of providing competitive and innovative products. Established in 1986, Kantech Systems has been designing and manufacturing integrated access control systems for industrial, government and military applications.

The DSC Group is recognized as a leading international manufacturer of security products. As a group, we currently supply hundreds of different security products that are distributed in more than 100 countries. We strongly believe in cost effective manufacturing and product innovation. Over one hundred engineers and technologists contribute to our on going R&D efforts with one goal in mind: providing high quality, cost effective and innovative products!

DSC group manufacturing facilities are spacious, efficient and equipped with the most advanced electronic assembly equipment operating on 24 hour production schedule to meet demand, quickly and efficiently.

ISO-9001 Certified Quality System

The international Organization for Standardization (ISO) is a worldwide federation of national standard bodies. ISO has developed a series of standards relating to a Quality System known as the ISO family standards. The ISO-9001 standard defines the highest level for this Quality System and is applicable to design, development, production, installation and servicing, final inspection and testing.

The system is audited twice a year and certified by outside auditors/registrars. Kantech's quality system also extends to its suppliers and customers. A supplier must be initially approved and thereafter, regularly appraised and rated. Customer feedback is documented and reviewed under formal procedures by Kantech's internal Continuing Improvement Committee composed of employees from every department.

Kantech Systems Inc.
3650-A Matte Boulevard
Brossard, Quebec
Canada J4Y 2Z2

Customer Assistance
Tel: 1(450) 444-2040 ext.: 399
Fax: 1(450) 444-2029
Web Site: http://www.kantech.com

Specifications may change at any time without prior notice

MARCH 2000

END-USER LICENSE AGREEMENT
FOR Kantech Software Provided With or Without Products or Components

IMPORTANT - READ CAREFULLY: Kantech Software purchased with or without Products and Components is copyrighted and is purchased under the following license terms:

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

SOFTWARE PRODUCT LICENSE

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

1. GRANT OF LICENSE. THIS EULA GRANTS YOU THE FOLLOWING RIGHTS:

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

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

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

2. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS.

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

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

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

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

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

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

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

3. COPYRIGHT.

All title and intellectual property rights in and to the SOFTWARE PRODUCT (including but not limited to any images, photographs, and text incorporated into the SOFTWARE PRODUCT), the accompanying printed materials, and any copies of the SOFTWARE PRODUCT, are owned by Kantech or its suppliers. You may not copy the printed materials accompanying the SOFTWARE PRODUCT. All title and intellectual property rights in and to the content which may be accessed through use of the SOFTWARE

Continuation from previous page...

PRODUCT are the property of the respective content owner and may be protected by applicable copyright or other intellectual property laws and treaties. This EULA grants You no rights to use such content. All rights not expressly granted under this EULA are reserved by Kantech and its suppliers.

4. EXPORT RESTRICTIONS.

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

5. CHOICE OF LAW: THIS SOFTWARE LICENSE AGREEMENT IS GOVERNED BY THE LAWS OF THE PROVINCE OF ONTARIO, CANADA.

6. ARBITRATION

All disputes arising in connection with this Agreement shall be determined by final and binding arbitration in accordance with the *International Commercial Arbitration Act*, R.S.O. 1990, c. I.9, or any successor or replacement legislation which may be in force, and the parties agree to be bound by the arbitrator's decision. The place of arbitration shall be Toronto, Canada.

7. LIMITED WARRANTY

(a) NO WARRANTY

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

(b) CHANGES IN OPERATING ENVIRONMENT

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

(c) LIMITATION OF LIABILITY; WARRANTY REFLECTS ALLOCATION OF RISK

IN ANY EVENT, IF ANY STATUTE IMPLIES WARRANTIES OR CONDITIONS NOT STATED IN THIS LICENSE AGREEMENT, KANTECH'S ENTIRE LIABILITY UNDER ANY PROVISION OF THIS LICENSE AGREEMENT SHALL BE LIMITED TO THE GREATER OF THE AMOUNT ACTUALLY PAID BY YOU TO LICENSE THE SOFTWARE PRODUCT AND FIVE CANADIAN DOLLARS (USD$5.00). BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

(d) DISCLAIMER OF WARRANTIES

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

(e) EXCLUSIVE REMEDY AND LIMITATION OF WARRANTY

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

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

Please click on the "I agree" button if You agree to terms of this End User License Agreement. If You do not agree to the terms of this EULA, press the "I Do Not Agree" button as Kantech is unwilling to license the SOFTWARE PRODUCT to You, and You have no right to use it.

TABLE OF CONTENTS

SECTION 1

Introduction to WinPass

Designed for installations of up to 64 card readers, WinPass bundles all the basic functions of access control in an easy to learn and understand structure. Learning time is reduced to a minimum. Familiar Windows screens are intuitive; on-line context sensitive help is always available throughout the system.

Up to 8,000 card users can be defined in the system. Each card user is assigned an access level that will allow entry at selected doors, only according to predefined schedules. All events are recorded by the system for future review.

Once the system is configured, the computer is required only to monitor/update the system or to print reports. The report generator can provide information sorted and printed according to your needs or displayed using clear graphics.

Important Information

If you are using KT-200 controllers and more information applies to the KT-200 controller on a specific subject, the phrase "**SEE SECTION 11 IF YOU ARE USING KT-200 CONTROLLERS**" will be displayed within the subject under the specific paragraph or picture.

The paragraph which has more information about the KT-200 will be identified with an asterisk (*). For example: if a subject has several paragraphs in which some specifications apply to the KT-200, then only the subject title and the specific section applying to the KT-200 will be available in Section 11.

Unique Features

Distributed data and true stand-alone capability:

Memory and processing located at every door. No degraded mode. The computer never makes a decision and is necessary only for maintaining the system's database or downloading buffered events in order to prepare reports.

Compatible with multiple reader technologies:

IoProx , Polaris mag stripe, ShadowProx proximity, XSF, Wiegand, bar code, biometrics, keypads and many others.

Automatic functions:

Unlock doors, activate relays and outputs, monitor inputs, according to schedules or system events.

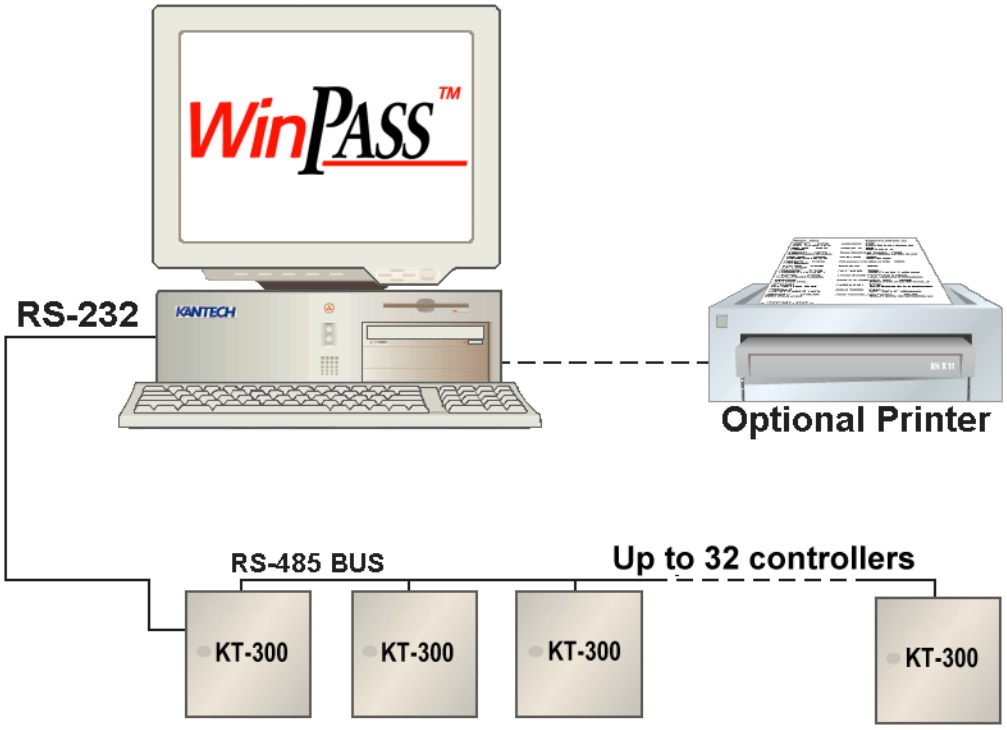
Cards can be added or deleted in seconds ; all events are buffered and can be saved on disk or printed for future reference. WinPass provides an easy-to-use report generator.

The report generator lets the user print or view the desired information from all the events saved to the computer's hard disk.

Compatible with 2 types of controllers:

For more flexibility and options, WinPass offers the possibility to use 2 types of controllers: KT-200 and KT-300, However **both types cannot** be installed on the same system.

WinPass Architecture (RS-232)



"SEE SECTION 11 IF YOU ARE USING KT-200 CONTROLLERS"

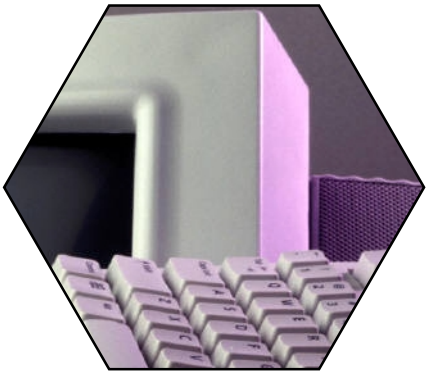
System Specifications

Features	Specifications
Number of cards (8 digits) using KT-300/128k	8,000 on-line / off-line
Number of cards (16 digits) using KT-300/128k	8,000 on-line and 4,000 off-line
Number of cards (8 and 16 digits) using KT-300/512k	8,000 on-line / off-line
Card families or site codes	No limit
Door controllers KT-300	32
Card readers	64
Keypads	64
Monitored inputs (with optional KT-PC4108)	256 (512)
Door lock outputs	64
Controlled Outputs (with optional KT-PC4216 or KT-PC4204)	64 (512)
LCD Keypad KT-LCD4501	64
Auxiliary outputs for reader LEDs and door alarms	128
Card user access levels	250
Schedules of 4 time zones each	100
Holidays	366
Operator workstations	1
System operator passwords	No limit
Operator security levels	1 fixed / 8 prog.
Concurrent operator languages	2
Number of printers	Windows limit
Number of events (buffer) using KT-300/128k (512k)	+ - 5,000 (+ - 18,000)

"SEE SECTION 11 IF YOU ARE USING KT-200 CONTROLLERS"

Part Numbers and Contents

Part Numbers	Description
WPASS-64	WinPass software and user manual with CBLK-10 cable 30 meters (100')
CBLK-10	30 meters (100') Cable/connector communicating in RS-232 protocol from host PC to master controller
W-PASS-64/REV	WinPass software upgrade
VC-485	Multi-function communication interface to be used as a communication line extender (to extend distance between host PC and master controller)



SECTION 2

WinPass Utilities

Within this section, you'll find:

1) Computer requirements for installation: indicates the minimum system requirements for the installation of the WinPass software.
2) The WinPass installation procedure: explains the software installation procedure.
3) How to use ExpressSetUp program: explains the procedure to use the ExpressSetUp program to define system components.
4) The login procedure: explains how to login to the WinPass software.
5) How to perform a backup: explains how to perform a backup of the system tables.
6) How to uninstall WinPass: explains the procedure to uninstall the WinPass software from your computer.

Computer Requirements

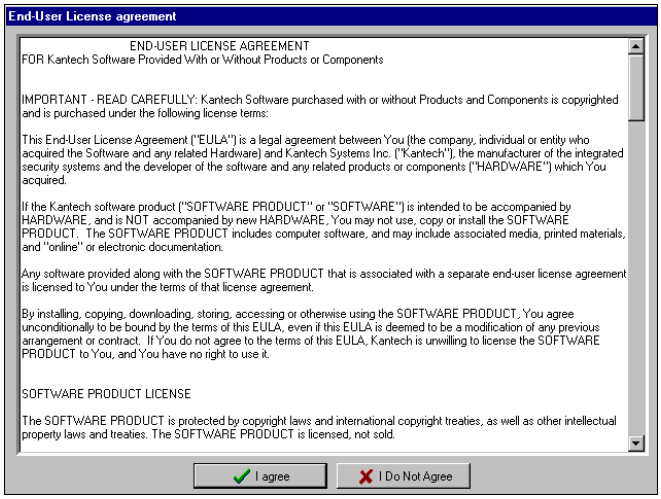
- Pentium 90 MHz processor or faster
- 32 MB RAM recommended
- Hard drive with 20 MB free disk space for software installation
- 900,000 events archived per 30 MB of disk space
- Windows 98 operating system
- VGA Monitor
- Dedicated computer not necessary *(computer necessary only for configuration and reporting, computer not required for operation).*

Software Installation

1) Insert diskette #1 in drive A:,

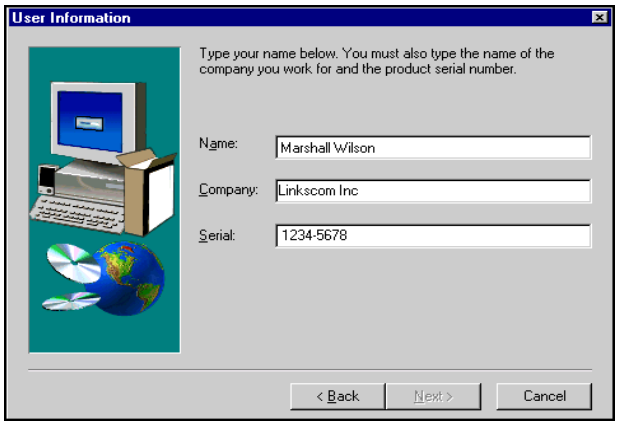
2) From the Windows Taskbar, click on Start and then select Run. The system will display:

3) From the Run window, type A:\setup and click on OK. The system will display the end-user license agreement. Read this license completely,



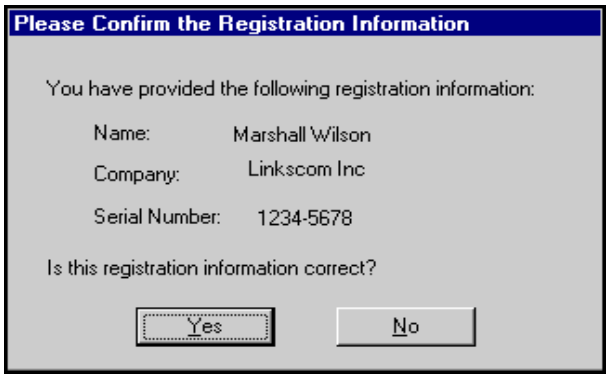
4) To activate the "I agree" button, scroll to the end of the display. Click on "I agree" to continue the installation or "I do not agree" to cancel the installation,

5) The WinPass installation procedure will start and ask to provide registration information such as the site name, the company name and the product serial number (can be found on diskette #1),



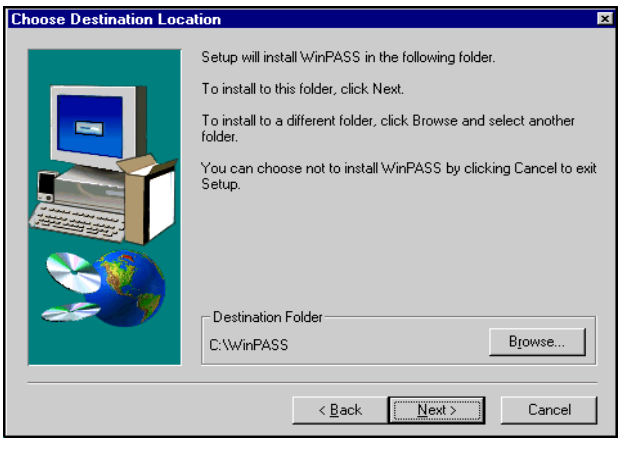
Note: *To stop or cancel the installation, click on Cancel at any time during installation.*

6) You will be asked to confirm the registration information entered in Step 5,



7) Click on Yes to continue or No to modify the information,

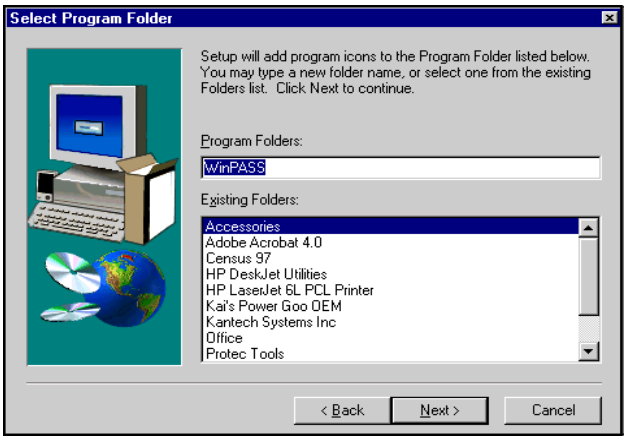
8) You will be asked to confirm the installation path,



9) Click on Next to install WinPass in the displayed folder or click on Browse to select another folder,

10) The setup will check your computer for the minimum system requirements and a warning message will be displayed if your computer does not meet these requirements,

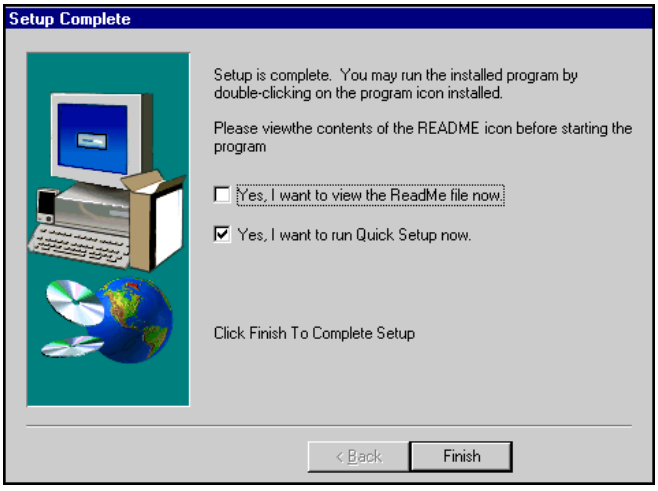
11) You will be asked to confirm the program folder,



12) Click on Next to continue, or type a new folder name or select one from the displayed list,

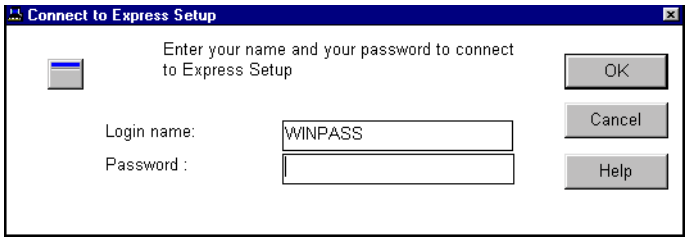
13) Once the setup is complete, you will be prompted to view the ReadMe file and run ExpressSetUp. Make your selections (it is recommended to view the ReadMe file and run ExpressSetUp before starting the program), click on Finish to complete the installation.

WinPass is now installed on your computer. To save installation and configuration time, **we strongly recommend that you use ExpressSetUp** so that the system is fully functional and ready to test the hardware and wiring.

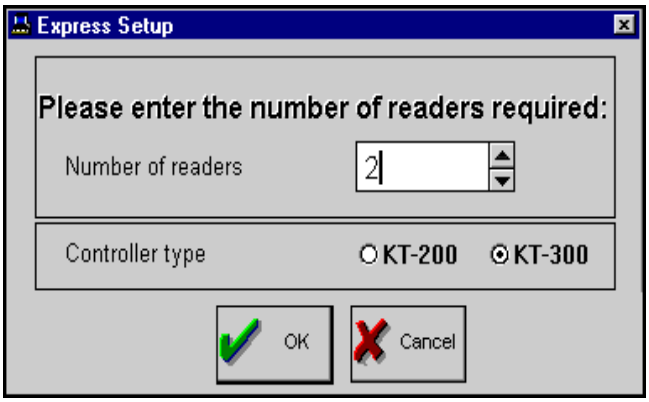


Using ExpressSetUp

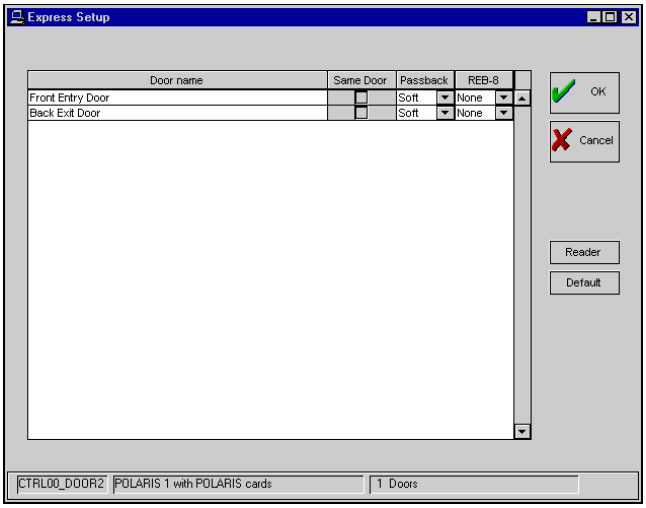
ExpressSetUp configures the system. Usually, if you do not require special options, the system will be ready to be used after you define the schedules, user access levels and cards.



1) When you use ExpressSetUp, the system will display the login window. Enter your login name and password **(default**: WINPASS (not case sensitive) and click on OK to continue,

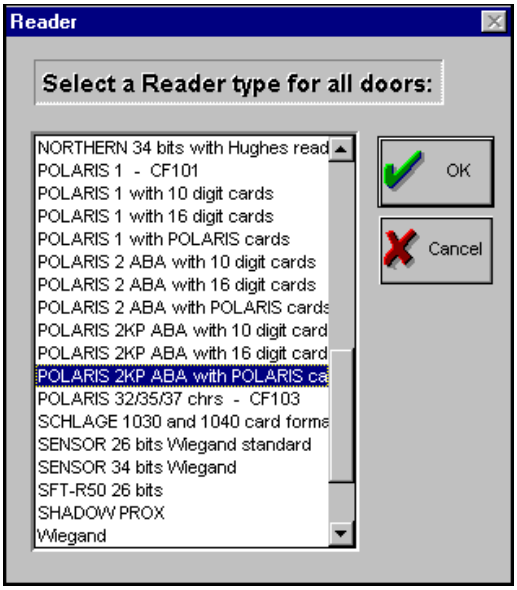


2) Enter the number of readers required and specify the controller type and click on OK to continue,

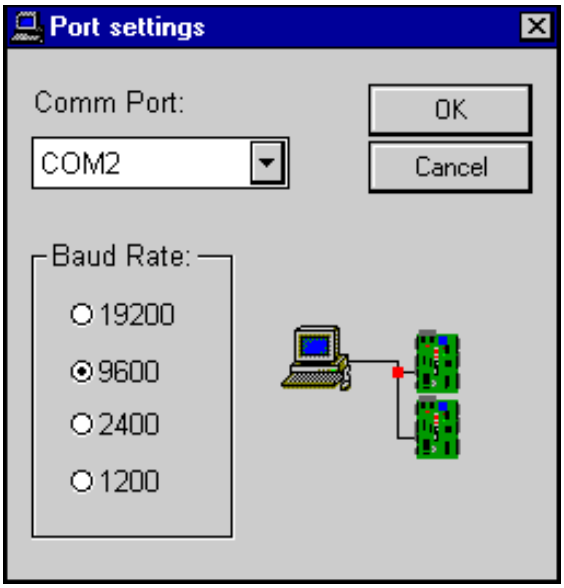


3) You can modify the door names. Select (check box) the doors (readers) on which Anti-Passback is required (see Controller Definition Section for more on Anti-Passback). Specify the type of Anti-Passback (soft or hard). Click on OK to continue the installation, *

"SEE SECTION 11 IF YOU ARE USING KT-200 CONTROLLERS"



4) By default, the reader type is Polaris 2 with Polaris cards, to select a different reader, click on the requested reader type and click on OK to continue the installation. Some readers offer the possibility the 16-digit card driver format,



5) Select the COM port and baud rate and click on OK to continue the installation. The default settings are COM Port 2 and 9600 baud rate.

   Note: The KT-300 controller selects its communication speed automatically. It can go up to 115,200 baud.

6) Once you have entered the baud rate, the system will display the following question:

ExpressSetUp may be used at the initial installation or you may run ExpressSetUp later. Whether it is the first time or not, the following warning message will appear: *This operation will modify all controllers' data. Do you want to continue?*

Click on YES if this is a first installation.

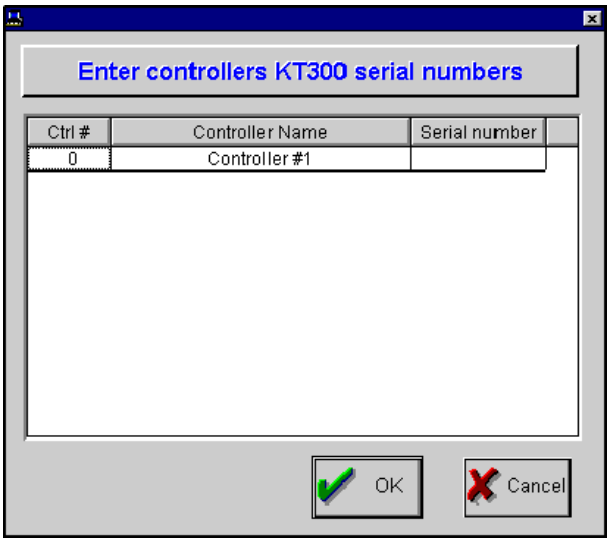
Warning: If you are running ExpressSetUp once the system is configured, the controller configurations including the Anti-Passback option, REB-8, number of readers, reader types and communication ports will be set to default. Other information contained in the database (event tables) and user (cards) information will not be modified.

ExpressSetUp associates the door contact for the first door of a controller to input 1 and the second door contact to input 3. The request-to-exit button or detector (REX) is associated to input 2 for door 1 and to input 4 for door 2. *

"SEE SECTION 11 IF YOU ARE USING KT-200 CONTROLLERS"

After answering the question, the system will define the necessary door controllers, the readers, the door contacts, the request-to-exit detectors, etc. so you have a working system.

7) Once the system has finished the installation, the following screen will be displayed:



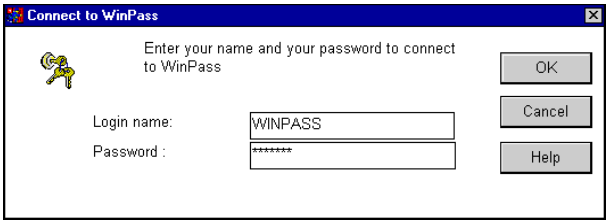
8) Click on "serial number" button and enter the serial number of the KT-300 controller (8 digits). The serial number allows communication between controllers and the computer. Click on OK to continue the installation.

Login the System

This section describes the login procedure.

1) Click on the login button 

, the system will display:



2) Enter "WINPASS" as login name,

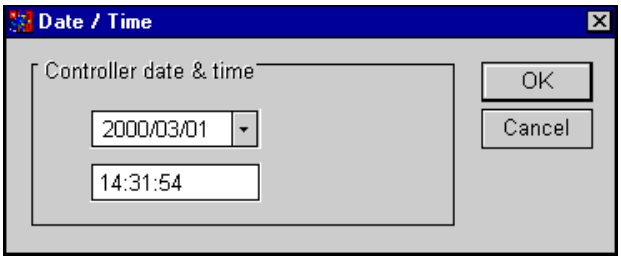
3) Enter "WINPASS" as password,

4) Click on the OK button.

***Note**: Remember to change this default password once the system*

is functional.

Once registered, you will be prompted to confirm the date and time in order to synchronize the date and time between the controllers and the computer.



The system should now be functional. Should communication problems be present, click on Configure Workstation (see Workstation Configuration in section 5) to verify the COM port and baud rate settings *.

"SEE SECTION 11 IF YOU ARE USING KT-200 CONTROLLERS"

Uninstalling WinPass

This section describes the procedure to remove the WinPass software from your computer.

From the Control Panel, select Add/Remove Programs, select WinPass and click on Add/Remove. Once the procedure is completed, a screen will be displayed informing you that the removal is completed but some files must be removed manually from your hard drive. To remove these files, you must:

1) Click on My Computer,
2) Select C\: drive or the other drive where WinPass was installed,
3) Select the WinPass directory,
4) Click on file and select Delete,
5) Winpass folder and directory will now be removed.

Warning: This option will delete all events and data.

1) Click on My Computer,
2) Select C\: drive,
3) Select Windows folder,
4) Delete the file named "winpass.ini".

Note: If you are having trouble locating the file, you may find it quickly by using Windows Explorer's find feature.

Backup Procedure

Performing a regular file backup safeguards them against loss if your hard disk fails or you accidentally overwrite or delete data.

Depending on what and how you want to backup your files, there are several options offered with Windows. Some of the available options are as follows:

1) Backing up selected files and folders,
2) Defining a set of files to be backed up,
3) Backing up a predefined set of files,
4) Backing up only files that have changed,
5) Backing up files quickly using drag and drop.

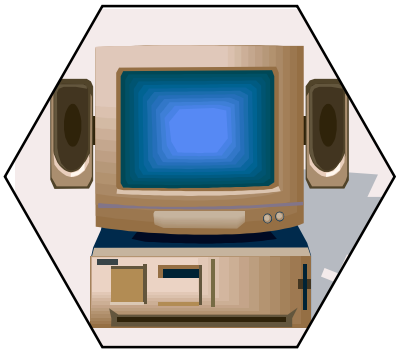
Below are the instructions for backing up selected files and folders (option 1). The instructions for the other options may be found in the Windows Help menu.

From the Taskbar, click on Start and select Programs. Point to Accessories and then from System Tools, click on Backup.

1) Click the Backup tab,
2) Click the plus sign (+) next to the drive that contains the folders or files you want to backup,
3) To select all the files in the folder, click the box next to it. To select only certain files, click the icon for the folder that contains the files, and then click the box next to each file on the right side of the window,
4) Click Next Step, click the destination where you want the backed up files to be stored, and then click Start Backup,
5) Enter a name for the backup set.

Upgrade Procedure

To upgrade your system, follow the installation procedure.



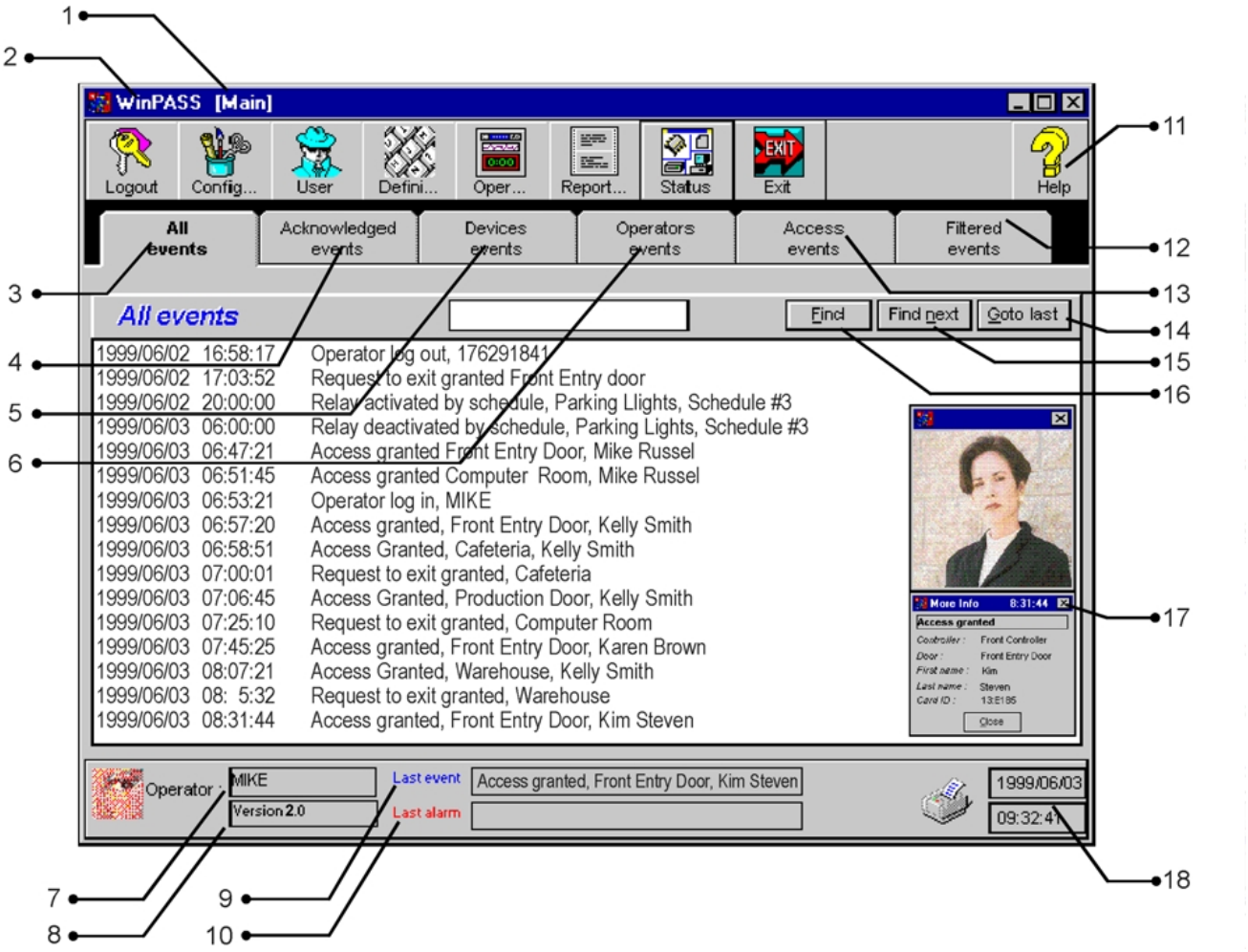
SECTION 3

WinPass Basics

Within this section, you will find:

1) The complete description of all the features contained in the main menu of the WinPass software,
2) A complete description of all the toolbars included in the WinPass software,
3) A complete description of all the common buttons (file tools) used throughout the system,
4) A preview of the system's features and capacities

Main Menu



1) Active menu or Sub-menu:

The description in brackets [***Main***,] indicates the active menu.

2) WinPass:

The first caption is the program name.

3) All events TAB:

This tab lists all the system events as defined in each of the event's display schedule.

4) Acknowledged events TAB:

This tab contains all the events which have been acknowledged by the operator. For example: "Door forced open" event has been defined to be acknowledged by the operator. This option is set under the event definition menu.

5) Devices events TAB:

This tab contains all events related to components such as: controllers, doors, relays, inputs and outputs.

6) Operator events TAB:

This tab contains events generated by the operator's activities such as: programmation, manual modifications, relay activation, reader disable, etc.

7) Operator:

Displays the name of the operator currently logged on.

8) Version:

Displays the version of the software.

9) Last event:

Displays the last recorded event.

10) Last alarm:

Displays the last acknowledged alarm event.

11) On-line help:

The HELP button provides context-sensitive help. For example, by clicking on HELP in Door Definition, the help topics provided will be related to the Door Definition menu.

12) Filtered events TAB:

This tab contains all the events which match the character string found at the top of that table.

13) Access events TAB

This tab contains all the events generated during door access by users.

14) Go to last:

This option repositions the cursor on the most recent event in the current table (tab). It also activates the automatic positioning. Since this requires use of a background task, the tables are momentarily locked during this operation and cannot be accessed.

It is possible to view the search progress on the taskbar 30% and in the progress window.

15) Find next:

This option allows you to search using the Find option from the actual cursor position (see Find option).

16) Find:

This option allows you to search events tables using one or more keywords. The system searches from the most recent to the oldest event. The tables will be locked during a search and cannot be accessed during this period, because the system is using a background task to complete the search.

It is possible to view the search progress on the taskbar or in the progress window.

17) More info:

By double-clicking on an event, you can view additional details concerning that event. For instance, in an access event, an additional screen displaying the cardholder's picture (if pictures are assigned in User Definition) is displayed. The "More Info" button is refreshed each time a new event is generated.

18) Date and time:

This section displays the system's date and time.

Toolbar Menus

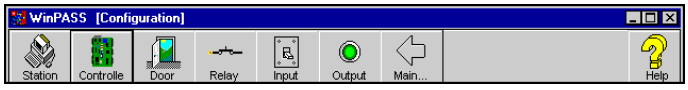
Toolbar menus are used throughout the system to perform various actions or operations in the system.

The Main toolbar:

After operator login, the main menu bar provides access to the sub-menus and enables the operator to access help, logout or exit the system.

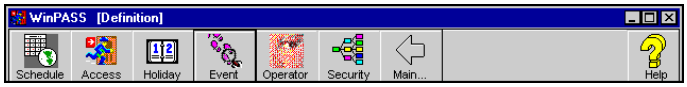
The Configuration toolbar

Lets you define how the components work and relate to each other. You can define workstations, controllers, doors, relays, inputs and auxiliary outputs.



The Definition toolbar

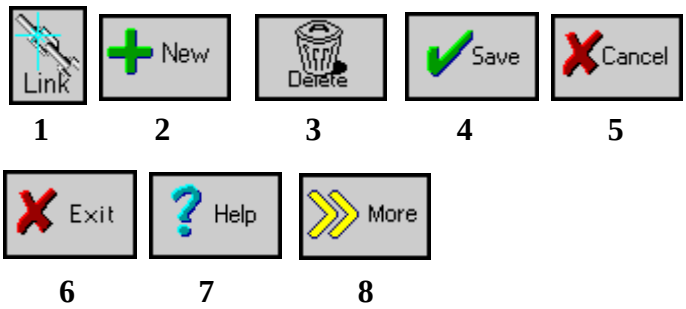
Lets you define schedules, access levels, holidays, event display and color, system operator password and operator security levels.



Operation toolbar

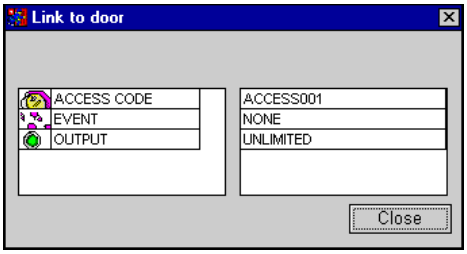
Lets you perform manual operations on doors, relays, inputs and outputs. You can also view the various components status, create a card list, reload controllers, change the date and time of your system and re-index the tables.

File Tools (buttons)



1) The LINK button:

This option is used to display the relationships between the component being edited and other components of the system. When used, it will display a screen containing two windows, the first one representing the category and the second one representing a component. By clicking on a category, you can view all components which are linked and may be affected by editing the selected record.



2) The NEW button:

This option is used to add a record to file. It will clear the actual screen and leave a blank new page for the new information. Once saved, the system controllers will be updated with the new information.

3) The DELETE button:

This option is used to remove a record from the database. Once this option is activated, WinPass verifies the links between the components, will warn the operator of these links and will require a confirmation. Once the deletion is confirmed, the system controllers will be updated as necessary.

4) The SAVE button:

This option is used after a new record has been created or after a record has been modified. Once pressed, the system controllers

are updated with the necessary changes.

5) The CANCEL button:

This option is used to cancel all changes made to a record since the last SAVE. After pressing CANCEL, the system will prompt the operator to confirm: **Do you want to save?** Click NO and none of the changes will be kept on records.

6) The EXIT button:

This option is used to close the current window.

7) The HELP button:

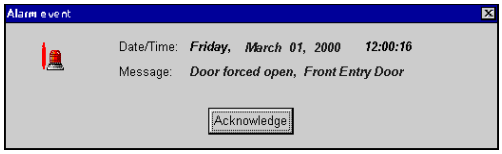
This option is used to provide the operator context-sensitive help.

8) The MORE button:

This option (if displayed) is used to view additional configuration parameters of a selected component.

Operator Acknowledgment

Operators can be required to acknowledge certain events such as alarms or card trace type of events. Events that require operator acknowledgment have to be defined under the Event Definition menu. When the operator is required to acknowledge an event, the computer's audible warning will sound and an alarm screen will be displayed on-screen:



The alarm event description will be displayed with time and date and the associated device. From the "Event Definition" menu, select all events which will require operator acknowledgement. The "Acknowledged Events" tab stores events that have been previously acknowledged by an operator.

Customizing the System

Follow this sequence to customize WinPass:

1) Define Controllers
2) Define Schedules
3) Define Doors
4) Define Relays
5) Define Inputs - Outputs
6) Define Access Levels
7) Define Cards
8) Define (operator) Security Levels
9) Define Operators
10) Define Holidays
11) Define Events

Defining Controllers

WinPass is designed to communicate with the door controllers via one of the 4 host COM ports.* The controllers are identified by their serial number *(refer to controller definition in section 5).*

"SEE SECTION 11 IF YOU ARE USING KT-200 CONTROLLERS"

Defining Schedules

It is possible to use the same schedule for different uses, but it is recommended to create a distinct schedule for each requirement. It is then much easier to modify a particular application's schedule without affecting other applications *(refer to schedule definition, in section 6).*

Defining Doors

Properly defining access doors when designing an effective access control system plays a crucial role in the system's integrity. Door types such as entry, exit, access, and the individual door schedules will be found in "Door Definition". All door timings including door open times, door unlock times, door contact inputs will also be found in "Door Definition".

KT-300 Door Programming Relays

Each KT-300 door controller is equipped with two open collector outputs. These controlled outputs are not to be confused with the door strike outputs. The controlled outputs may be programmed to activate or deactivate to follow certain inputs. Also, the activation/deactivation times may be user defined and schedules may be defined for individual relays. * If relays are required, see the system specifications of section 1.

SEE SECTION 11 IF YOU ARE USING KT-200 CONTROLLERS

Monitoring Inputs

WinPass may control 8 inputs per KT-300. When an expansion module is added inputs are increased to 16.* If additional inputs are required, see the system specifications in section 1.

SEE SECTION 11 IF YOU ARE USING KT-200 CONTROLLERS

Programming Outputs

In addition to having two form "C" controlled outputs on each KT-300, four open-collector auxiliary outputs have also been provided. These outputs are typically used to activate the reader's LED on an access granted and the piezo alarm buzzer on a T.REX request-to-exit detector door alarm *(please refer to output definition in section 5).**

SEE SECTION 11 IF YOU ARE USING KT-200 CONTROLLERS

Access Levels

Up to 250 access levels may be defined in WinPass. Access levels determine to which doors and at what time cardholders will have access. For example, office employees may have access at door 1 "Front door" only from 7:00AM to 5:00PM on weekdays *(please refer to access level definition in section 6).*

Defining Cards

WinPass will control a maximum of 8,000 cards per system (see System Specifications for more details on cards and controller types). Cards may be easily programmed in "Card definition". All user definable fields, PIN codes, access levels, valid card times will be found in "Card Definition" *(please refer to Card Definition in section 4).*

Security Levels

Operators in "Operator definition" must be assigned a security level. This security level determines which menus the operator will have access to and what level of database functions the operator will use (ex. View, Modify, Delete or Print). There are 8 programmable security levels and one (1) pre-defined *(please refer to security level definition in section 6).*

Holidays

Up to 366 holidays may be defined in WinPass. Each holiday may be defined in 1 of 4 classes (HO1-HO4). Once a holiday has been defined, the holiday is selected in the "Schedule Definition" to permit different valid access times during each holiday type *(please refer to holiday definition in section 6).*

Defining Events

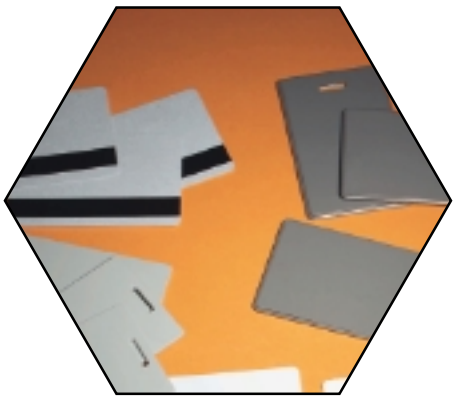
The term "Event" is used to describe activities or alarms detected or generated by the system. There are many different system events such as Access granted, Input in alarm, Card modified by operator, etc.

The Event Definition capacity is a powerful feature of the system. For each event, it is possible to determine how the event should be displayed or printed. These dispatches can also be limited by schedules that will allow, for example, to print or display some events only during a particular period of time such as after regular hours.

Each event related to a device can be individually associated to a corresponding set of actions such as display, acknowledge or print.

For example: the "Door open to long" event is defined for each individual door of the system. This also permits a different action or response on a door to door basis.

Critical alarm events should be set to require an acknowledgment from the operator *(please refer to event definition in section 6).*



SECTION 4

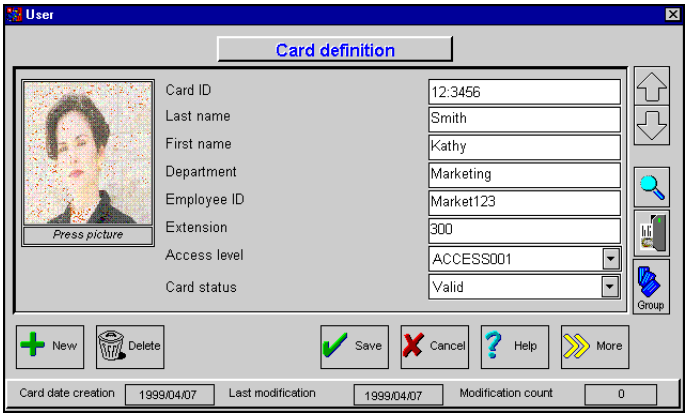
Defining System Users

This section is used to create new cards in the system. When creating cards, you can use the Group feature to define multiple cards at a time, you can also use the Assign Picture feature to assign pictures to cardholders ; these pictures will be displayed on the Event Monitoring screen when the cardholder presents its card at a reader.

Card Definition

This screen is used to define new cards, modify or delete existing cards, assign pictures to cardholders, define multiple cards (group feature) and obtain a card ID number.

A card number usually consists of two elements: the family or site code and the card's own identification number. The card family code usually has a hexadecimal value between 00 and FF. The card's identification number is usually in decimal format. When entering the card number, type all preceding zero(s) for numbers shorter than 5 digits. Decimal format range is between 00000 and 65535.

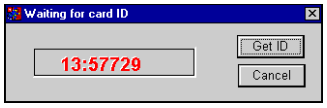


You can use the "up/down arrows" feature - (if you want to scroll through the defined cards to select one), or you can use the "More" feature to specify additional information such as: trace the card, if the user must use a pin number at the keypad, etc. (lets you enter more information concerning a cardholder).

"Get Card ID" button

You can use the "Get Card ID" button (if you want to define a card but don't know its number). To define many cards, use the Group feature.

To use this feature, click on the "New" button, the sytem will display a blank new screen. Swipe the card at a reader connected to the controller. The card number will be displayed:



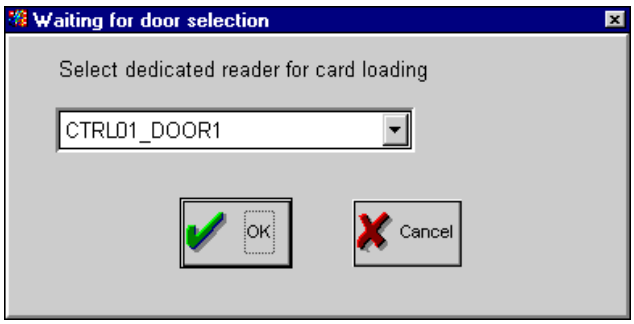
Click the "GET ID" button to return to the card definition screen so you may continue to enter the information in the fields.

Note: Only non-existant card numbers will be captured.

"Group" button

You can use the "Group" feature to select a reader at which cards will be passed (if you have many cards to be defined):

1) Click on the GROUP button, the system will display:



2) Select a dedicated reader. It allows you to select a reader with which cards will be attributed in the system.
3) As you swipe a card, you can enter the user's definition in the fields.
4) You can proceed with step 3 as often as needed.
5) When you are done, press the CLOSE button and the system will automatically save all the cards you have previously entered.

Field Definition

Last name / First name

Enter the cardholder's name, up to 30 characters for each or less. It is recommended not to use commas as field separators for importing purposes.

User definable 1, 2 & 3

These user definable fields are 30 characters long and can be used to store additional information regarding the cardholder. Common use for these fields are: employee number, department, address, telephone number, etc...

Access level

Select an access level to which the user will be assigned. Access levels are usually defined before entering a new card. The access levels determine which doors according to a specified schedule the cardholder will be permitted access to.

Card status

The usual setting is "valid". Setting the card status to invalid, lost, stolen, status #4 or status #5 , will disable the card and the system will deny access to this card. The system will also generate the appropriate event such as "access denied-invalid", "lost", etc.

When a card is lost, it is better to set it to "lost" than deleting the card from the system. This way, all the data concerning the user can be kept within the system and if anyone ever attempts to use the card, the card will be denied access and the event will identify the actual card's previous owner. The system automatically sets card status to "expired" or "pending" according to the card's validity dates.

Picture selection

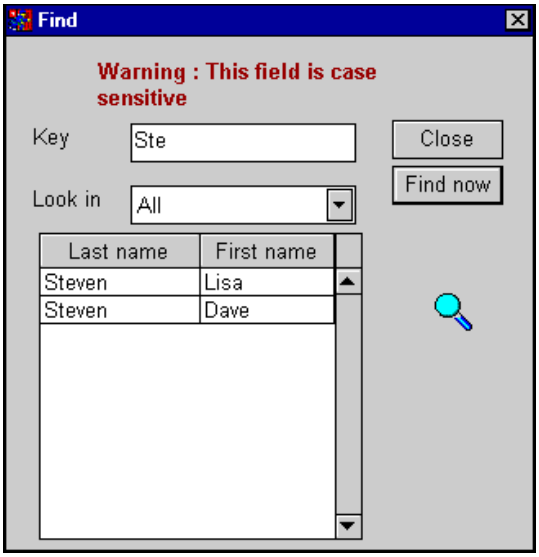
This feature lets you assign a picture to the cardholder. Follow these steps to assign a picture:

1) Double-click on the picture area,
2) Select a picture from the pick list,
3) Click on the ARROW button to return to the card definition screen.

Note: By default, all pictures must be selected from the \WinPASS\picture directory. This path may be modified by specifying the location of the picture files in the workstation configuration menu option.

Find button (search a cardholder)

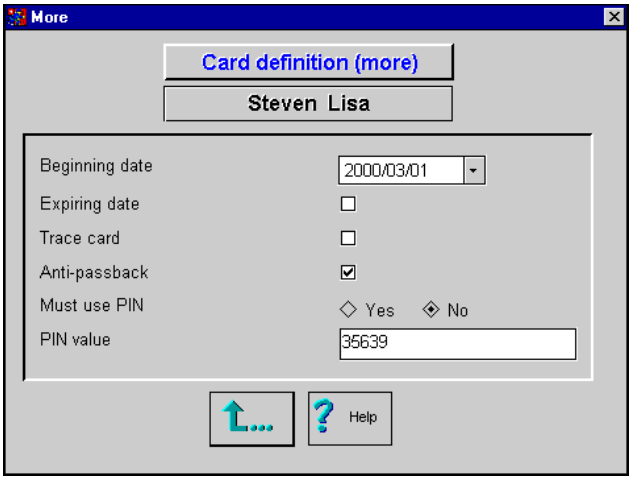
1) From the Card Definition screen, click on the Find button,



2) Enter a keyword(s) to search in the KEY field (case sensitive),
3) Click on the Find Now button to initiate the search,
4) Once the search is done, WinPass will display the user's profile. If no match was found, the current profile will be displayed.

"More" button

This button opens an additional screen. From the displayed screen, you can select various options.



Field Definition

Beginning date / Expiring date

Period of time during which the card will be valid. WinPass will, by default, set each new card to be valid (effective immediately). If there is a date entered in the expiring fields, the expiry date must be greater than the beginning date.

Trace Card

When selected, this parameter will generate a "Card traced" event each time the card is used. This is useful to keep track of a particular card.

Anti-Passback

Determines whether Anti-Passback control will be enforced for that cardholder.

Must use PIN

Setting this value to YES means that the user must enter a PIN number after a valid swipe in order to be granted access to a door equipped with a keypad.

PIN Value

Every time a new user is entered, the system will automatically generate a PIN number automatically. You may modify the PIN number by entering a number with 5 digits from 00000 to 65535.

Click on the up arrow to return to the Card Definition menu.

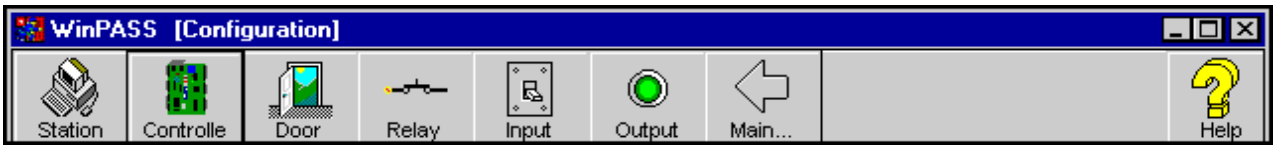
SECTION 5

Physical Components Configuration

This section is used to configure the physical components of the WinPass system. It is used to define:

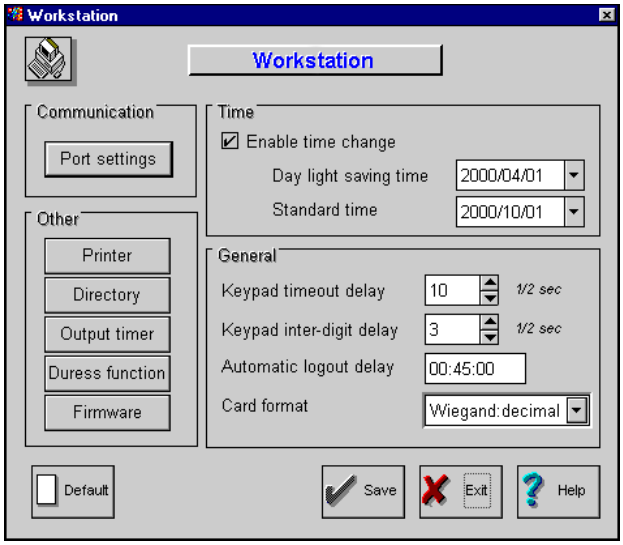
1) The workstation parameters: card format, port settings, log printer, duress function, time changes, keypad delays, etc.,
2) The controller parameters: type, serial number, reader/keypad type, Anti-Passback, assign expansion modules, set dip switches, communication port, tamper & AC schedules, etc.,
3) The door parameters: door type (entry/exit), reader or keypad, locked state, unlock schedule, keypad schedule, activate relays on door events, interlock schedule, REX schedule, etc.,
4) The relay parameters: normal state, activating schedule, activation period, etc.,
5) The input parameters: normal condition, shunt delay, relay activated by input, monitoring schedule, etc.,
6) The output parameters: normal state, flash time, select how events will trigger the outputs, etc.

THE CONFIGURATION MENU TOOLBAR



Workstation Configuration

This feature is used to define the workstation's parameters.



Field Definition

Time:

Enable time change

Click here to activate the time change mode. Set the dates for automatic time change.

Daylight savings time

The Daylight savings time date change can be entered here and the system will automatically, at 2:00 am, advance the time to 3:00 am on the first Sunday of April.

Standard time

The Standard time date change can be entered here and the system will automatically, at 2:00 am, set back the time to 1:00 am on the last Sunday of October.

Note : It is very important to enter the correct year.

General:

Keypad time-out delay

The keypad time-out delay is set in seconds for a maximum of 127 seconds which represents the time allowed for a user to begin entering his or her personal identification number (PIN) at a keypad.

Keypad inter-digit delay

The keypad inter-digit delay is set in seconds, up to two minutes. It represents the maximum delay permitted between each selection of a keypad key by a user.

Automatic logout delay

The Automatic logout delay is the predetermined time set after which the system automatically logs out the operator who is inactive. The time is entered in hours, minutes and seconds. This feature provides additional security to prevent access to the system by an unauthorized person.

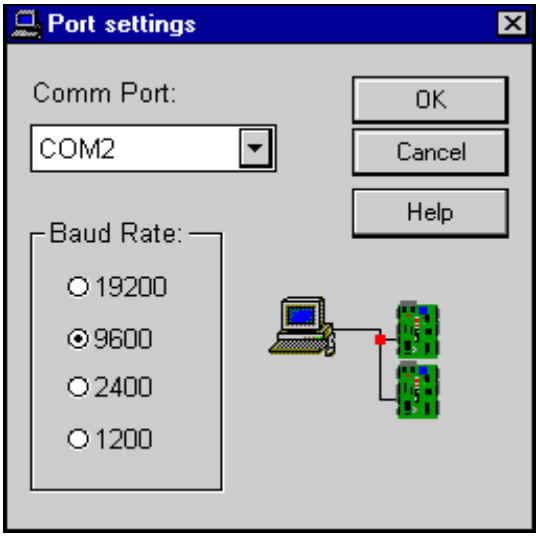
Card format

The card format setting determines how the card numbers will be represented throughout WinPass. Usually displays 8 digits, but some readers offer the 16-digit format.

Buttons

"Port Settings" button

Select the baud rate speed that will be used to poll the door controllers. There are four choices: 1200, 2400, 9600 and 19200. Setting a lower poll rate on the controllers may correct some communication problems due to induction or faulty cabling.



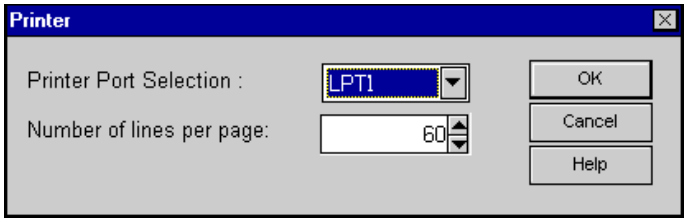
***Note**: To select the COM port on which the controllers are connected to the host computer, refer to Section 5 under controller definition menu under "More" button.*

***Note**: When selecting the baud rate in the software, the KT-300 will automatically adjust to the selected rate.**

"SEE SECTION 11 IF YOU ARE USING KT-200 CONTROLLERS"

"Printer" button

This printer is used to print events as they occur and recorded by the system. This is normally used to print events which are of high importance. The events to print must be defined with a printing schedule (see Section 6 - Event Definition). You cannot use a Network printer as a log printer.



Field Definition

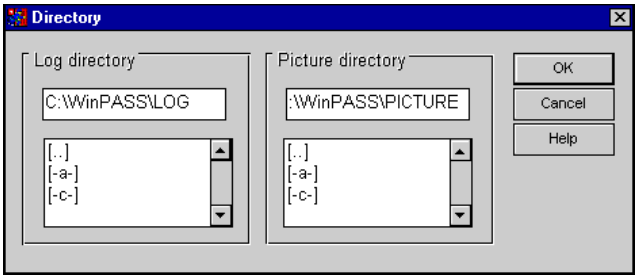
Printer Port Selection

Select the LPT Port to which your printer is connected. The default setting is LPT2.

Number of lines per page

This option is used by the "Log Printer" only. It is used to determine the number of events to be printed on a page and/or page breaks. The default value is 60.

"Directory" button



Field Definition

Log directory

This field allows you to select the directory in which the daily event files of the system will be stored. Events are saved in a daily file on disk and labeled according to the following format: YYYYMMDD representing the date (i.e: 20000301.dbf, for March 1st, 2000 events).

Picture directory

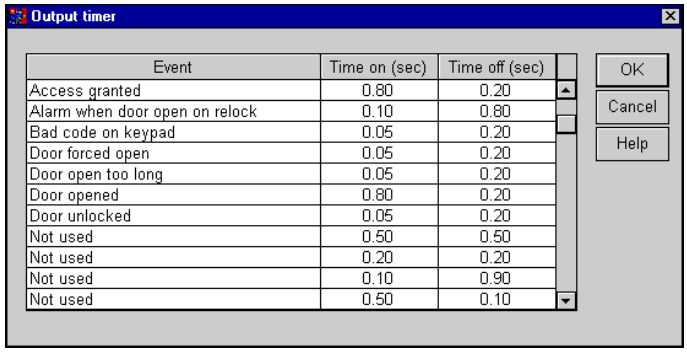
This field allows you to select the directory in which the photo files (bmp, gif, pcx, tif, etc.) will be selected from when assigning pictures to cardholders in the card definition menu. The default directory is C:\WINPASS\PICTURE.

"Output timer" button

A list of events is provided by the system. These events control the time from which the auxiliary outputs (LED & BUZ = light and buzzer) for the door readers will remain ON or OFF (toggle). Select the delays at which the output will remain on then go off when its associated event occurs.

See "Output Definition" menu -- Section 5 to set the status (steady, flash, steady timed, flash timed and none) of the outputs.

Enter the ON/OFF flash time of the outputs that are programmed in the auxiliary output definition relative to each event.



"Duress function" button

The manual activation of a silent alarm by entering at the keypad/reader a code different from the normal arm/disarm code. The duress feature has to be implemented on an integrated reader/keypad.

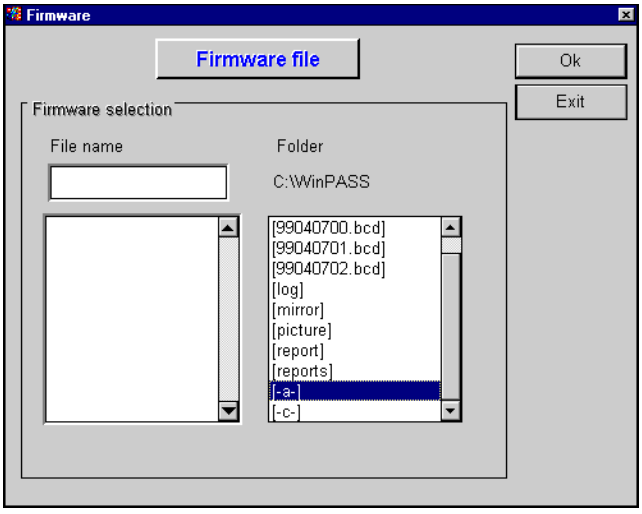
The chosen code will have to be entered after the NIP once the access is granted or access denied or both (according to the duress option chosen) in order to produce either a silent alarm which is designed to allow a person to call for help without arousing suspicion.

A choice of using the function on access granted or access denied or both will be offered. Select which code is to be used from 0 to 9 and #.

Note: *"*" is not available with POL/-2KP because there are 2 wires contact for the "*" button.*

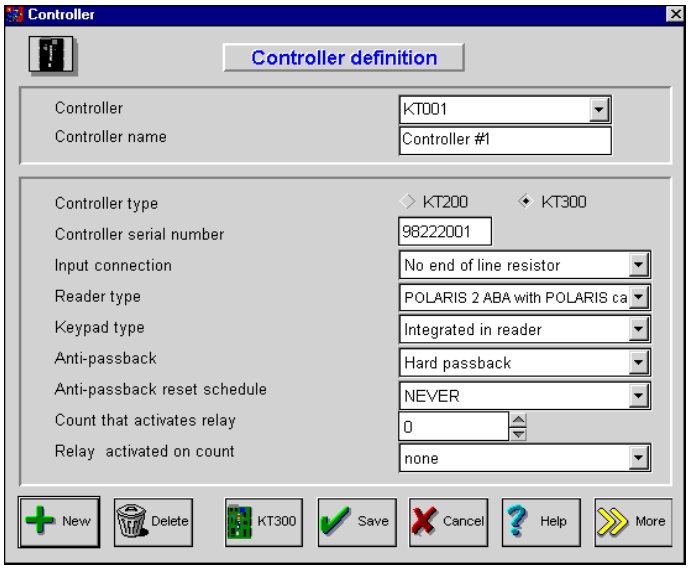
"Firmware" button

This button is used to select the directory in which the firmware file for the KT-300 is located. To update the controller's firmware, use the Reload function from the Operation menu.



Controller Definition

This feature is used to define the controllers (reader type, keypad type, controller type, etc).



Field Definition

Controller

Enter the controller's identification label or click on the pick list.

The controller label is composed of 12 alphanumeric characters or less. It is used to identify a controller in the system. For example, the label may be used to select a specific controller when defining doors.

Controller name

Enter the name or the location of the controller. The controller name is composed of 30 alphanumeric characters or less and provides detailed information concerning the controller.

Controller type

Select which controller type will be used with WinPass. A system cannot be defined using two different types of controllers.

Controller serial number

You must enter the serial number of the controller (located on the bottom left portion of the controller). Without this number, the controller will not communicate with the computer.

Input connection

Select if the controller will be used with:

- No end-of-line resistor
- Simple end-of-line resistor, or
- Double end-of-line resistor.*

"SEE SECTION 11 IF YOU ARE USING KT-200 CONTROLLERS"

Reader type

Select the reader type used with the controller. Click on the pick list for a list of available readers.

Keypad type

Select the keypad type used with the controller. Click on the pick list for a list of available keypads.

Anti-Passback

Select the type of Anti-Passback used: NONE, SOFT, or HARD Anti-Passback.

Purpose:

Anti-Passback allows you to prevent tailgating by cardholders thus increasing the level of security. Only cards programmed with the Anti-Passback option set to "yes" are monitored for Anti-Passback violations. It keeps track of the number of monitored cardholders in an area defined by corresponding ENTRY/EXIT readers.

You can verify the status (ENTRY/EXIT) of monitored cards according to their last use in the *Card List* option. A relay can be activated when a certain number of monitored cards are located inside the area; the relay deactivates when the number of cards in the area drops below the selected count.

Hard Passback:

A card used at an ENTRY reader will not be able to access the same ENTRY reader again until it has used the corresponding EXIT reader and vice versa.

Soft Passback:

Allows the person to use an ENTRY (or EXIT) reader more than one time even though the corresponding EXIT (or ENTRY) reader was not used. Each entry/exit granted event that is out of sequence will generate a passback fault event but will allow the user to enter.

Anti-Passback reset schedule

The schedule you select will reset all controlled cards to "un-known location status" until the cards are used at either of the controller's readers.

The card will be set to ENTRY or EXIT (depending on which of the two readers it is used at next) and, from then on, the system will keep track of the card until the next scheduled or manual reset.

Count that activates relay

Select a number between 1 and 8000. The system keeps track of the number of monitored cards that are in the area and changes the state of a relay when this count is reached.

When cards exit the area, the counter decrements and the relay will eventually reset when the count is lower than the value defined. If "0" is selected the relay will not trigger.

Note: Only cards programmed with the Anti-Passback option set to "yes" (see user definition menu) will increment or decrement the count. For a reliable count, all cards should be monitored and hard Anti-Passback should be implemented.

Typical application for count function

A company with 200 employees has a parking lot with 100 parking spots. The parking lot entrance/exit is fitted with an ENTRY/EXIT reader set to hard Anti-Passback. *All employees who want to access the parking lot must use a card with Anti-Passback monitoring.*

The system will keep track of how many cars are in the parking lot. When the count reaches 100, a relay can turn on the power to a

"PARKING LOT FULL" sign, when the count goes back below 100 the relay will be deactivated and the sign will turn off.

You have the option of setting up the system to prevent access after the count is reached or just turn on the sign but still allow access.

Preventing access affects all cardholders, this option cannot be limited to cardholders who are monitored for Anti-Passback.

Relay activated on count

Select a local relay that will be activated when the count is reached.

Assigning Expansion Modules

To assign expansion modules, click on the "KT-300" button.

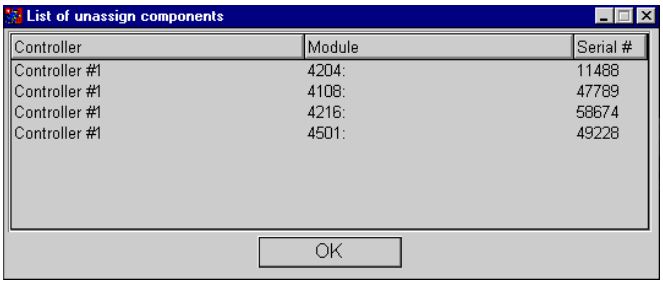
The Combus terminals on the **KT-300** controller are used to connect expansion modules to add more inputs, outputs, relays and LCD keypads. The four Combus terminals of the main panel must be connected to the four Combus terminals or wires of all modules.

There are 4 expansion modules that can be connected to **KT-300**'s Combus (more specifications of each of these modules can be found in Section 7 - Combus Specifications, Repower and Modules)

1) **KT-PC4108 - (8-Zone Input Expansion Module)**
2) **KT-PC4204 - (4-Relay/Power Supply Expansion Module)**
3) **KT-PC4216 - (16-Zone Output Expansion Module)**
4) **KT-LCD4501 - (LCD Time & Date Display Module)**

During installation of the modules, it is necessary to inform the system that new modules have been installed on the Combus. To assign the modules to your system (software), follow these steps:

1. Establish communication between the computer and the controllers,
2. Remove the tamper switch wire (or only the wire if tamper switch is not used, of each module you want to define (if using KT-LCD4501, press the # key of each keypad),
3. A list of unassigned components should be displayed on the screen, on the same window, you should see the type of module, the serial number and on which controller it is connected. Note these numbers. See example below:



4. Select the functionality of each module (in controller definition menu) and enter the serial number in the appropriate field (see following information for each module).

Field Definition

Controller

Identifies the controller on which the modules are wired.

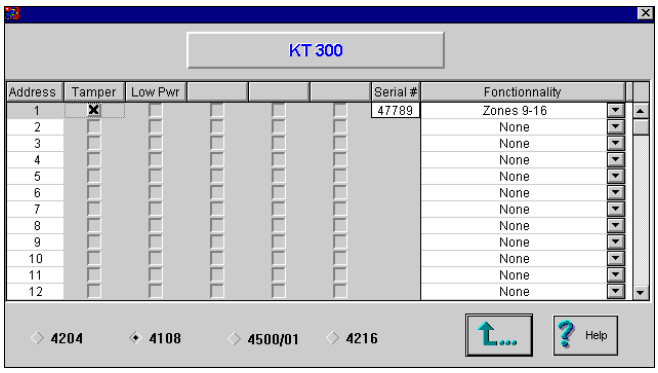
Module

Identifies the module type that is wired to the controller.

Serial

Identifies the serial number of the wired module. Note the serial numbers and press OK to accept. This number has to be entered in the controller definition.

KT-PC4108 - 8-zone input expansion module



Field Definition

Address

This field identifies the physical address of the module.

Tamper

If selected, the system will generated a Combus module defect event on the controller, whenever the tamper is disconnected from the module.

Low Pwr

If selected, the system will generate a Combus module defect event on the controller, for a lost of power from the module.

Serial

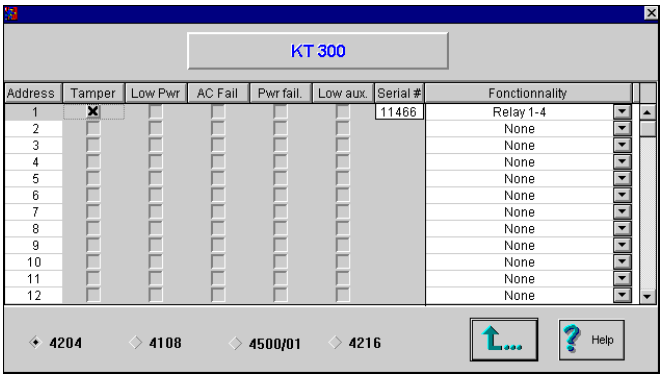
Register the serial number of the module, showed in the List of unassigned components screen.

Functionality

Select the module's functionality. Zones 9-16 will define the 8 inputs of the modules as a physical address from 9 to 16.

KT-PC4204 - 4-relay and additional power supply module

The KT-PC4204 can be used to "repower" the Combus. Depending on how many modules are connected to the Combus and how far they are from the **KT-300** controller, you may need to "repower" the controller's Combus (see Section 7 - Combus Repower for more details).



Field Definition

Address

This field identifies the physical address of the module.

Tamper

If selected, the system will generated a Combus module defect event on the controller, whenever the tamper is disconnected from the module.

LowPwr

If selected, the system will generate a Combus module defect event on the controller, for a lost of power from the module.

AC Fail

If selected, the system will generate a Combus module defect event on the controller, for a lost of AC power from the module.

Pwr Fail

If selected, the system will generate a Combus module defect event on the controller, for a lost of power from the module.

LowAux

If selected, the system will generate a Combus module defect event on the controller if the voltage of the auxiliary output is too low. The auxiliary output is used when the module is wired as a "repower" module, if not, it can be used for other purposes but there is no control over that output (always activated).

Serial

Register the serial number of the module, showed in the List of unassigned components screen.

Functionality

Select the module's functionality.

Relay 1 to 4 - Will define the 4 relays of the module as a physical address from 1 to 4 in your software.

***Note**: All KT-PC4204 modules that are used for Combus repower should be assigned as relays 1-4.*

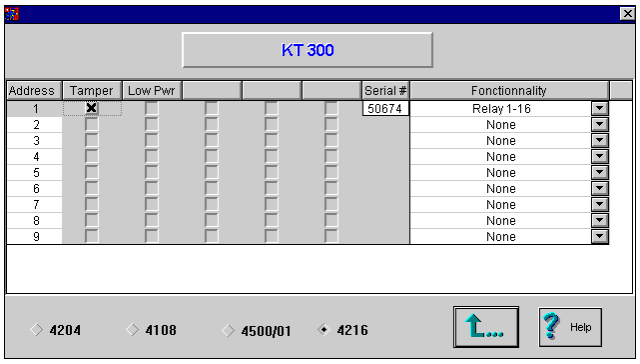
Relay 5 to 8: Will define the 4 relays of the module as a physical address from 5 to 8 in your software.

Relay 9 to 12: Will define the 4 relays of the module as a physical address from 9 to 12, etc.

***Important Note:** When using the KT-PC4204 in "repower" mode, the first relay of the module will be reserved for the "repower function". You will have to assign an "all valid" schedule to the first relay so it is "permanently activated". If you are using a KT-PC4204 in "repower" mode and other KT-PC4204 modules that are assigned as relays 1-4 or KT-PC4216 modules that are assigned as relays 1-16 are also connected to the same loop, do not use relay 1 of those modules or relay 1 of the KT-300 door controller. Please also note that all KT-PC4204 modules that are used for Combus repower should be assigned as relays 1-4. The jumper 1 "J1" on the KT-PC4204 must be moved to the Combus relay position.*

***Note:** Do not use any power supply other than the KT-PC4204 to repower the Combus. In the event of a power surge or transient, a module may lock up and cease to communicate with the controller. If the **KT-300** loses communication with the module, it will initiate a module reset and will power down the Combus for five seconds in attempt to reset the problem module. After five seconds, the controller will reapply power to the Combus and the problem module should begin to operate as intended.*

KT-PC4216 - 16-zone output expansion module



Field Definition

Address

This field identifies the physical address of the module.

Tamper

If selected, the system will generated a Combus module defect event on the controller, whenever the tamper is disconnected from the module.

LowPwr

If selected, the system will generate a a Combus module defect event on the controller, for a lost of power from the module.

Serial

Register the serial number of the module, showed in the List of unassigned components screen.

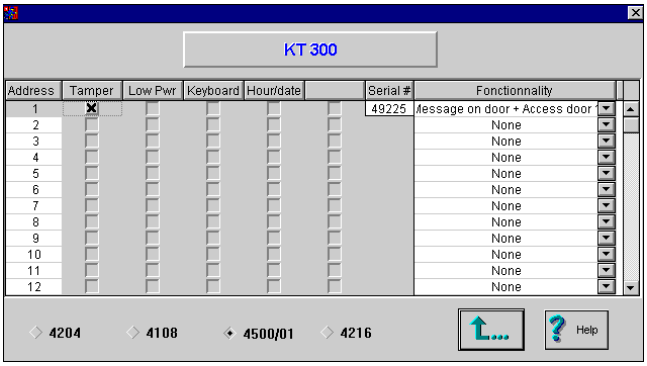
Functionality

Select the module's functionality.

Relay 1 to 16: Will define the 16-zone outputs as a physical address from 1 to 16 in your software.

***Note:** If you are using a KT-PC4204 in "repower" mode on the same loop, do not use the first relay of the KT-PC4216 (see KT-PC4204).*

KT-LCD4501 - LCD Time & Date Display Module



Field Definition

***Note** : Before you make any selection, you have to select the module's functionality.*

Address

This field identifies the physical address of the module.

Tamper

If selected, the system will generated a Combus module defect event on the controller, whenever the tamper is disconnected from the module (some keypads are not equippled with a tamper).

LowPwr

If selected, the system will generate a a Combus module defect event on the controller, for a lost of power from the module.

Keyboard

Must be selected to be used as a keypad for access or time and attendance. If you wish to use the LCD module as a keypad (access), then you have to select the "Integrated in reader" field in the "Keypad type"of the controller definition menu.

Hour/Date

Must be selected if you wish to display the time and date on the keypad screen.

Serial

Register the serial number of the module, showed in the List of unassigned components screen.

Functionality

Select the module's functionality:

1) Message on door:

   When you select this option, this means that the module will not be used as a keypad (door access). It can therefore be used only to display the time and date (you have to select "Hour/ date" field).

2) Message on door + Access door 1:

   Selecting this option means that the module will be used as a keypad for access on door 1. To use as a keypad, you have to select the "Integrated in reader" field in the "Keypad type"of the controller definition menu. You can also display the time and date by selecting the "Hour/time" field.

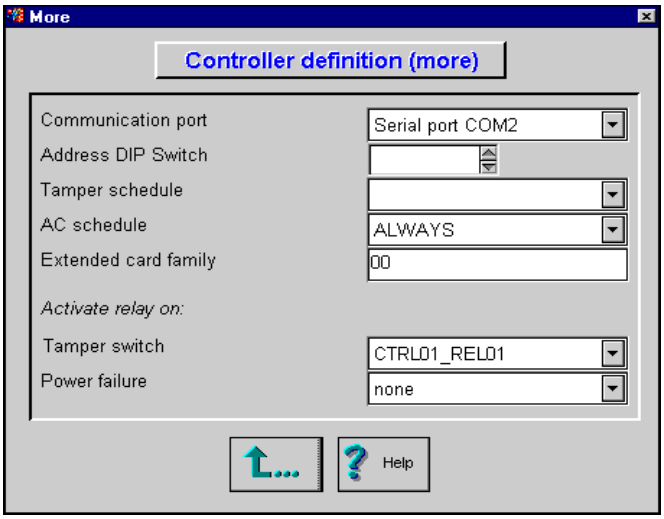
3) Message on door + Access door 2:

   Selecting this option means that the module will be used as a keypad for access on door 2. To use as a keypad, you have to select the "Integrated in reader" field in the "Keypad type"of the controller definition menu. You can also display the time and date by selecting the "Hour/time" field.

Note: No matter which feature is chosen, the module will always display the version of the firmware every time the power is switched on. If you wish to use the LCD module as a keypad (access), then you have to select the "Integrated in reader" field in the "Keypad type"of the controller definition menu.

"More" button 

If you press the more button from the controller definition screen, the system will display the following screen:



Field Definition

Communication port

Select the serial port on which the controller bus will be connected to the host computer. To select the baud communication speed, refer to Section 5 under workstation definition menu under "Port setting" button.

Address DIP switch

This field applies only if you are using KT-200 controllers. The address selected here must be the same as the physical address on the controller. Enter the controller's address (1 to 32 max). Two controllers cannot share the same address.

Tamper schedule

Select a schedule to activate tamper switch monitoring.

AC schedule

Select a schedule to activate AC monitoring.

Extended card family

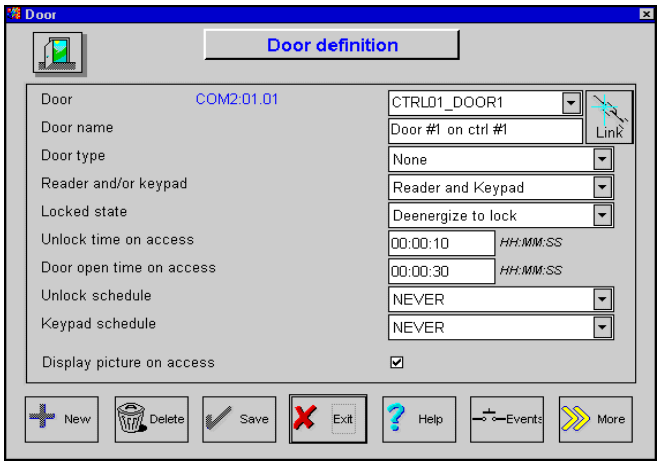
Enter the extended card family when applicable. When selected, you will have to enter these numbers on the card definition screen.

Activate relay on

Allows you to select a relay which will be activated on the events: "Tamper switch" (KT-200 only) and "Power failure".

Door Definition

This feature is used to define the doors of the system (door type, unlocking schedule, etc).



Field Definition

Door - COM2:01:01

The door address is a physical address consisting of the serial port, the physical address of the controller *, and the physical address of the doors (1 or 2). The door address cannot be modified unless the controller serial port setting is modified at which time the door address is automatically changed by the system.

"SEE SECTION 11 IF YOU ARE USING KT-200 CONTROLLERS"

Door

The door label consists of 12 alphanumeric characters or less and is used to identify the door within the system.

Door name

The door name consists of 30 alphanumeric characters or less. It also gives detailed information concerning the door *i.e.: Front Entry Door.*

Door type

Indicates if the door is considered as an entry or an exit. For doors that have readers on each side, select ENTRY for the outer reader and EXIT for the inner reader (must be used for Anti-Passback).

Reader and/or keypad

Indicates how access to the door is controlled: by a reader, a keypad or both.

Locked state

Selects the operating mode of the lock installed on the door. "DEENERGIZED TO LOCK" is used for doors with fail-secure devices such as door strikes and "ENERGIZED TO LOCK" is used for doors with fail-safe devices such as mag locks.

Unlock time on access

The time during which the door is unlocked following a valid card reading or a valid request-to-exit (REX). Maximum time allowed is 4 minutes and 15 seconds.

Door open time on access

The time period during which a door can remain open following a valid access or a REX. Applies only to a controlled door monitored with a contact. Maximum time allowed is 4 minutes and 15 seconds.

Unlock schedule

The door will automatically unlock according to this schedule. To view other defined schedules, click on the pick list.

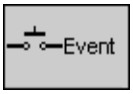
Keypad schedule

Used with doors defined as "Reader/keypad". This is the schedule according to which it will be necessary to enter a PIN code at the keypad after presenting a valid card. Applicable only to those card users set to "Must use PIN" in Card definition.

Display picture on access

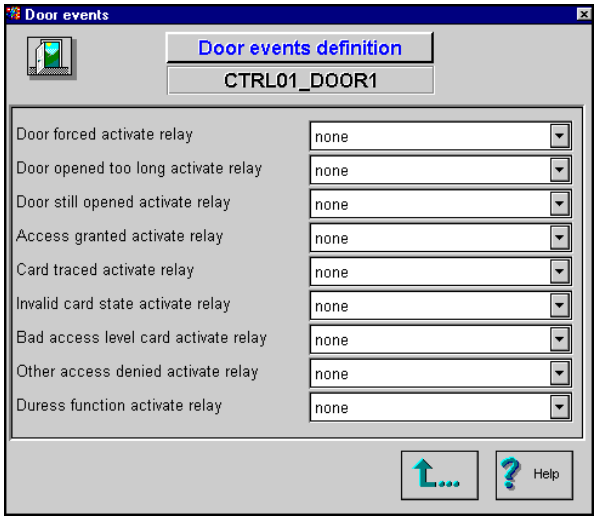
This option allows you to automatically display the user's picture when an access event is generated.

Buttons



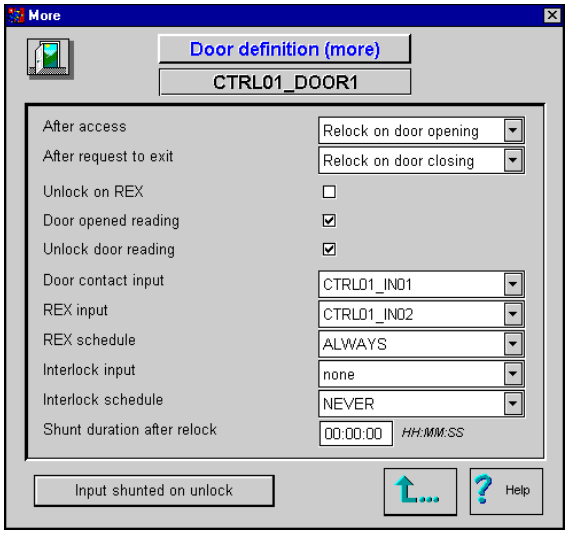
Allows for activation of a selected relay, when the chosen event is reported. The following events can be selected to activate a relay: door forced, door open too long, door still opened, access granted, card traced, invalid card state, bad access level card, other access denied and duress function.

If you click on the Events button from the door definition screen, the system will display:



Select the relays to be activated when the selected event occurs.

Allows to enter more information concerning the door. If you select the "More" button from the door definition screen, the system will display an addtional screen for the chosen door.



Field Definition

After access

This will determine if the door will re-lock on opening or, re-lock on closing, after a valid access. Applies only to a controlled door monitored by a contact.

After request-to-exit

This will allow the door to re-lock on closing or re-lock on opening during an exit detection or REX. Applies only to a controlled door monitored by a contact.

Unlock on REX

Must the controller actually unlock the door when a request-to-exit is detected? Usually NO for door strikes and YES for mag locks. Click on the check box to activate this option.

Door opened reading

Selecting YES will allow users to have a card read while a door is open during a valid access, without having to close the door between each read. Click on the check box to activate this option.

Unlock door reading

Indicates if we allow card reads on a door which has been manually unlocked or unlocked by a schedule. Click on the check box to activate this option.

Door contact input

This input supervises the state of the monitored door. This input must be located on the controller controlling the door. Inputs 2 and 4 are reserved for the door contacts on door 1 and 2. Click on the pick list for a choice of available inputs.*

"SEE SECTION 11 IF YOU ARE USING KT-200 CONTROLLERS"

REX input

This input supervises the request-to-exit input. This input must be located on the same controller operating the door. Click on the pick list for a choice of available inputs. Recommended: Input 2 for REX on door 1 and Input 4 for REX on door 2.*

"SEE SECTION 11 IF YOU ARE USING KT-200 CONTROLLERS"

REX schedule

This is a schedule according to which the controller will detect request-to-exit signals originating from the exit contact. Applies only to a door with a request-to-exit device. Click on the pick list to select schedules.

Interlock input

The interlock input is to supervise the state of the interlock or mantrap. An interlock is used to prevent access to a user when another door is opened. Both doors, contacts and interlock inputs must be located on the same controller. You also need to assign a schedule to use this function.

1st door on the controller:

Set the interlock inputs

Door contact input = input 1 of the controller

Interlock input = door contact of the second door

2nd door on the controller:

Set the interlock inputs

Door contact input = input 3 of the controller

Interlock input = door contact of the first door

Click on the pick list for a choice of available inputs.

Interlock schedule

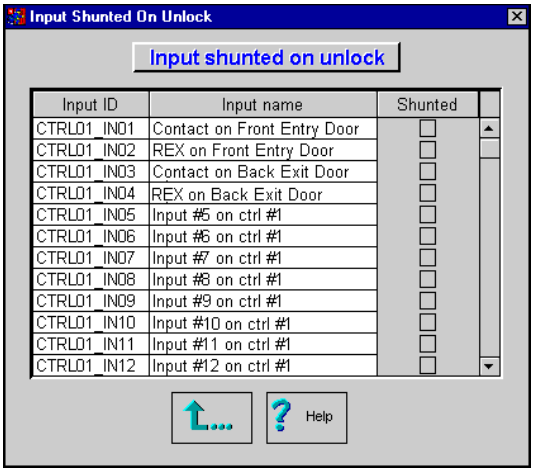
The schedule according to which the state of the mantrap is checked by the controller before permitting access to a user.

Shunt duration after re-lock

The inputs that were shunted on unlock, can be programmed to stay shunted for a specified period of time after the door re-locks. Usually set to a few seconds to prevent false alarms during the few seconds after a door closes and stabilizes.

Maximum time allowed is 4 minutes and 15 seconds.

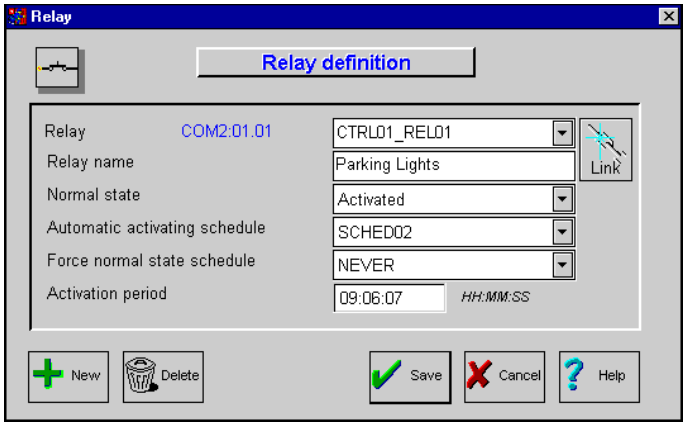
You can select the inputs that will be shunted as soon as the door is unlocked. This permits associating other inputs such as a mag-lock or electric strike switches to operate as a separate input that will be shunted during valid door openings. If you select the "Input shunted on unlock" button from the door definition "More" screen, the system will display an additional screen:



Select (from the Shunted column) the inputs that will be shunted on unlock (not monitored).

Relay Definition

This screen is used to define when relays will be triggered according to schedule and what they will trigger.



Field Definition

Relay - COM2:01:01

The relay address is a physical address consisting of the serial port, the physical address of the controller and the physical address of the relay. *

"SEE SECTION 11 IF YOU ARE USING KT-200 CONTROLLERS"

Relay

The relay label is composed of 12 alphanumeric characters or less.

Relay name

The relay name is composed of 30 alphanumeric characters or less. It provides additional information concerning the relay.

Normal state

Select the state of the relay when no event, schedule or manual operation is activating it (deactivated or activated).

Automatic activating schedule

Select a schedule according to which the relay will automatically be activated.

Force normal state schedule

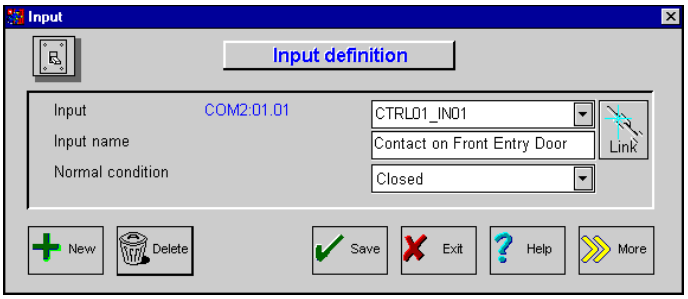
The schedule according to which the relay will be forced to remain in its normal state. Only a manual operation could change the status of the relay.

Activation period

Activation period is set in hours, minutes and seconds. It's the time period during which the relay will be momentarily activated.

Input Definition

This feature is used to define inputs (monitoring schedule, relay activated by input, etc).



Field Definition

Input - COM2:01:01

The input address is a physical address consisting of the serial port, the physical address of the controller and the physical address of the input (1 to 8 - without expansion module).*

"SEE SECTION 11 IF YOU ARE USING KT-200 CONTROLLERS"

Input

The input label is composed of 12 alphanumeric characters or less. The label is used to identify the input in the system.

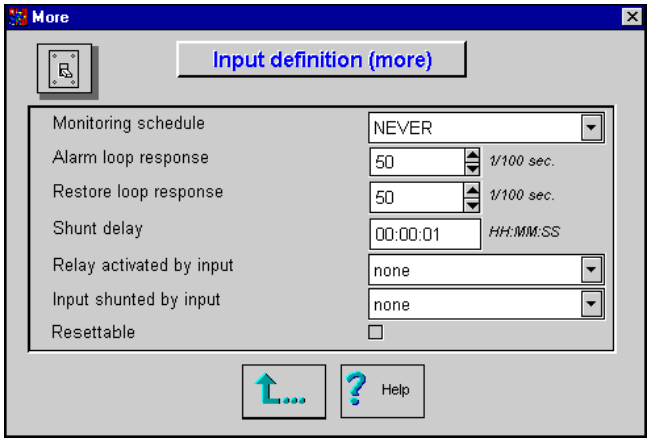
Input name

The input name is composed of 30 alphanumeric characters or less.

Normal condition

Set to either normally open or normally closed.

Input Definition - 



Field Definition

Monitoring schedule

Schedule according to which the system will supervise the condition of the input. When the schedule is valid, a changed condition of the input generates either a "Input in alarm" or "Input restored" event.

Alarm loop response

Delay in hundredths of a second from 10 to 65535 indicating the

necessary time period during which an input must remain in an alarm condition to be reported. For example 200 delay means that a new condition must remain stable for at least 2 seconds before it will be reported in alarm.

Restore loop response

Delay in hundredths of a second from 10 to 65535 indicating the necessary time period during which an input must remain in a restore condition to be reported. For example, 200 delay means that a new condition must remain stable for at least 2 seconds before it is reported in normal condition.

Shunt delay

The shunt duration of this input when it is being temporarily shunted by another input. The valid range is from 1 second to 9:06:07 hours.

Relay activated by input

Select a relay that will be activated when the input being programmed goes into alarm.

Input shunted by input

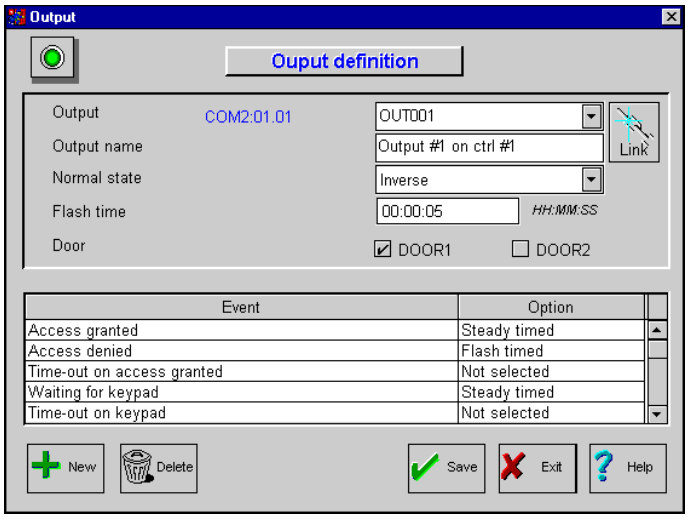
Select an input that will be shunted when the input being programmed goes into alarm.

Resettable

If this feature is selected, it allows the "Shunt delay" time period associated to the input to be reset every time this input is "shunted" by another input.

Output Definition

This screen is used to define how the events will trigger the outputs.



Field Definition

Output - COM2:01:01

The output address is a physical address consisting of the serial port, the physical address of the controller, and the physical address of the output (1 to 4).*

"SEE SECTION 11 IF YOU ARE USING KT-200 CONTROLLERS"

Output

The output label is composed of 12 alphanumeric characters or less and is used to identify the output in the system.

Output name

The output name is composed of 30 alphanumeric characters or less. It provides additional information concerning the output.

Normal state

Select whether the output is normal or inverse in passive normal state.

Flash time

This field defines the activation time during which the output remains active when it is programmed for a temporary activation.

The duration of the activation period of the output if set to "steady timed"or "flash timed" for an event.

Door selection

Select which door will affect the output you are configuring by placing an "x" next to the door. For example, if you want Output 1 to be activated when an access granted occurs only on door 1, place an "x" next to door 1 only.

Events

For each listed event, you can select how the event will trigger the output.

Options:

The option sets the state of the output when its associated event occurs. A timed selection means that the output will remain activated for the period of time defined in the "flash time" field, otherwise, it will remain activated until the condition (event) returns to normal.

Not selected

The output given this option will not affect its state. Nothing will happen.

Steady timed

The output given this option will not flash, it will remain activated for the "flash time" specified and will return to its normal state when the activation period is over.

Flash timed

The output given this option will flash and will remain activated for the "Flash time" specified and will return to its normal state when the activation period is over.

Steady

The output given this option will not flash, it will remain activated until its condition (event) returns to normal.

Flash

The output given this option will flash and will remain activated until its condition (event) returns to normal.

Note:

When outputs flash, they flash (toggle from red to green) according to the on-off delays pre-defined in the workstation definition menu under output time button.

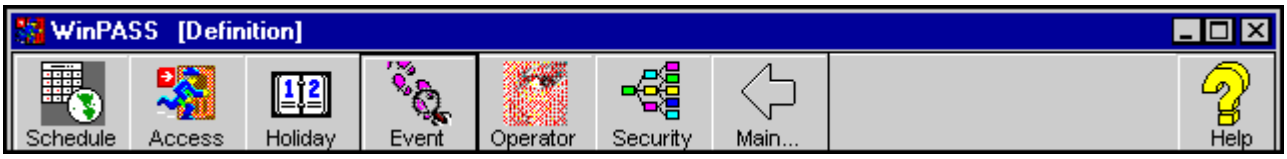
SECTION 6

Logical Components Configuration

This section is used to define the logical components of the WinPass system. It is used to define:

1) Schedules: define the start and end times,
2) Access levels: associate doors with schedules,
3) Holidays: define holidays,
4) Event parameters: define events with components, acknowledging schedule, printing schedule, priority, display color (on the monitor),
5) System operator: login name, name, security level, password, login schedule and language,
6) Operator security levels: define if components can be viewed, modified, deleted or created by the operator who will be assigned this level of security.

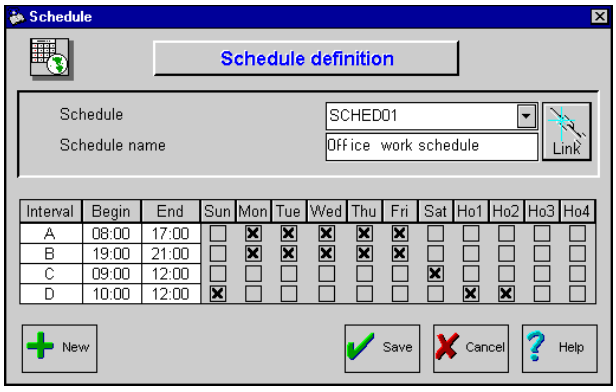
THE DEFINITION MENU TOOLBAR



Schedule Definition

Schedules are used throughout the system. For example, you need to determine times during which a cardholder may have access to some or all doors.

Schedules can also be used to determine when events are reported, activate relays controlling different functions (lighting, heat, etc.), etc. It is also possible to use the same schedule for different applications, but it is recommended to create a distinct schedule for each application. It is then much easier to modify a particular application schedule without affecting other applications.



Field Definition

Schedule

The schedule label is composed of 12 alphanumeric characters or less and is used to identify the schedule within the system.

Each schedule is composed of four intervals; each interval includes a start time and a stop time. Select by placing an 'X' under the days of the week that the interval should be valid.

The 'Ho' abbreviation corresponds to 4 different holiday types as defined under Holiday definition.

Schedule names

The schedule names consists of 30 alphanumeric characters or less *(i.e.: Office Work schedule, always, never, etc).*

Always

This pre-defined schedule is Always valid and cannot be modified.

Never

This pre-defined schedule is Never valid and cannot be modified.

Intervals (A, B, C, D)

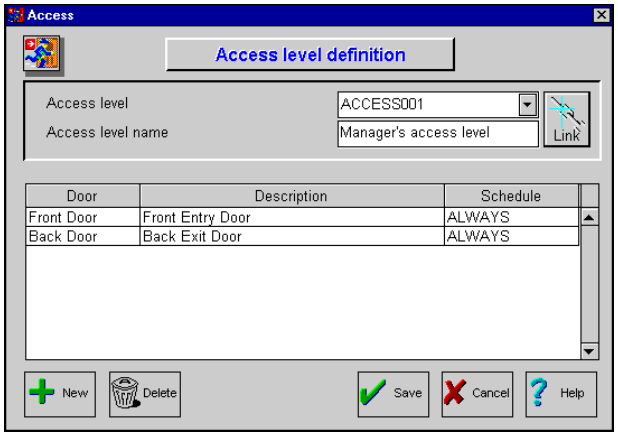
An interval is defined by entering the start time (first field) and the end time (second field); the end time must be equal or greater than the starting time.

Select the days applicable to the interval by placing an 'X' under the selected days. In order to create an interval from Monday 20:00 (8PM) to Tuesday 8:00 (8AM), the interval must be divided in two intervals.

A first interval is defined for Monday form 20:00 to 24:00 and the second interval is defined for Tuesday form 00:00 to 08:00. The system therefore considers these two intervals as one continuous interval.

Access Level Definition

The purpose of assigning an access level to a cardholder is to provide that cardholder access to specific doors according to specific schedules. Each cardholder must be assigned a set of user parameters that will allow entry to authorized doors for that individual and deny entry to unauthorized doors.



Each access level represents a group of users, for example, office employees, managers, staff, etc., that share the same user rights. After defining access levels, assign one of the access levels to each cardholder in Card Definition. An access level is created by assigning a schedule for each of the system's doors.

Field Definition

Access level

The access level label is composed of 12 alphanumeric characters or less. When you click on New, the system will automatically number the new access level being created.

Access level name

The access level name is composed of 30 alphanumeric characters or less (i.e.: manager's access level).

Door

The system displays all the doors of the system. Select a schedule for each displayed door. If you don't want to include the door, set

the schedule to “Never”

Description

Displays the description of the door as labelled in the system.

Schedule

For each of the doors listed, a schedule must be assigned. The schedule determines the time during which an access to the door will be authorized for cardholders assigned with that access level.

ALWAYS schedule

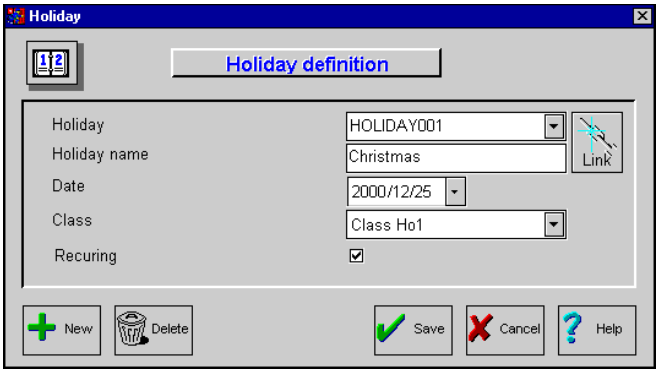
This access level permits access to all doors at all times and cannot be modified.

NEVER schedule

This access level denies access to all doors all the time and cannot be modified.

Holiday Definition

This feature is used to define holidays.



Field Definition

Holiday

Select a holiday to be modified from the displayed list or click on NEW to create a new holiday. The holiday label is composed of 12 alphanumeric characters or less.

Holiday name

The holiday name is composed of 30 alphanumeric characters or less. It provides detailed information concerning the holiday (i.e. Christmas Day).

Date

Enter the date corresponding to the holiday (i.e.: 2000/12/25).

Class

Each holiday must be assigned to one of four holiday types. See Schedule definition for holiday types. It is recommended to define holidays at the beginning of the year and review holidays that are not on fixed dates (Easter, Thanksgiving, etc.).

Recurring

This option allows programming of fixed recurring holidays which are on the same date every year. If this parameter is selected, the holiday will automatically be taken into account every year.

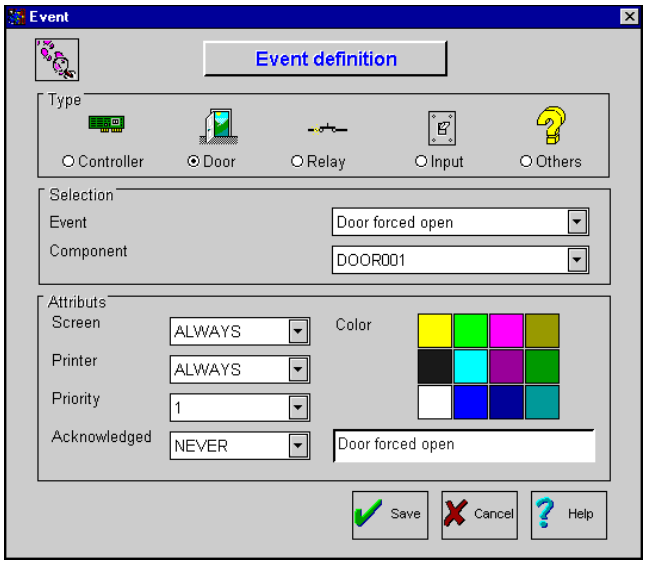
Event Definition

The term “Event” is used to describe activities or alarms detected by the system or generated by the system. There are many different system events such as Access granted, Input in alarm, Card modified by operator, etc..

Event definition is a powerful feature of the system. For each event, it is possible to determine how the event should be dispatched to a combination of the following devices: Screen and printer. These dispatches can also be limited by schedules that will allow, for example, to print or display some events only during a particular period of time, such as after regular hours. Each event related to a device can be individually associated to a corresponding set of actions such as display or print.

For example: The “Door open to long” event is defined for each individual door of the system. This also permits a different action, or response on a door to door basis. Alarm events should be set to require an acknowledgment from the operator.

WARNING: The screen schedule **also** controls the recording of the events to the disk.



Field Definition

Type

There are 5 categories of events: controller, door, relay, input and other related events. When a category is selected, the “Event” selection field will only list events related to the selection (i.e.: if controller is selected, the Event field will only contain controller related events).

Event

This list only contains the events related to your selection in the “Type” field ; (i.e.: if controller was selected, this field would only contain controller related events).

Component

The component list is relative to the selected event. For example, if you select “Door forced open”, the system will display a list of all the doors of the system. Once the desired door is selected, you can select the attributes you wish to modify (display color, priority, display on screen schedule, etc.).

Screen

Select the schedule according to which events will be displayed on-screen and saved to disk.

Printer

Select the schedule according to which events will be printed on the log printer (to select a log printer, refer to the Workstation Configuration menu under printer).

Priority and color

Each event concerning a specific device can be assigned a priority from 1 to 16 (1 is the highest and 16 the lowest) as well as a display color. The priority determines the sequence in which alarms, in the alarm queue, will be displayed to the operator. The priorities have been preset to the most common values.

You can also select the display color of the event. The color scheme is preset as: red for alarms, green for normal and restored events and yellow for warnings and faults.

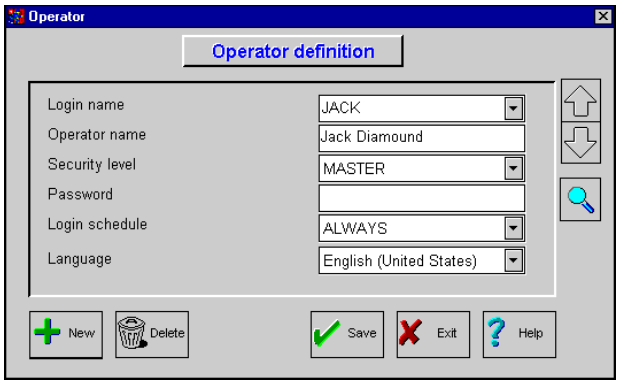
Acknowledged

Specify the schedule during which the system will request that the operator acknowledges the event by pressing the acknowledgment button. Only an operator who is logged in can acknowledge events.

Operators can be required to acknowledge certain events such as alarms or card trace type of events. Events that require operator acknowledgment have to be defined in Event Definition. When the operator is required to acknowledge an event, the computer's audible warning will sound and an alarm window will appear on the monitor. The alarm event will be displayed with time, date and the description of the event.

Operator Definition

This screen is used to define the parameters for each operator of the WinPass system.



Field Definition

Login name

The "login" name is composed of 30 alphanumeric characters or less. It is used when connecting to the system in order to identify the operator.

Operator name

The operator name is composed of 30 alphanumeric characters or less.

Security level

Determines the security level of an operator. The system offers 1 fixed level and 8 programmable levels of security. Security level "Master" is predefined and allows access to all of the system's commands. You must program the other security levels if you want to limit operator access to commands and/or menu options.

Password

The password is an alphanumeric code of 12 characters or less. It is required by the system to confirm operator login to WinPass. When a new operator is created, the default password is identical to the login name (i.e.: OP002 login name has the password OP002).

To modify the password, delete the asterisks and enter and confirm the new password. The password is not displayed and cannot be printed.

***Note**: The default operator WINPASS has the password "WINPASS" and security level MASTER.*

Login schedule

Select the schedule according to which the operator will be allowed to log in the system.

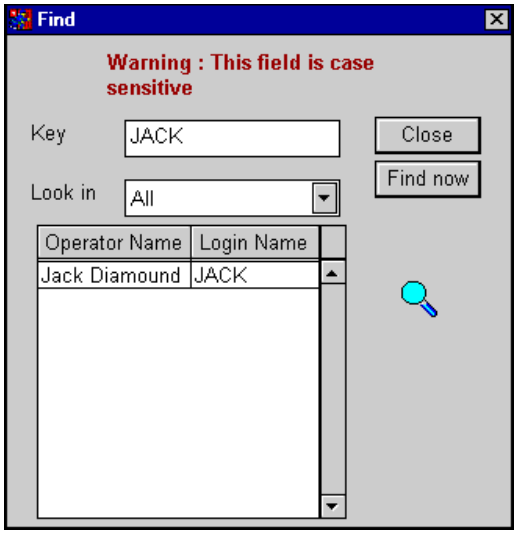
Language

Select the operator's language. Available in English and French.

Search an operator

This option allows you to search for an operator's record.

1) Click on the Find button,
2) Enter one or more search words i.e.: "Jack",
3) Click on the Find now to start search,
4) Once the search is terminated, WinPass will display the record or records found.

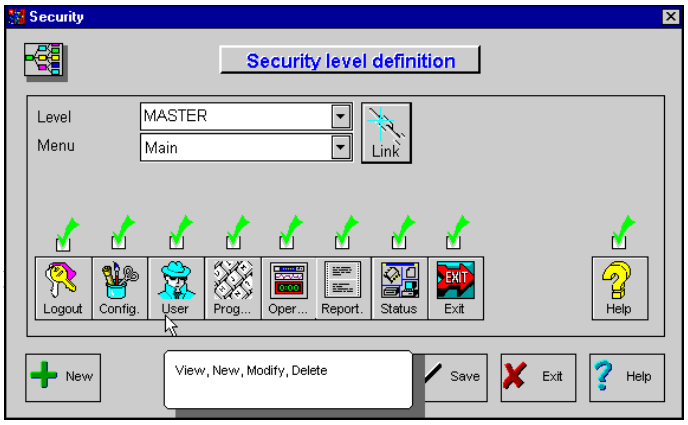


Security Level Definition

Every operator in "Operator definition" must be assigned a security level. This security level determines which menus the operator has access to and what levels of access the operator can use (i.e.: View, Modify, Create or Delete).

There is one predefined security level labeled "MASTER" which cannot be modified. You can create up to eight (8) security levels.

***Note**: If an operator does not have access to an item of a menu, for example "Delete" in the card menu, the button "Delete" will not appear at the bottom of the definition menu screen.*



The items of each menus are selected by pressing the option button and will appear. An option screen may be displayed according to your selection (see "option" field below).

Field Definition

Level

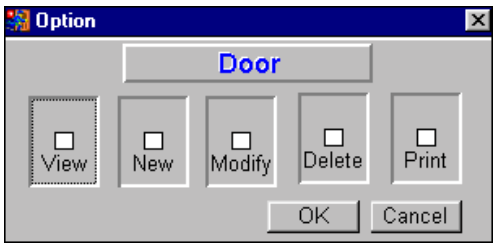
Select the access level to be modified, or click on New to create a new one.

Menu

Select the menu (login, main, definition,configuration, operation and report) on which you wish to make selections.

Option

When you click on a button to select it, a list of options will be available according to your selection. Select if the operator assigned this security level will be able to view, create (new), modify, delete or print the selection.



VIEW: If selected, the operator assigned this security level will only be able to view, will not be able to modify, create, delete or print.

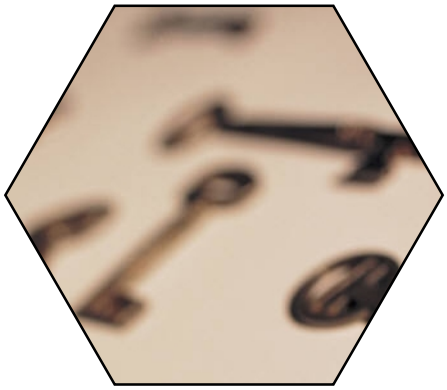
NEW: If selected, the operator assigned this security level will be able to create new components and save them.

MODIFY : If selected, the operator assigned this security level will only be allowed to modify an existing record, will not be able to create, delete or print.permits changes to an existing record only.

DELETE : If selected, the operator assigned this security level will only be allowed to delete existing records.

PRINT : If selected, the operator assigned this security level will only be allowed to print records.

You can select all of the options or just a few. A ***yellow*** check mark will appear if partial rights are selected for an option.



SECTION 7

Performing Manual Operations

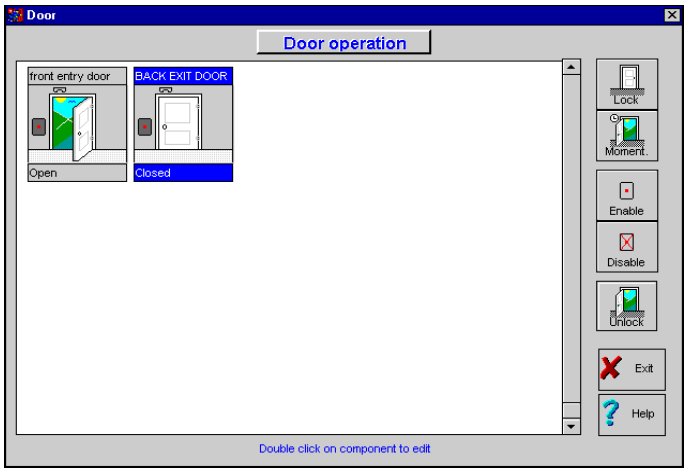
This section is used to perform manual operations on various components of the system. You can manually:

- Lock, unlock and momentarily unlock doors,
- Enable and disable door readers,
- Activate, deactivate or momentarily activate relays,
- Shunt, unshunt or momentarily shunt inputs,
- Activate and deactivate outputs,
- Display a complete or summary status of the controllers and peripherals,
- View and reset cards inside/outside an area (Anti-Passback),
- Reload controllers (soft/hard reset, reload and controller firmware download),
- Change the system's date and time and re-index files.

THE OPERATION MENU TOOLBAR

Door Operation

This window allows the operator to manually lock/unlock doors and to enable/disable the readers. The graphical view displays the door' status and access events as they occur (you can actually see the door open and close!).



Field Definition

Door name

Label identifying the door in the system. The door name is displayed on top of each door drawing.

Door status

Door status is represented in text format here at the bottom of the door drawing (i.e.: *open, closed, forced open).*

To select a door

To select a door just click on the selected door name and the name of the door will be displayed in white capital letters highlighted with a blue background. All manual operations are executed on that selected door.

Buttons

Lock / Unlock

Select a door to be locked or unlocked, then click on the appropriate button.

When the door is unlocked, the reader' status light becomes green and when locked the reader' status light changes to red.

Momentarily Unlock

Select a door to be momentarily unlocked according to the duration of the "unlock time on access" field programmed in "Door Definition". After this period the door will automatically re-lock.

Enable / Disable reader

Select a door on which the reader has to be enabled or disabled. This command is useful in case of emergencies to instantly remove access rights to all individual cardholders who usually have access to that door.

Status

Door State

The door state is represented by a graphic of the door. The graphic can display 3 door states: door open, door closed and door forced open.

For example "door forced open". 

Reader State

The reader' state is represented by a graphic of the reader. There are 4 different states:

- **Enabled** (red dot)
- **Disabled** (red X)
- **Door unlocked** (green dot)
- **Door locked** (red dot).

Rex State

A door equipped with a REX (request-to-exit device) will display a REX icon door drawing (enabled - grey).

The REX can be enabled or disabled (yellow).

Alarm State

The alarm state is represented by an annunciator. When the door is in alarm, the red flasher drawing will appear. The annunciator's color will change according to the alarm; red for top priority and yellow for a pre-alarm.

Unknown State

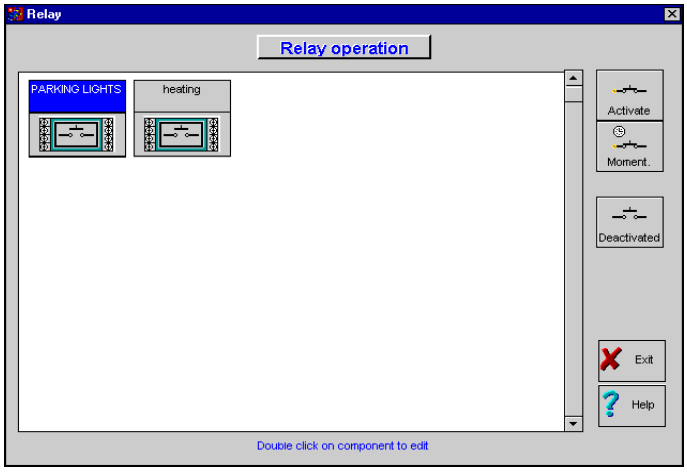
The door is considered to be in the "Unknown State" when the system has not communicated with the controller. Unknown state is represented by a **blue question mark** on the door.

Communication State

Communication errors or failures are represented by a **red question mark** on the door.

Relay Operation

This feature allows manual operations on relays such as: activation or deactivation. It also shows the actual state of the relays.



Field Definition

Relay name

Label identifying the relay in the system. The relay name is displayed on top of each relay graphic.

How to select a relay

To select a relay just click on the drawing for that relay. The selected relay's name will appear in capital white letters highlighted with a blue background. All manual operations are executed on the selected relay.

Buttons

Activate/deactivate relay

To activate or deactivate a relay, click on the appropriate button.

When a relay is activated the relay closes and the animation will be visible  .

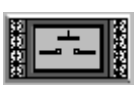
Momentarily activation

The duration of a temporary activation is programmed in Relay Definition.

Relay state

The relay state is represented by a drawing of the relay. This drawing can display two states: activated and deactivated.

Activated **Deactivated**



Unknown state

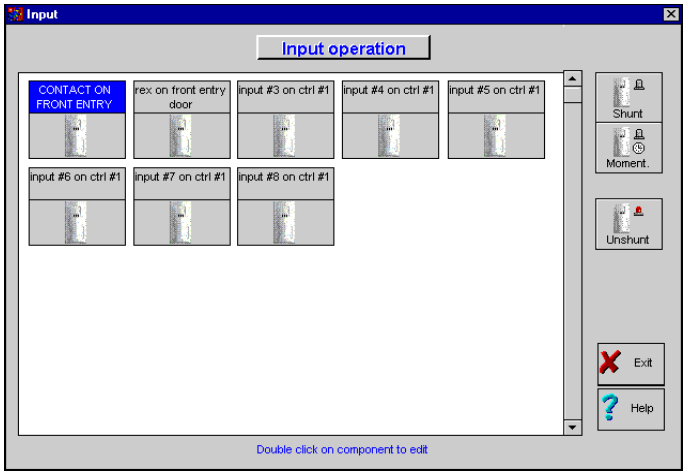
The relay state is unknown when the system has not communicated with the controller. The unknown state is represented by a **blue question mark**.

Communication state

Communication failures or error are represented by a **red question mark**.

Input Operation

This screen allows the operator to graphically view the actual input status. It also allows manual supervision or shunting inputs.



Field Definition

Input name

Description of input. The description is displayed on top of the input graphic.

To select an input

To select an input, just click on the specific input drawing. The selected input's name will appear in capital white letters highlighted with a blue background. All manual operations are executed on the selected input.

Shunt/Unshunt Input

An input can be shunted by a schedule, another input, a door or manually by an operator  . An input which is shunted by an operator overrides the monitoring schedule. Therefore, only the operator can unshunt the input  . An input is unshunted only if its schedule is valid. The manual unshunt will modify only the input which has been manually shunted.

Momentary shunt

The momentary shunt  has the same criteria as the shunt button. The duration will depend on what has been specified in "Input Definition" and will begin once the button is activated.

States

Active/Inactive State

An input is active when the detector's light changes from grey to red  (active = red, inactive = grey).

Shunt / Unshunt State

An input is unshunted if a red annunciator is displayed . However, the input will be shunted by a schedule if no annunciator is visible, by a door or by another input if the annunciator is grey , by an operator if the annunciator is grey with a face or momentarily by an operator if the annunciator is grey with a clock .

Input in alarm

An input in alarm is activated and unshunted.

Unknown State

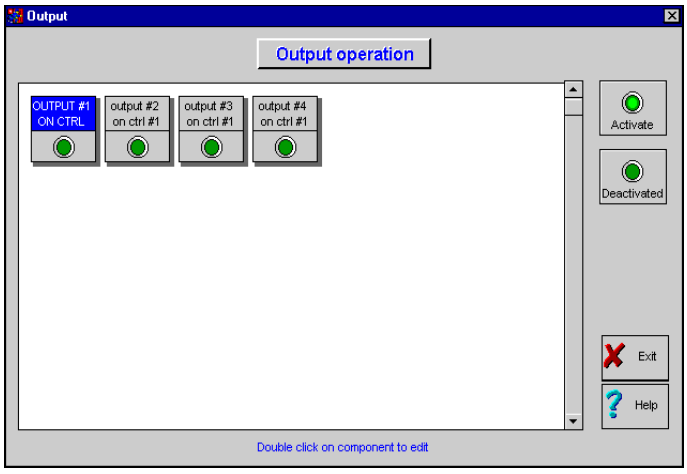
The input state is unknown when the system has not communicated with the controller. The unknown state is represented by a **blue question mark** on the input.

Communication State

Communication failure or errors are represented by a **red question mark** on the input.

Output Operation

This window permits manual operations on outputs such as activation or deactivation. It also shows the current state of the outputs.



Field Definition

Output Name

Label identifying the output in the system. The output name is located on top of each output graphic.

How to select an output

To select an output just click on the drawing for that output. The selected output's name will appear in capital white letters highlighted with a blue background. All manual operations are executed on the selected output.

Buttons

Activate

Press this button to activate an output. It will remain activated until deactivated by an operator.

Deactivate

Press this button to deactivate an output. It will remain deactivated until activated by an operator.

States

Output state

The output state is represented by a drawing of the output. This drawing can display two states:

1) **Activated** (green)
2) **Deactivated** (red)

Unknown State

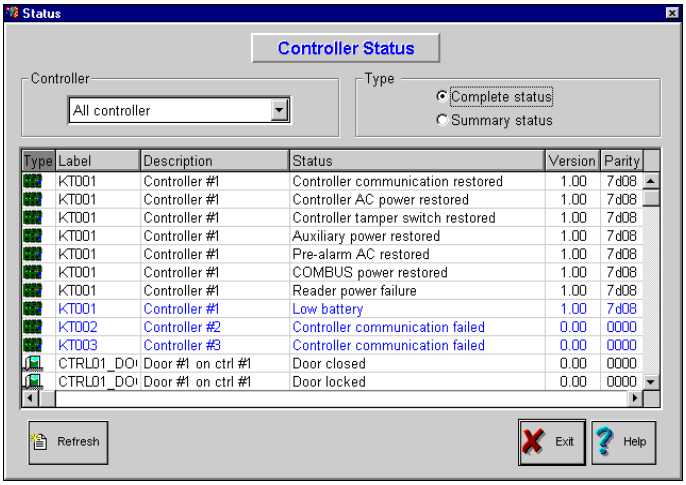
The output state is unknown when the system has not communicated with the controller. The unknown state is represented by a **blue question mark**.

Communication State

Communication failure or errors are represented by a **red question mark**.

Controller Status

The controller's status is sorted by peripherals in order of controllers, doors, relays, inputs and outputs. All states are displayed in text format.



Field Definition

Controllers

Select a controller from the displayed list.

Type

There are two types of status that can be displayed:

Summary: Only displays abnormal or activated conditions.

Complete: Displays a detailed status listing of all components.

Colums:

Type

This column displays a graphic of the component.

Label

This column displays the label name of the component.

Description

This column displays the name (description) of the component (i.e.: controller, door #1 on ctrl #1, etc.).

Status

This column displays a text status of the component.

Version - only for controller

This column displays the version number of the controller's firmware (flash memory).

Parity - only for controller

This column display the parity of the controller's firmware.

Buttons

Refresh

The controller' status is refreshed every time this button is pressed.

How to sort

To modify the displayed sorting, click on the column header on which you wish to sort the information (i.e.: Status, will sort all the information in alphabetical order).

Card List

If you have one or more controllers configured with Anti-Passback, this function allows you to view a list, for each controller, of cardholders which are considered inside or outside of an area defined by an Entry and an Exit reader.

You can also manually reset the Anti-Passback status of all cardholders, for each area (controller). Card users will not be considered inside or outside until the next use of their card at that Entry or Exit reader.

Field Definition

Controller

Select a controller from the displayed list.

Status Line

The status bar is used to show the state of the request. For example: "*Card inside request in progress...*" or "*5 cards found*".

Change Sort Key

When a card list is displayed, select the sorting key by clicking on the column's heading.

- If you click on the Card ID column, the cards will be displayed in ascending order (from smallest to greatest).
- If you click on the First Name column, the cards will be sorted by first name (alphabetical order).
- If you click on the Last Name column, the cards will be sorted by last name (alphabetical order).

Buttons

Card Inside Request

This option displays how many cards are considered to be inside the area.

Card Outside Request

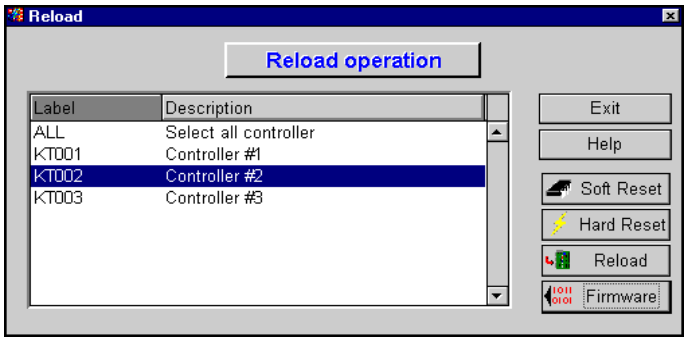
This option displays how many cards are considered outside an area .

Forgive

This button will reset all cards which are considered inside the area to an "unknown" status. The next time the card is read at an "Entry" or "Exit" reader, the system will set the card status to "In" or "Out".

Reload Controller

This feature is used to reload controller(s).



Field Definition

Select all

To select all controllers choose the ALL option. Select controllers by clicking on the controller's name. Once selected, the controller name becomes green. To unselect, click on it again.

Sort controller list

To change the way the list is sorted, select a column.

Buttons

Soft reset

This option will initiate a reset of one controller or a group of controllers without reloading controller data.

Hard reset

This option will initiate a reset of one controller or a group of controllers and then reload all controller data from the computer.

Reload

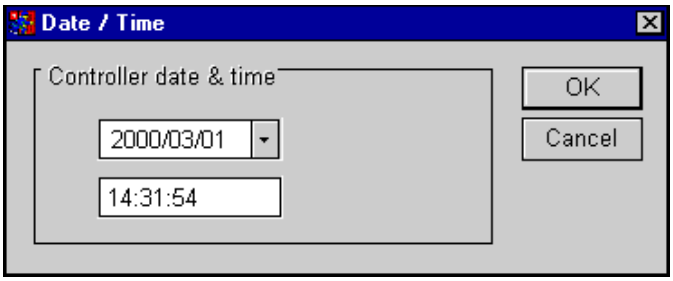
This command will reload the database of one or a group of controllers. Used to refresh all or some parameters of a single or a group of door controllers.

Firmware

To download the firmware to the controller, you must select this option. You must specify the directory where the firmware is located on your hard drive or diskette, see the workstation configuration menu under firmware.

Date & Time

This feature is used to change the system and controller's date and time.



Note: If you change the time or date, the new events will be placed in chronological order (events are sorted by time and date).

Re-Index

This option updates the index files (sort). This option is generally used for maintaining or correcting damaged files.

SECTION 8

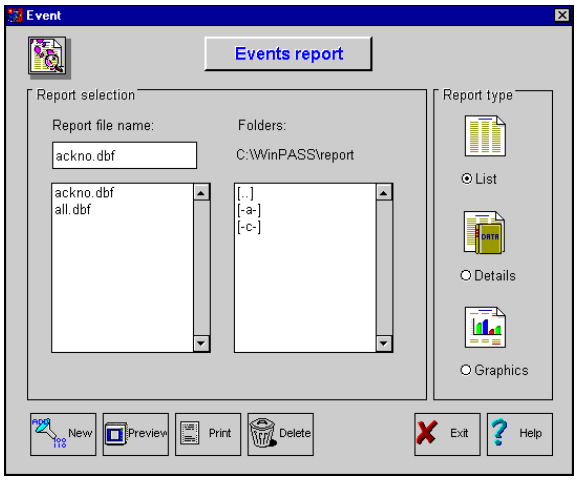
The Reports

This section is used to request reports.

- You can create reports containing specific events such as: access events, all events, acknowledged events, devices events, operator events, filtered events, etc.
- You can also create card reports according to your specific requirements.

Events Report

This feature is used to create reports containing specific events such as: access events, all events, acknowledged events, devices events, operator events and filtered events.



Once a report has been compiled, this report can be previewed as a list, details or graphics.

Field Definition

Report filename

Displays the name of the event report selected.

Folders

Displays the folder and directory selection for report files. By default, reports are saved in the C:\WINPASS**reports** directory.

Report Types:

List

Event report in text format. The events listed are sorted by chronological order. This report contains the date, time and a description of the event.

Details

Event report in text format with a graphic. The events listed here are grouped by category and sorted by chronological order. This list includes a daily pie chart graphic which summarizes the daily events by category.

Graphics

Event report in bar graph format. The events listed in this graphic are grouped by category. Each bar can represent a time, a day, a week, a month or a year according to the selected sample. The bars are subdivided by category.

Buttons

New

This option can compile a new event report according to the requested conditions. A compilation of a new report is completed by a background task. The report is available only once the compilation task is completed.

Preview

This option allows you to preview the report before it is printed.

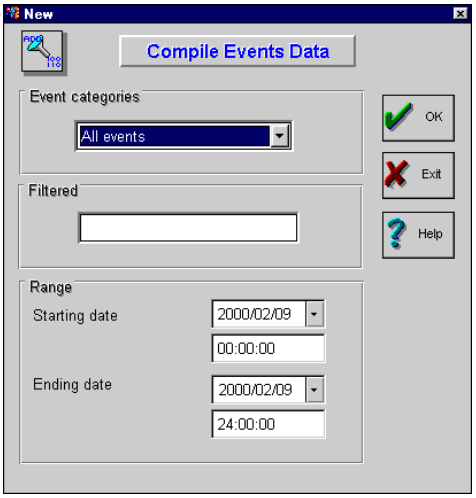
Print

This option prints the selected report.

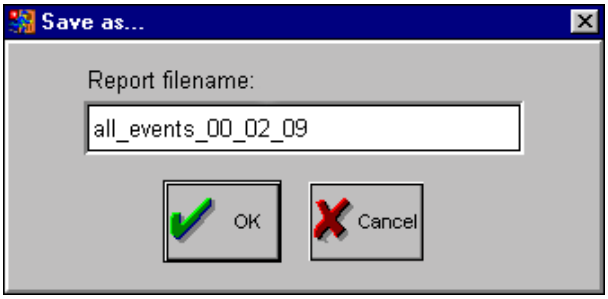
Delete

This option permanently erases the selected report file from the database.

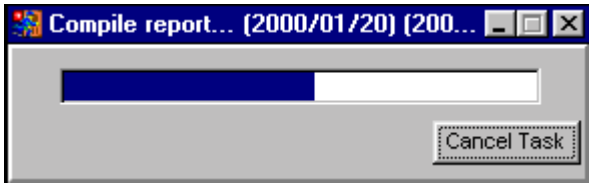
To create a new report, click on the New button, and the system will display:



Make your selections and click on OK. The system will display an additional screen. Enter the name of the new report and click on OK; the system will execute the report.



Once you have executed the report, the system will display the progression screen indicating the progress:



Field Definition

Event Categories

Select an event category for the report. There are 6 event categories:

1) **All**: To compile all events.

2) **Filtered events**: To only compile events that are filtered.
3) **Acknowledged events**: To only compile acknowledged events.
4) **Device events**: To only compile events that are related to devices.
5) **Operator events**: To only compile events that are related to operators.
6) **Access**: To only compile access events.

Filtered

Within this field, you can specify a filter for your report. For example, if you print access events, you can specify the door label "Front Door" as displayed on your event monitoring screen. Only events containing that specific string will be processed.

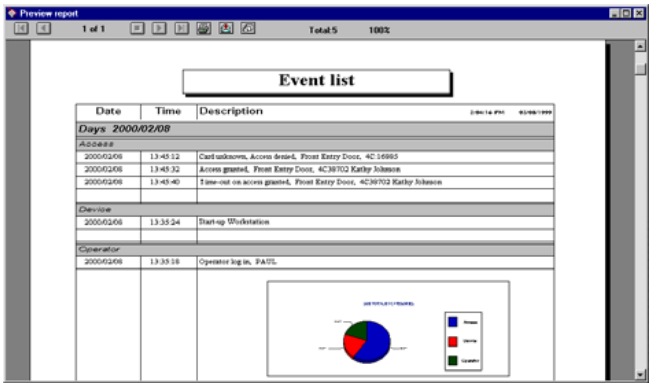
Range - Starting & Ending Date and time

Select the start and end dates for the compilation of the events. You can also specify a start time and an end time.

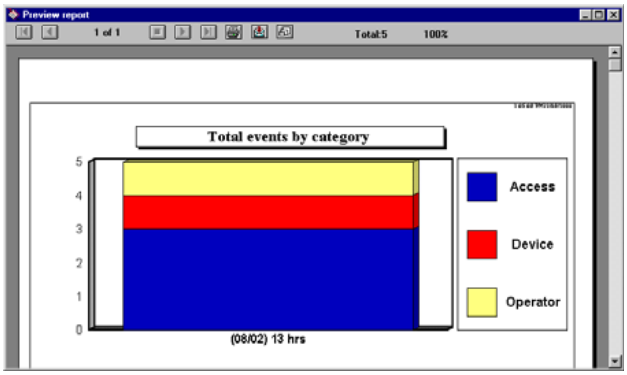
Example of print previews:

List:

Details:



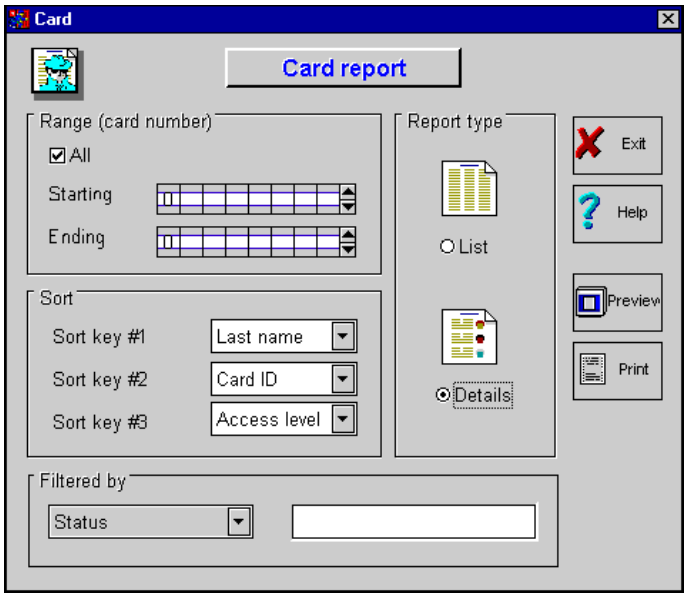
Graphics:



From these screens, you can zoom in / out and print the report.

Card Report

This feature is used to create card reports according to your specific requirements. These reports are not saved, you have to request them as needed.



Field Definition

Range (card number)

These parameters are used to include a series of cards by determining the Starting and Ending identification (decimal) card numbers. You can also select ALL to include all the cards.

Sort (keys)

A card report can be sorted with 3 sort keys. Select the keys from the following fields: Last Name, User Def #1 #2 #3, Access Level, Card ID and Status.

Filtered by

A filter may be used on one of the 7 information fields: Last Name, User Def #1, #2, #3, Access Level, Card ID and Status. To use a filter, select the information field and enter the label or the corresponding description. Example: ACCESS LEVEL and it's label ACCESS001 or USER DEF #1 and it's label SHIPPING

CLERK.

Note: Label field is case sensitive.

Report Type

List

This is a report that is generated in text format. This list is sorted according to the selected sorting keys or in chronological order of creation if no sorting keys are selected. This report contains the following information fields: Card ID, First Name, Last Name, Access Level and Card Status.

Details

This report is generated in text format and also groups the information into 3 sections: General Information, Notes, and Date. This list is sorted according to the selected sort keys or in chronological order of creation if no sort key is selected. This report contains the following information fields: Card ID, First Name, Last Name, User Def #1 #2 #3, Access Level and Card Status, Valid From, Valid Until and Last Modification.

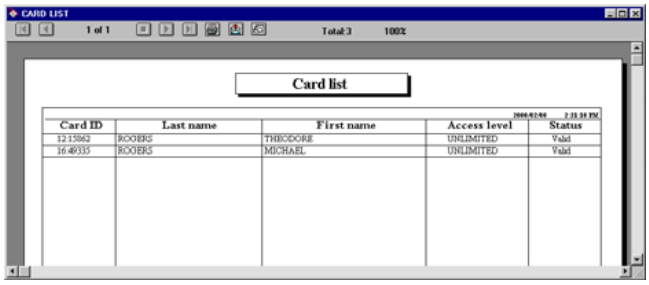
Buttons

Preview & Print

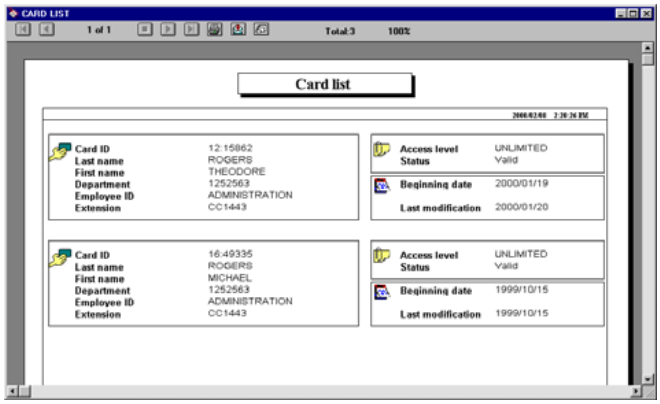
This option lets you preview the report before printing. This option prints the selected report.

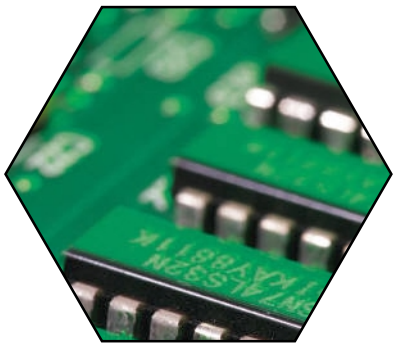
Example of print previews:

List:



Detailed:





SECTION 9

KT-300 - Installation & Configuration

This section introduces the KT-300 door controller, the installation procedure and optional expansion modules.

Technical Specifications

AC power ..... 16VAC, 40VA, class 2 transformer
Battery backup ..... 1 battery 12 V, 7Ah, supervised, provides up to 12 hours of operation
Cabinet measurements ..... 29.9cm H x 28.8cm W x 7.7cm D (11-3/4" H x 11-3/8" W x 3" D) EMT 1.9cm (3/4")
Weight (with metal cabinet) ..... 2,4 kg (5.4 lbs)
Operating temperatures ..... From 2^0 C to 40^0 C (35^0 F to110^0 F)
Reader types ..... Wiegand, proximity, bar code, magnetic, integrated keypad and others
Monitored points ..... 8 monitored points, NO/NC, with / without end-of-line resistors (expandable to 16)
Points maximum wiring ..... 600 meters (2,000 feet) - (AWG #22)
Door strike power ..... 12VDC, 250mA max/each, supervised
Auxiliary outputs ..... 4 outputs, 25mA max/each, Open collector
Relay controlled outputs ..... 2 relay controlled outputs, 25mA (max) each. Open collector to ground (use form "C" relays Kantech # KT-RM1 if needed)
Auxiliary power output ..... 12VDC @ 125mA max, protected and supervised
Reader power outputs ..... 12VDC and 5VDC @ 175mA total, protected and supervised
Communication ports ..... RS232, RS485 and Combus
Communication speeds ..... Up to 115,200 baud (automatic detection)
Firmware Flash memory 128k
RAM memory ..... 128k (512k unit available) Protected by a lithium battery
Network autonomy ..... Distributed data and processing
Certifications / Listing ..... CE, FCC, UL294

KT-300 and Accessories

KT-300 CONTROLLER AND ACCESSORIES	
KANTECH PRODUCT NUMBER	**PRODUCT DESCRIPTION**
KT-300/128k	Door controller with 128kB memory including KT-300CAB, KT-300ACC and KT-300LOCK
KT-300/512k	Door controller with 512kB memory including KT-300CAB, KT-300ACC and KT-300LOCK
KT-300PCB/128k	KT-300/128kB PCB only and KT-300ACC
KT-300PCB/512k	KT-300/512kB PCB only and KT-300ACC
KT-300ACC	Accessory kit including: 2x1.0k ohm, 10x5.6k ohm, 2x120 ohm, PCB standoffs, lock hole cover, ground wire and screwdriver
KT-PC4108	8-Zone input expansion module for KT-300
KT-PC4204	4-Relay and Combus additional power supply module for KT-300
KT-PC4216	16-Output expansion module for KT-300
KT-RM1	External isolation relay SPDT for KT-300 output (RL1/RL2)
KT-LCD4501	LCD time & date display for KT-300
KT-300CAB	KT-300 black metal cabinet including KT-300LOCK
KT-4051CAB	Standard black metal cabinet for KT-PCxxxx modules (order keylock sep.)
KT300LOCK	Keylock for KT-300CAB/KT-4051CAB metal cabinet (2 keys/same as KT-200)
KT-300TAMP	Tamper switch for KT-300CAB / KT-4051CAB metal cabinet
TR1637W/CSA	Transformer, Wire-In, 110V/16V (37VA) CSA
TR1640P/CSA	Transformer, Plug-In, 110V/16V (40VA) CSA
TR1640P/UL	Transformer, Plug-In, 110V/16V (40VA) UL
TR1640W-220	Transformer, Wire-In, 220V/16V (40VA) CE
VC-485	Multi-function communication interface (not UL listed)

Installers familiar with the installation can use the checklist with the "☑" symbol

Step 1. Preparing to Install the KT-300

☑ **Required to install the KT-300:**
- **KT-300 controller with accessory kit**
- **AC transformer 120 / 220 VAC/16 VAC, 40 VA, class 2 ***
- **One 12 volt battery 7A/h ***
- **Ground clamp ***

A visual verification should be made when unpacking the **KT-300**. Any missing item/part or damaged component should be reported immediately.

***Not included**

Step 2. Physical Installation

☑ **Check for ideal indoor location**
☑ **Stay away from electrical or communication devices**

The **KT-300** controller cabinet has been designed to be mounted on a wall without any additional enclosures. The cabinet is large enough to accommodate the battery backup supply and the necessary wiring connections for most applications. EMT (electrical metallic tubing) conduit knockouts are provided in 2.2 cm (7/8") on all sides of the cabinet.

The cabinet should be mounted indoors, in a secure location providing normal temperature and humidity levels, leaving 23 cm (8") clear space around all sides and a minimum of 33 cm (13") clear space in front of the cabinet. The location should be easily accessible for servicing the equipment and it is recommended that controllers be located close to the controlled doors.

Controllers must be located at a minimum distance of 2 meters (6 feet) from any high voltage equipment or wiring and from electrical equipment susceptible of generating electrical interference; at a minimum distance of 1 meter (3 feet) from telephone equipment or lines; and at a minimum of 8 meters (25 feet) from any transmitting equipment.

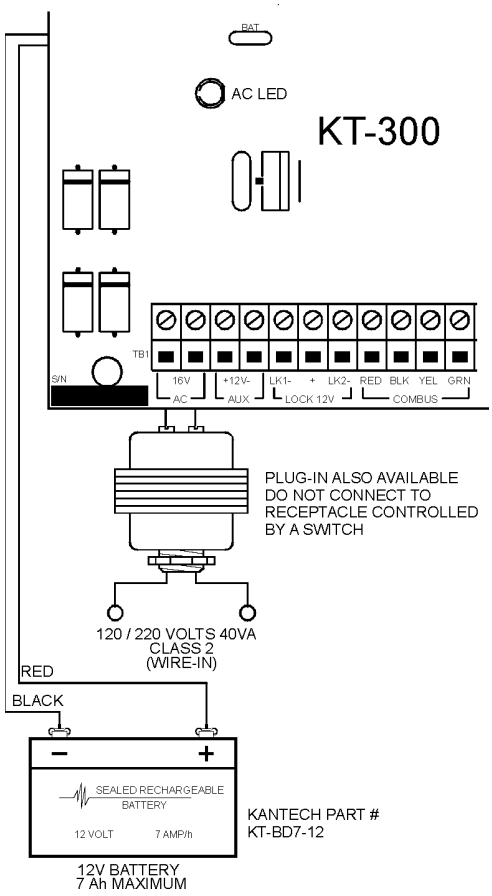
Physical access, using keys, on controlled doors must be provided so that the **KT-300** can easily be accessed for servicing purposes in case of malfunctions.

Step 3. Power Requirements

☑ **DO NOT POWER AT THIS POINT!**
☑ **Install 120 / 220VAC/16VAC, 40VA, class 2 transformer**
☑ **Place battery in cabinet**
☑ **DO NOT POWER AT THIS POINT!**

The **KT-300** controller must be powered by a 16VAC/40VA class 2 wire-in or plug-in transformer.

Power should only be applied to the unit when all connections are completed and tested.



If the AC supply is removed, the backup 12 volt gel type of 7 Amp/hour battery (if fully charged) will support normal operation for up to 12 hours. An internal battery verification will cut the battery power if the battery voltage level falls below 9.5 volt.

Note: The KT-300 unit will not start on battery alone.

Step 4. Earth Grounding

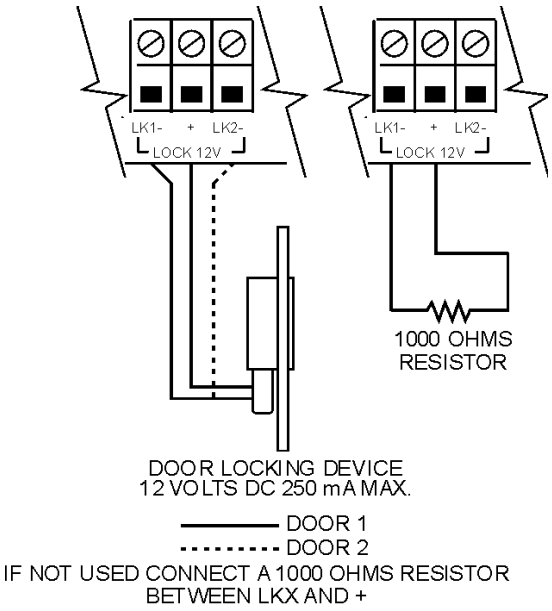
☑ **AWG#18 grounding wire to EGND**

Since the KT-300 uses high performance communications, proper grounding must be provided to ensure proper operation. **An AWG#18 single conductor solid copper wire must be used to ground each controller to a good earth ground as per the local electrical code (be careful of ground loops). The ground clamp should be located below any other ground.**

It is also recommended to install an AWG#18 single conductor copper wire between each controller.

Step 5. Door Locking Devices

- ☑ **Connect door locks to + and LK1- (+ and LK2-)**
- ☑ **Maximum 250mA at 12VDC per output**
- ☑ **Check local "mag locks" regulations**



The LK1-, LK2- and + terminals are located on the bottom left of the **KT-300** controller's terminal strip. The locking device outputs are controlled according to the end user programmed parameters for allowing access to or unlocking doors according to schedules and access levels. These 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 modes (normal or reverse action). The maximum DC current for each lock output is 250mA.

Note: Use 1K ohm EOL (end-of-line resistor) between + and LK- if not used. This resistor is already included within the controller's packaged box (KT300-ACC).

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

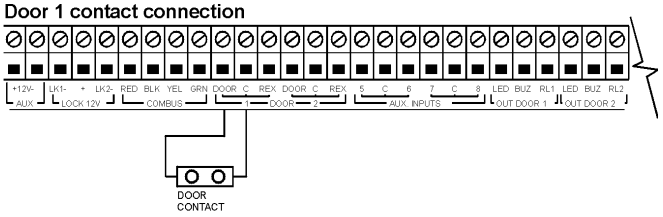
Step 6. Hooking Up Inputs

- ☑ **Connect devices to inputs 1 to 8**
- ☑ **Resistors (included with KT-300) for all inputs 5.6K ohm (if selected)**

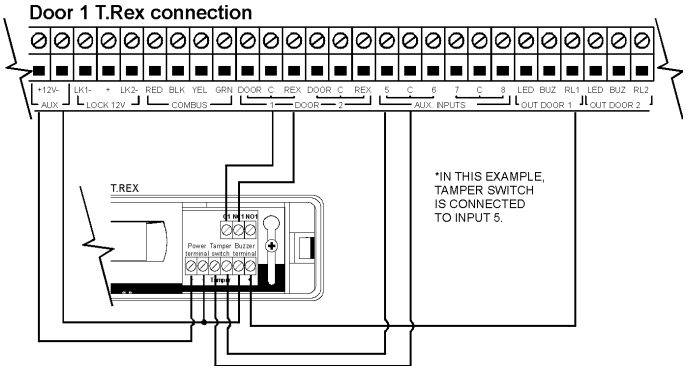
The **KT-300** has an on-board capability of monitoring 8 input points (can be expanded to 16 if KT-PC4108 module is used). Each input is supervised with or without end-of-line resistors (5.6K ohm). The maximum distance of one line is 600m (2,000 feet) with AWG#22 (Kantech part #CBL-R2).

Note: Inputs can be define with: none or one EOLs (end-of-line) resistors according to your EntraPass V3 or WinPass V2 software's settings.

Door 1 contact connection

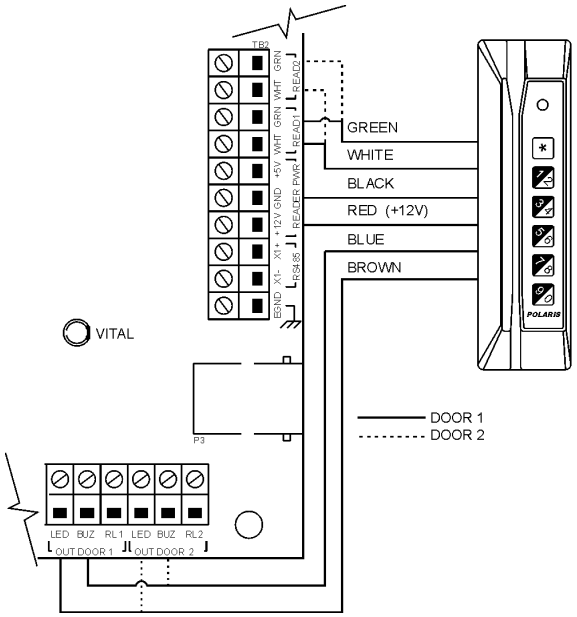


Door 1 T.Rex connection



Inputs 1-2 are automatically reserved for the first controlled door. The contact is assigned input 1 and the associated request-to-exit detector as input 2. Inputs 3 and 4 are automatically reserved for the second controlled door. The contact is assigned input 3 and the associated request-to-exit detector as input 4. There is no obligation to follow these rules but such a standard convention makes it easier for servicing.

Step 7. Readers and Keypads



READER CONNECTION TERMINAL - WARNING: Connecting the red wire lead (or power lead) of a 5VDC reader to the 12VDC terminal may damage the reader. See your reader installation procedure for proper power connection.

Up to 2 readers can be connected to a **KT-300**. They can be installed on one door to control both entry and exit or on two separate doors operating independently to control access in one direction only.

The distance between the readers and the **KT-300** controller varies by reader type (please consult the reader manual for details). Auxiliary outputs provide access operation visual and/or audible feedback at the controlled door . Outputs "OUT DOOR 1 LED & BUZ" are used for the first door and "OUT DOOR 2 LED & BUZ" are used for the second door.

The 12 VDC auxiliary power can also be used to power low current audible devices usually located at the controlled door.

Step 8. Relay Control Outputs

- ☒ **Connect controlled outputs to low voltage devices (25mA max.)**
- ☒ **Add external relays for high voltage devices - (optional - Kantech#KT-RM1)**

The **KT-300** provides two controlled outputs - RL1 & RL2 (open collector to 12 VDC current limited to 25mA). Use a KT-RM1 (optional) to switch larger currents or voltages or to supply a dry contact.

Can be expanded up to 16 controlled outputs when using a KT-PC4216 module. This module allows a maximum of up to 50mA per output. Since the KT-300 only supports 500mA, a power supply module can be used to provide an additional 1A to the Combus.

***Note**: If you are using a KT-PC4204 in "repower" mode and other KT-PC4204 modules that are assigned as relays 1-4 or KT-PC4216 modules that are assigned as relays 1-16 are also connected to the same loop, do not use relay 1 of those modules or relay 1 of the KT-300 door controller (see Combus Repower).*

Step 9. Auxiliary Outputs

- ☒ **Connect auxiliary outputs to readers & local warning devices**

Auxiliary outputs are used for visual and audible signals. They can be activated according to schedules, input conditions or events and local alarms.

Auxiliary outputs "OUT DOOR 1 & 2 LED" provide visual feedback of access operation, and auxiliary outputs "OUT DOOR 1 & 2 BUZ" can activate audible warning devices, such as T.REX, to signal door alarms.

Step 10. Tamper Protection

- ☒ **Install tamper switch on cabinet - (optional - Kantech part#KT-300TAMP)**

A tamper switch may be installed on the unit to detect unauthorized opening of the cabinet (Kantech part no. KT-300TAMP). The normally closed tamper switch is connected to an input (choose an unused input (5 to 8) as tamper input or any other unused inputs on the KT-PC4108 module (if used).

***Note**: The tamper switch is required for a UL listed installation.*

Step 11. Connecting the KT-300 to the RS-485 Bus

- ☒ **Connect RS-485 cable to X1+, X1- and GND**
- ☒ **If not using VC-485: connect a 120 ohm end-of-line resistor on the first and last KT-300 (X- & X+)**
- ☒ **If using VC-485: connect a 120 ohm end-of-line resistor on the last KT-300 only (X- & X+)**

Controllers are linked together through their RS-485 connectors. The maximum communication loop length with the appropriate cable is 1.2 kilometers (4,000 feet). Connecting several **KT-300** controllers at a single point is not acceptable nor are "Y" or "spider web networks".

The RS-485 communication loop should be wired with Ethernet Category 3 double twisted pair network cable (see cable specifications Belden 1227A or equivalent). The RS-485 loop can operate from 1,200 to 115,200 baud under normal conditions. Intermittent communication problems or erratic operation may require to slow down the network speed to 9,600 or 19,200 baud. Varying the network speed does not perceptibly change the operation speed of the system. Usually, most installations should be set at 19,200 baud.

Without a VC-485: Connect a 120 ohm end-of-line resistor between terminals X1- and X1+ of the **first** and **last** KT-300.

With a VC-485: Connect a 120 ohm end-of-line resistor between terminals X1- and X1+ of the **last** KT-300. No need to connect on the first KT-300 since the VC-485 contains an end-of-line resistor.

Step 12. Connecting the Master Controller to the Host Computer

- ☒ **Connect flat cable from the KT-300 to the computer**

From 0 to 30m (0 to 100 feet):

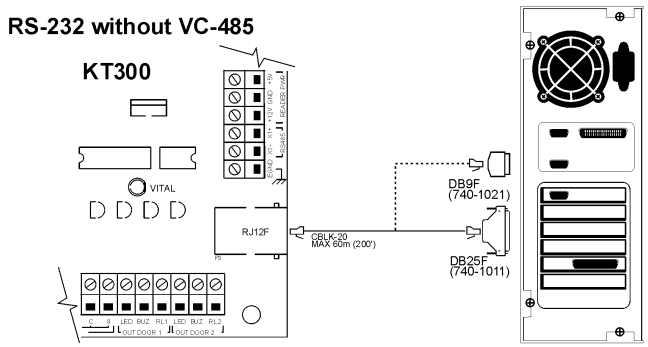
If the local master controller is located less than 30m (100 feet) from the host computer, use the On-Board RS-232 RJ12 jack and the supplied flat cable.

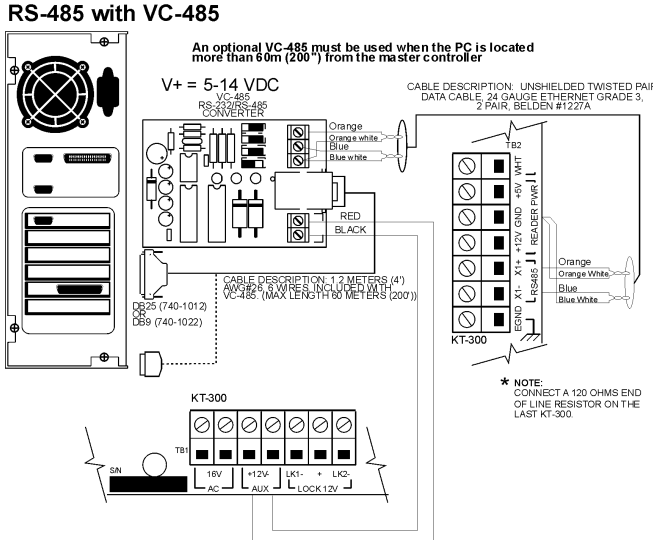
From 30 m to 60m (100 to 200 feet):

Since the master controller can be located up to 60m (200 feet) from the host computer, an extra 100 feet cable can be added to the existing cable (Kantech part no. CAB100ext).

From 60m to 1.2 km (200 to 4,000 feet):

If, on the other hand, the master controller is located more than 60m (200 feet) , an optional VC-485 multifunction communication interface must be used. It can also be used when running communications cable in areas unusually high in electrical noise.





Step 13. Powering the KT-300

☒ **Power the KT-300 controller**

After you have completed all the necessary steps, you may power the KT-300 controller.

How to:

1. Connect AC power
2. Connect the battery

Note: The KT-300 unit will not start on battery alone.

KT-300 FCC & IC Compliance Notice

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received including interference that may cause undesired operation. This class B digital apparatus meets all requirements of the Canadian Interference Causing Equipment Regulations. The **KT-300** is also compliant with EN55022: 1994, amendment 1: 1995, Class B.

KT-300 CE Compliance Notice

This equipment has been tested and found to comply with the limits to EN 50130-4 : 1995.

KT-300 UL Compliance Notice

In order to comply with UL listings, the following has to be respected:

- Use of a UL listed computer
- Use of UL listed readers (Wiegand 26 and 34 bits, mag stripe 26 and 34 bits, have been tested and found to comply)
- Use of a tamper switch on every housing cabinet for the KT-300
- Do not use a VC-485 (not UL listed)
- Do not use the SmartLink option (has not been investigated by UL)
- Use a KT-LCD4501 module on each KT-300 controller
- Do not use a 220V transformer (not UL listed)
- Use only UL listed cables
- Use only UL listed adaptors

Note: Backup battery provides operation of up to 12 hours but has been tested only 4 hours as per Section 33 of UL 294, fifth edition.

Note: All circuits are power limited

Electrical Specifications

VOLTAGE OUTPUTS	MAXIMUM CURRENT	ABSOLUTE COMBINED MAXIMUM
Lock Outputs (12 VDC)	500 mA (250 mA each)	1.5 A
Auxiliary Power (12 VDC)	125 mA	
Reader 5 VDC and 12 VDC	175 mA	
Combus	500 mA	
Battery Charging (12VDC)	250 mA	
OPEN COLLECTOR OUTPUTS	**MAXIMUM CURRENT**	
LED (door 1 & 2)	25 mA (each)	
Buzzer (Buz, door 1 & 2)	25 mA (each)	
Controlled Relay 1 & 2 (RL1 & RL2)	25 mA (each)	

Troubleshooting Communication Problems

Default Initialization:

The **KT-300** default initialization is done at Kantech. The following steps should only be done if :

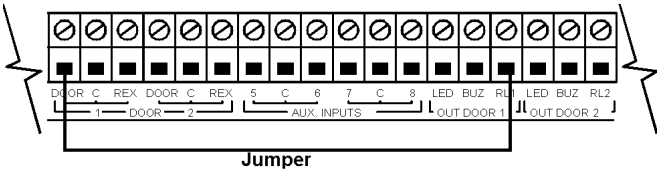
(A) You changed the software (e.g.: you were using EntraPass, then installed WinPass) and there's no communication;

(B) The **KT-300** was communicating via the RS-232 port and you installed a VC-485 to communicate via the RS-485 port;

(C) You were using the **KT-300** at a local site and now want to configure it for remote operation.

How to use the default initialization:

1) Disconnect the transformer and the battery;
2) Remove all connections of DOOR1 and RL1 terminals;
3) Place a jumper between the DOOR1 and RL1 terminals;
4) Apply AC power to the transformer. The VITAL LED should flash 4 times. This means that the controller is in the initialization mode;
5) Disconnect the jumper;
6) When the controller is communicating with the computer, the VITAL LED will flash 3 beats at a time;
7) Reconnect the battery.



KT-300 Controller Maintenance Recommendations

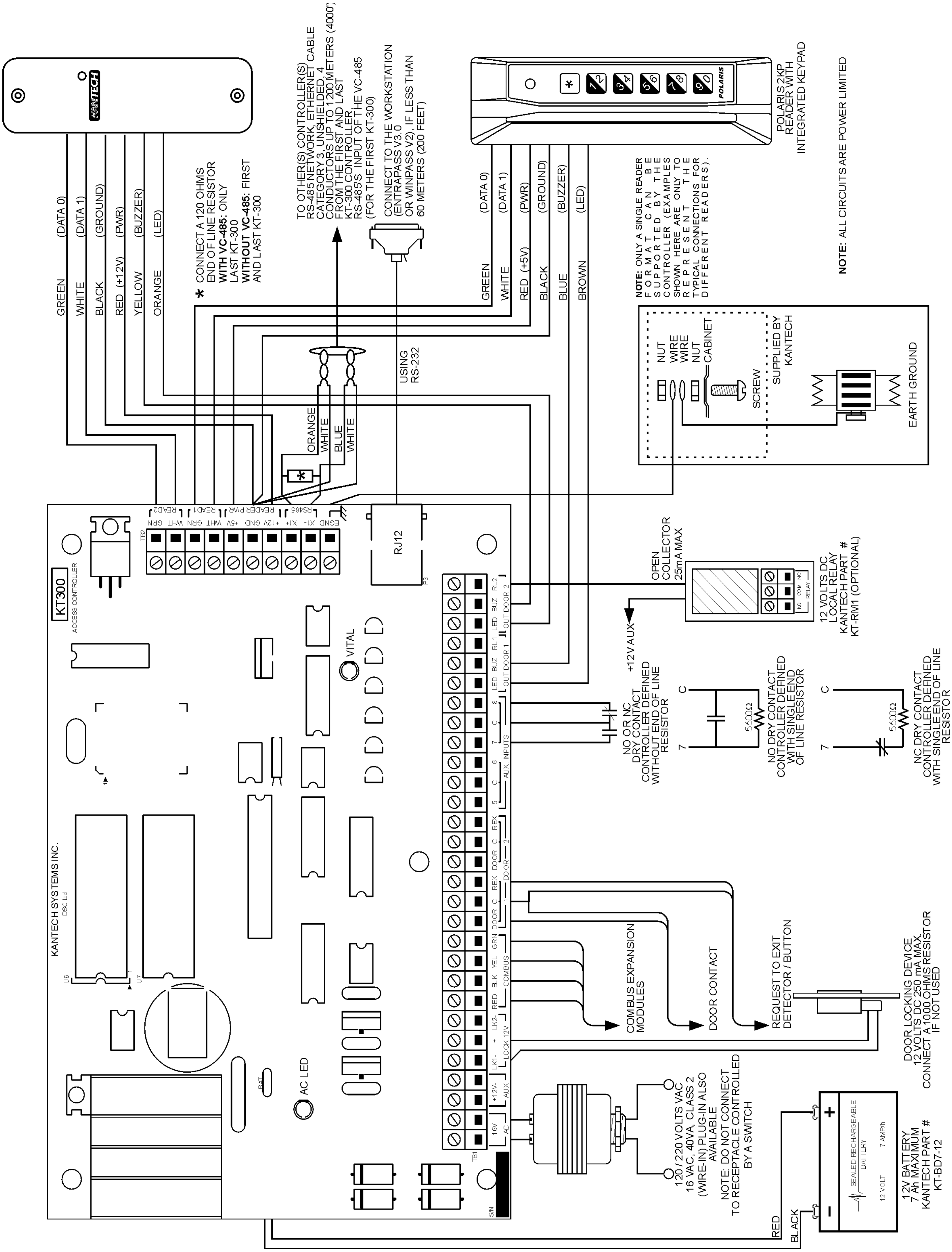
It is highly recommended to test the KT-300 controller by performing the following tests:

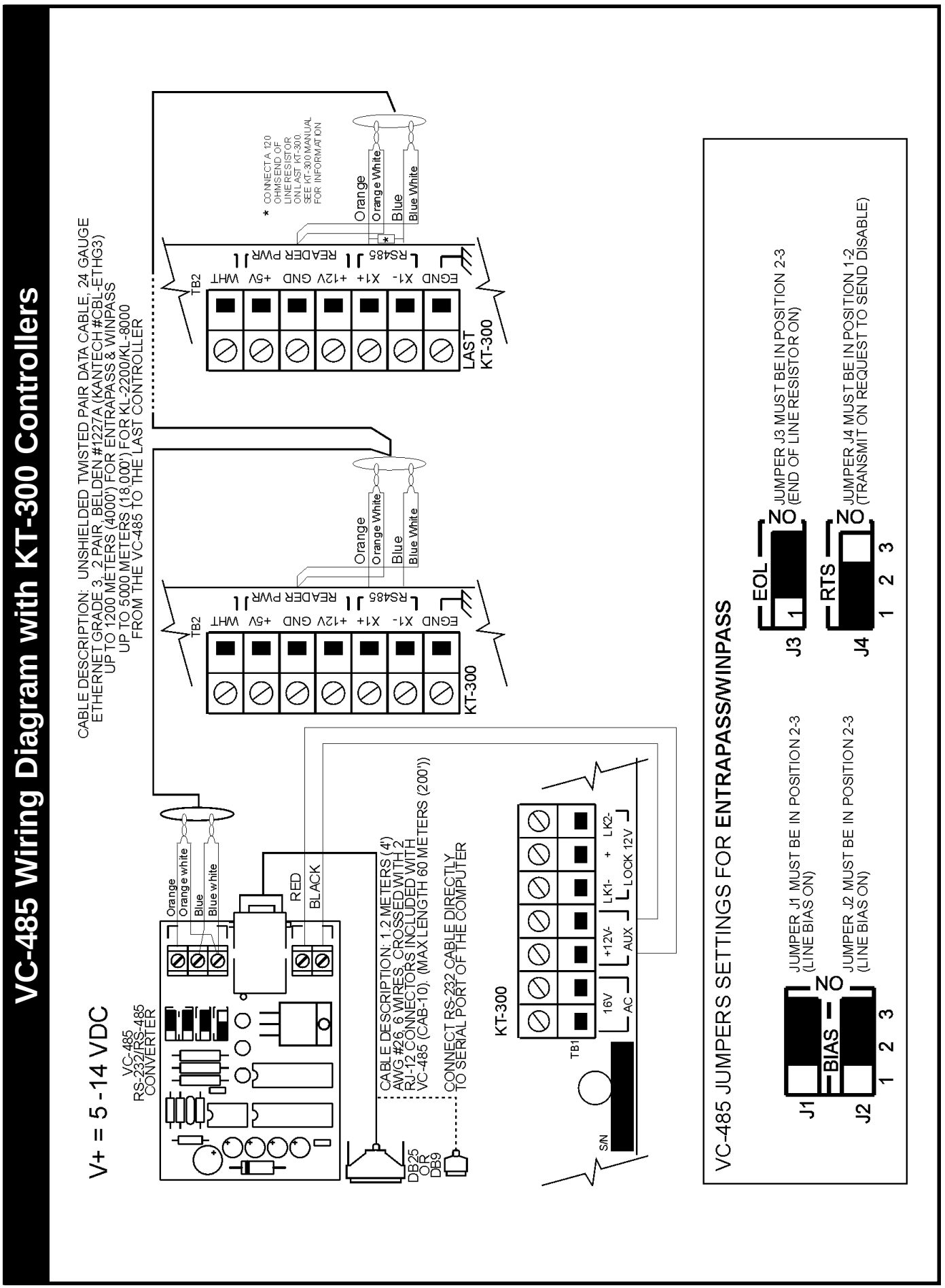
1) Biannual test for battery:

Remove AC power from the controller and connect the battery to the controller for one hour. This test will ensure that if a power failure occurs, the battery will be able to support normal operations. This test should be performed twice a year. Once the test has been performed successfully, reconnect AC power to the controller.

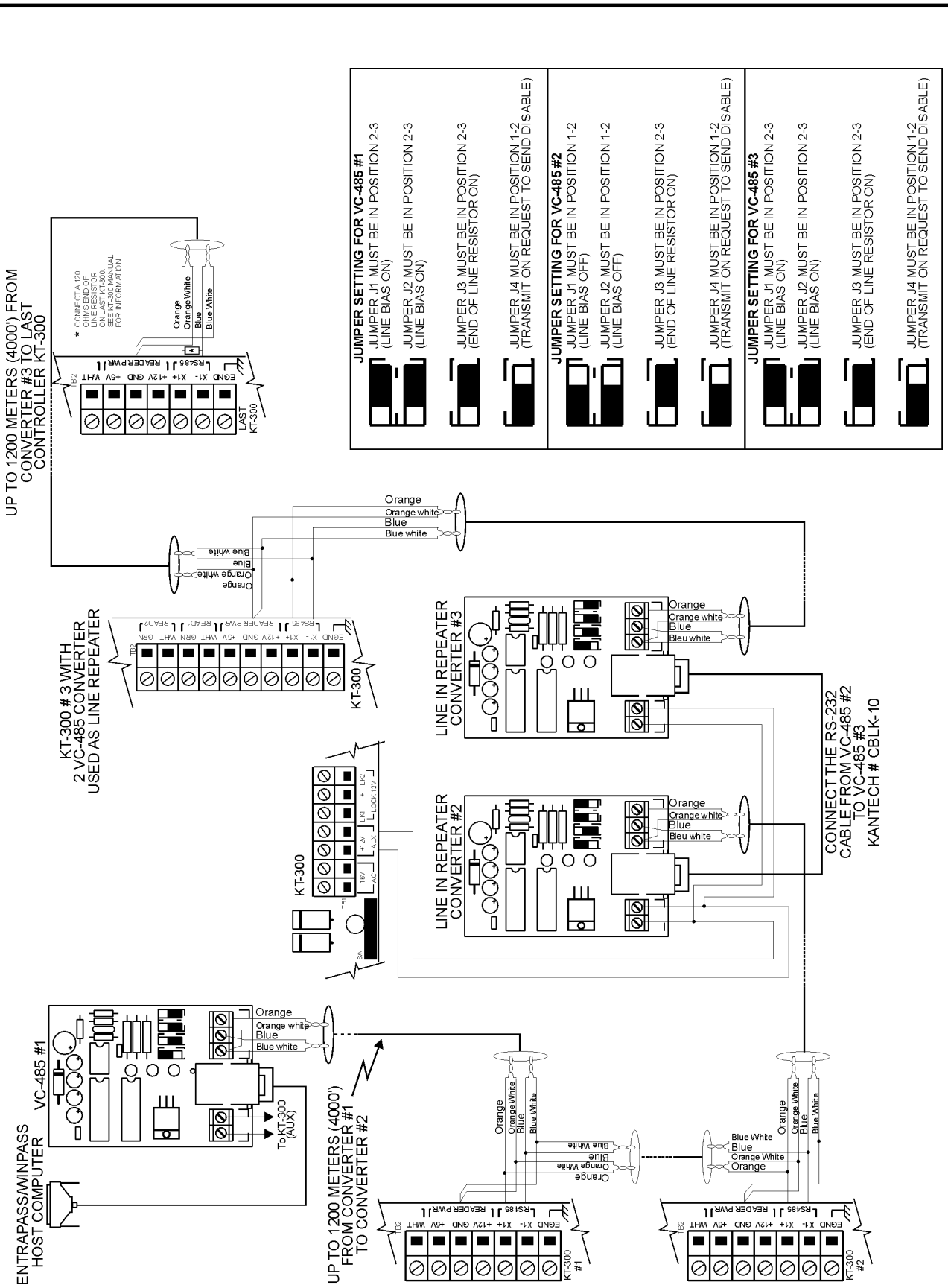
2) Annual test for emergency lithium battery:

Measure voltage of lithium battery when power is totally removed from the controller (AC & DC power). To ensure maximum operation and prevent loss of power, if the lithium battery voltage measures below 2.5VDC, please contact Kantech Technical Support to obtain an RMA # to return the KT-300 for maintenance.


GREEN (DATA 0)
WHITE (DATA 1)
BLACK (GROUND)
RED (+12V) (PWR)
YELLOW (BUZZER)
ORANGE (LED)
* CONNECT A 120 OHMS END OF LINE RESISTOR WITH VC-485: ONLY LAST KT-300 WITHOUT VC-485: FIRST AND LAST KT-300
TO OTHER(S) CONTROLLER(S) RS-485 NETWORK, ETHERNET CABLE CATEGORY 3, UNSHIELDED, 4 CONDUCTORS UP TO 1200 METERS (4000') FROM THE FIRST AND LAST KT-300 CONTROLLER, RS-485'S INPUT OF THE VC-485 (FOR THE FIRST KT-300)
CONNECT TO THE WORKSTATION (ENTRAPASS V3.0 OR WINPASS V2), IF LESS THAN 60 METERS (200 FEET)
USING RS-232
ORANGE
WHITE
BLUE
WHITE
GREEN (DATA 0)
WHITE (DATA 1)
RED (+5V) (PWR)
BLACK (GROUND)
BLUE (BUZZER)
BROWN (LED)
POLARIS 2KP READER WITH INTEGRATED KEYPAD
NOTE: ONLY A SINGLE READER FORMAT CAN BE SUPPORTED BY THE CONTROLLER (EXAMPLES SHOWN HERE ARE ONLY TO REPRESENT THE TYPICAL CONNECTIONS FOR DIFFERENT READERS).
NOTE: ALL CIRCUITS ARE POWER LIMITED
NUT
WIRE
WIRE
NUT
CABINET
SCREW
SUPPLIED BY KANTECH
EARTH GROUND
RJ12
KT300
ACCESS CONTROLLER
VITAL
KANTECH SYSTEMS INC.
DSC Ltd
AC LED
OPEN COLLECTOR 25mA MAX
+12V AUX
12 VOLTS DC LOCAL RELAY KANTECH PART # KT-RM1 (OPTIONAL)
NO OR NC DRY CONTACT CONTROLLER DEFINED WITHOUT END OF LINE RESISTOR
NO DRY CONTACT CONTROLLER DEFINED WITH SINGLE END OF LINE RESISTOR
NC DRY CONTACT CONTROLLER DEFINED WITH SINGLE END OF LINE RESISTOR
5600Ω
COMBUS EXPANSION MODULES
DOOR CONTACT
REQUEST TO EXIT DETECTOR / BUTTON
DOOR LOCKING DEVICE 12 VOLTS DC 250 mA MAX CONNECT A 1000 OHMS RESISTOR IF NOT USED
120 / 220 VOLTS VAC 16 VAC, 40VA, CLASS 2 (WIRE-IN) PLUG-IN ALSO AVAILABLE
NOTE: DO NOT CONNECT TO RECEPTACLE CONTROLLED BY A SWITCH
SEALED RECHARGEABLE BATTERY
12 VOLT 7 AMP/h
12V BATTERY 7 Ah MAXIMUM KANTECH PART # KT-BD7-12
RED
BLACK



VC-485 Wiring Diagram as Line Repeater with WinPass using KT-300



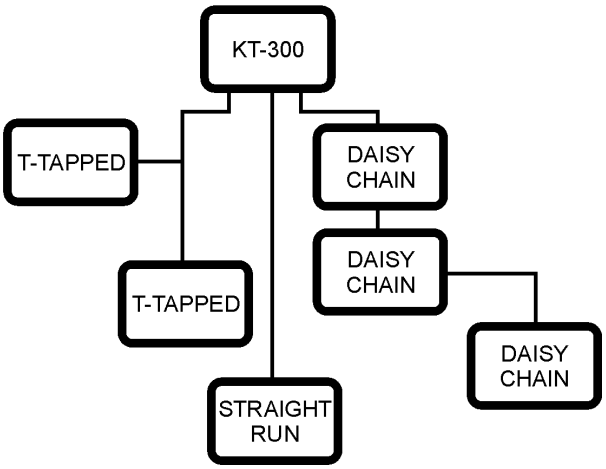
Combus Specifications

The Combus provides 500mA at 12 volt (13.85VDC). The recommended cable is 22 AWG (Kantech part number: CBL-ZN). Each loop (module to KT-300) cannot exceed 300 m (1000') and the total maximum cable length of all connected loops cannot exceed 1200 m (4000').

For example:

- Only four wireruns at 1000' from the KT-300
- Only eight wireruns at 500' from the KT-300
- Only ten (10) wireruns at 400' from the KT-300

Shielded wire should only be used in areas that present excessive RF noise or electromagnetic interference. Modules can be straight run, connected in a daisy chain or T-tapped anywhere on the Combus.



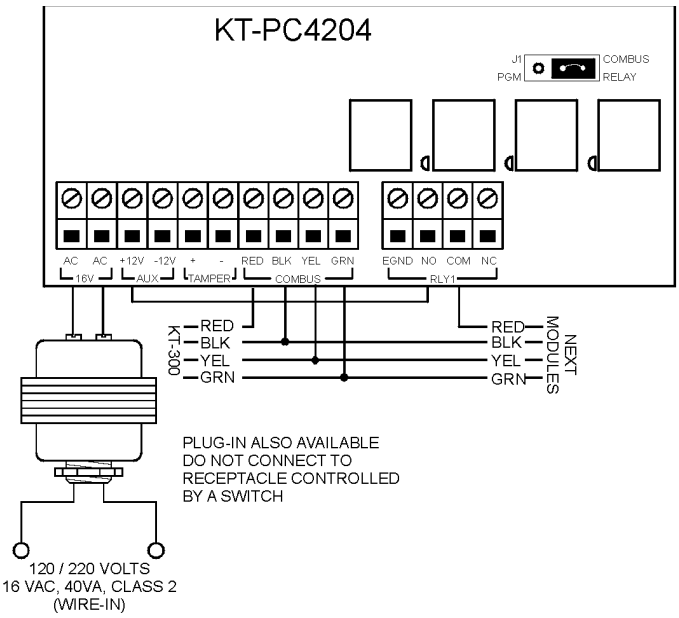
During installation of the modules, it is necessary to inform the system that new modules have been installed on the Combus. To assign the modules to your system (software), see "assigning modules" in the controller definition menu for detailed information.

Combus Repower (if required)

Depending on how many modules are connected to the Combus and how far they are from the **KT-300** controller, you may need to "repower" the controller's Combus. The Combus needs to be "repowered" if the voltage between the black and red wires of the last module of each loop drops below **12.5 volt** (the modules will still operate but there will be no communication between the modules and the controller and an event "Combus module defect" will be generated from the controller). This voltage drops if modules are drawing too much current (500mA maximum for the Combus of each KT-300).

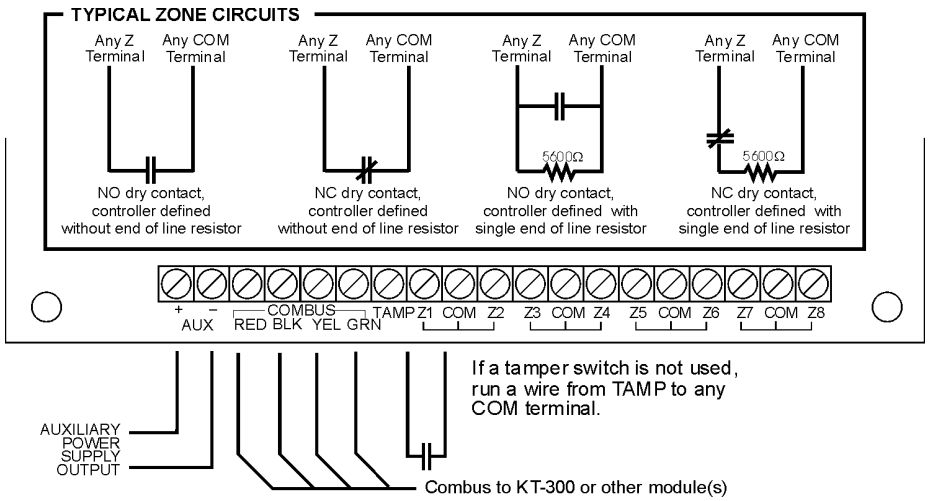
With a multimeter, you should verify this voltage and determine if you need to install a KT-PC4204 in "repower" mode. Using this configuration, you will be provided with an additional 1 amp of current on the controller's Combus. The KT-PC4204 is generally installed at the beginning of the loop.

When using the KT-PC4204 in "repower" mode, the first relay of the module will be reserved for the "repower function". You will have to assign an "all valid" schedule to the first relay so it is "permanently activated" (see your software reference manual in the "controller definition" menu under "assign modules" for the exact procedure). If you are using a KT-PC4204 in "repower" mode and other KT-PC4204 modules that are assigned as relays 1-4 or KT-PC4216 modules that are assigned as relays 1-16 are also connected to the same loop, do not use relay 1 of those modules or relay 1 of the KT-300 door controller. Please also note that all KT-PC4204 modules that are used for Combus repower should be assigned as relays 1-4. *The jumper 1 "J1" on the KT-PC4204 must be moved to the Combus relay position.*



Note: Do not use any power supply other than the KT-PC4204 to repower the Combus. In the event of a power surge or transient, a module may lock up and cease to communicate with the controller. If the **KT-300** loses communication with the module, it will initiate a module reset and will power down the Combus for five seconds in an attempt to reset the problem module. After five seconds, the controller will reapply power to the Combus and the problem module should begin to operate as intended.

KT-PC4108 - 8-Zone Input Expansion Module



Introduction

The **KT-PC4108** module is a zone input module that adds up to 8 fully programmable zones to the KT-300 controller.

1. Specifications

- Connects to the controller via 4-wire Combus
- Current draw: 30 mA (from Combus)
- Supports single end-of-line and no end-of-line (5600 ohm resistors) zone loops.
- AUX+ output: 12VDC, 250mA max. (drawn from Combus)
- Tamper contact input

2. Installing the KT-PC4108

2.1 Unpacking

The KT-PC4108 package includes the following parts:

- One KT-PC4108 circuit board
- 16 end-of-line resistors (5600 ohm)
- Four (4) plastic standoffs

2.2 Mounting

The KT-PC4108 module should be located inside a compatible cabinet (Kantech part no. KT-4051CAB), mounted in a dry, secure location. Preferably, it should be placed at a convenient distance from the connected devices.

Perform the following steps to mount the unit:

1. Press the four (4) plastic standoffs through the mounting holes on the back of the cabinet.
2. Secure the cabinet to the wall in the desired location. Use appropriate wall anchors when securing the cabinet to drywall, plaster, concrete, brick or any other surfaces.
3. Press the circuit board into the four (4) plastic standoffs to secure the unit to the cabinet.

Once the unit is mounted, wiring may be started.

2.3 Installation and Wiring

Before beginning to wire the unit, ensure that all power (AC transformer and battery) is disconnected from the controller.

Perform the following steps to complete wiring:

1. Connect the four Combus wires to the KT-PC4108. Connect the red, black, yellow and green Combus wires to the RED, BLK, YEL and GRN terminals, respectively.
2. Complete all zone wiring to the zone input terminals (Z1-Z8). See the EntraPass or WinPass manual for details on zone wiring configurations.
3. Connect the external tamper switch, if used.

Consult the wiring diagram above for further information.

2.4 Applying Power

After all wiring is completed, apply power to the controller. Connect the battery leads to the battery, then connect the AC transformer.

***Note**: Do not connect the power until all wiring is complete.*

3. Assigning the Module

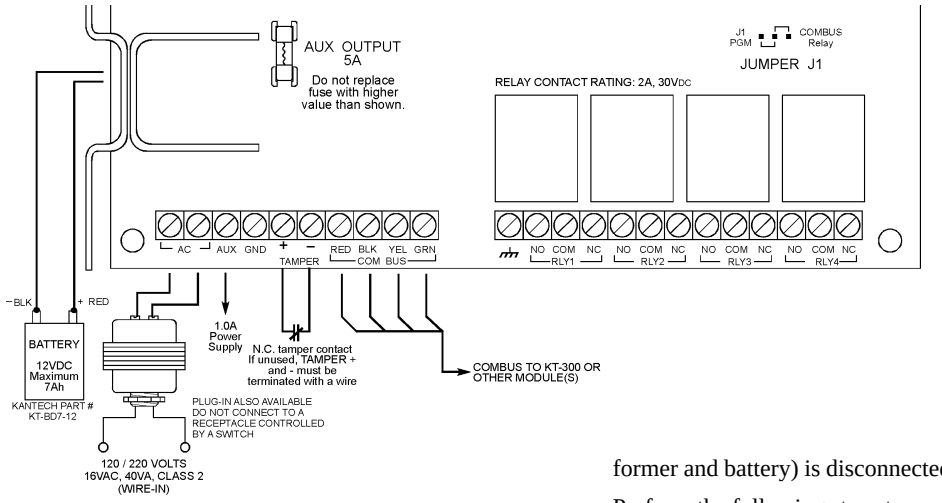
Once all wiring is complete, the module must be assigned to the system. To assign the module, perform the following:

Once all wiring is complete, the module must be assigned to the system. To assign the module, perform the following steps:

1. Establish communication between the PC and the controller,
2. Remove the tamper switch wire,
3. A serial number should be displayed on the screen. In the same window where the serial number is located, you should see the type of module and on which controller it is connected,
4. From the software, select the functionality of the module and enter the serial number in the appropriate field (see controller definition -- assign modules for more details).

***Note:** Don't forget to reconnect the tamper switch (or the wire, if there is no tamper switch)*

KT-PC4204 - 4-Relay and Additional Power Supply Module



Introduction

The **KT-PC4204** module is an output module with four programmable relays. This module can be used to repower the Combus. The KT-PC4204 is also used for elevator control or other purposes.

Note: Do not use any power supply other than the KT-PC4204 module to repower the Combus. If a power supply other than the KT-PC4204 is used, the Combus repower function will not operate as intended.

1. Specifications

Current draw: 30 mA (from Combus) - 40VA 16V transformer required - Maximum 7A/h battery required - Connects to the controller via 4-wire Combus - Four programmable relay contacts rated 2A, 30VDC - AUX current: 1.0A maximum - Tamper contact input - Can be used to repower the Combus - Can be used for elevator

2. Installing the KT-PC4204

2.1 Unpacking

The KT-PC4204 package should include the following parts/items:

- One KT-PC4204 circuit board
- One ground wire assembly
- Five plastic standoffs
- One 5A replacement fuse

2.2 Mounting

The KT-PC4204 should be located inside a compatible cabinet (Kantech part no. KT-4051CAB), mounted in a dry, secure location. Preferably, it should be placed at a convenient distance from the connected devices.

Perform the following steps to mount the unit:

1. Press the five plastic standoffs through the mounting holes at back of the cabinet
2. Secure the cabinet to the wall in the desired location. Use appropriate wall anchors when securing the cabinet to drywall, plaster, concrete, brick or other surfaces
3. Press the circuit board into the plastic standoffs to secure the module to the cabinet.

Once the unit is mounted, wiring may be started.

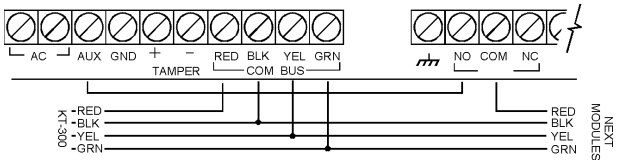
2.3 Installation and Wiring

Before beginning to wire the unit, ensure that all power (AC transformer and battery) is disconnected from the **KT-300** controller.

Perform the following steps to complete wiring:

1. Connect the four Combus wires to the KT-PC4204 Connect the red, black, yellow and green Combus wires to the RED, BLK, YEL and GRN terminals, respectively.

   If the module is used for Combus Repower, connect the Combus wires according to the following diagram. Note that for this option, Jumper J1 must also be set for "Combus Relay."



2. Complete all output wiring
3. Connect the external tamper switch, if used

2.4 Applying Power

After all wiring is completed, apply power to the **KT-300**. Connect the battery leads to the battery, then connect the AC transformer. Then, connect power to the KT-PC4108 the battery leads followed by the AC transformer.

***Note**: Do not connect the power until all wiring is complete.*

3. Assigning the Module

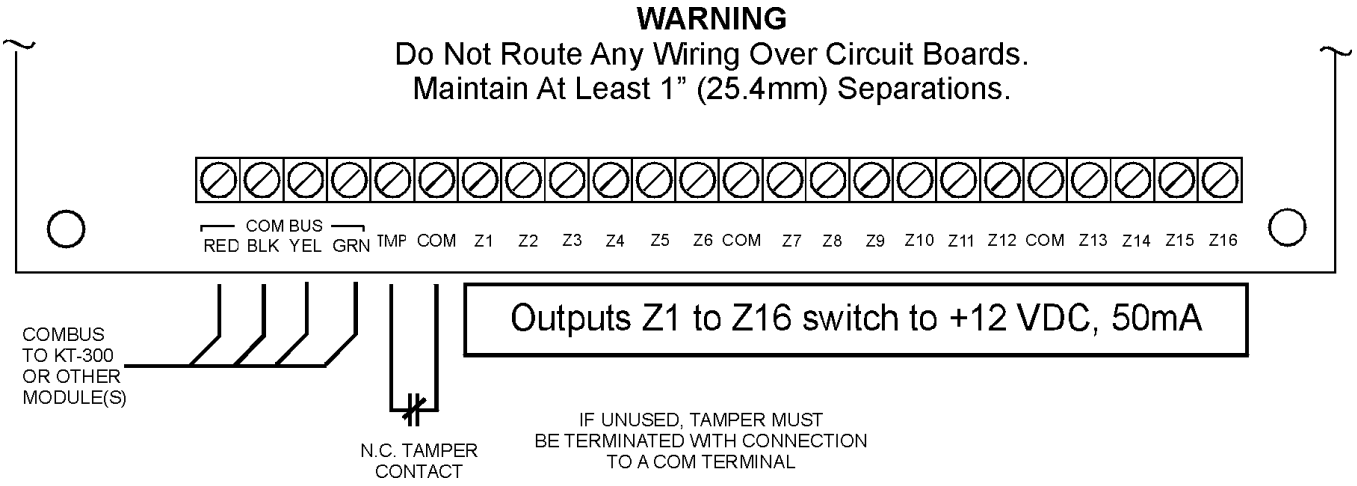
Once all wiring is done, the module must be assigned to the system. To assign the module, perform the following:

1. Establish communication between the PC and the controller,
2. Remove the tamper switch wire (or only the wire if tamper switch is not used),
3. A serial number should be displayed on the screen. In the same window where the serial number appears, you should see the type of module and on which controller it is connected,
4. From the software, select the functionality of the module and enter the serial number in the appropriate field (see your software reference manual under controller definition -- assign modules for more details),
5. If the module is used in "repower" mode, assign an "all valid" schedule to relay 1 and assign the module's functionality to "relay 1 to 4" in your software.

***Note:** Don't forget to reconnect the tamper switch (or the wire, if there is no tamper switch).*

***Note:** Ensure that Jumper J1 is set to "Combus Relay" position if used as "repower".*

KT-PC4216 - 16-Zone Output Expansion Module



Introduction

The **KT-PC4216** module is an open collector to 12 VDC 16- zone output module. Can be used for elevator access control (may require additional hardware) or other purposes.

1. Specifications

- 16-output low current module, 12V, 50mA max. each, power drawn from Combus (since Combus can handle a maximum of 500mA, a KT-PC4204 module in "repower" mode can be used to increase the current of the Combus of 1A)
- Connects to KT-300 via 4-wire Combus
- Nominal current draw of 15mA
- Tamper contact input
- Can be used for elevator control

2. Installing the KT-PC4216

2.1 Unpacking

The KT-PC4216 package should include the following parts:

- One KT-PC4216 circuit board
- 4 plastic standoffs

2.2 Mounting

The KT-PC4216 should be located inside a compatible cabinet (Kantech part no. KT-4051CAB), mounted in a dry, secure location. Preferably, it should be placed at a convenient distance from the connected devices.

Perform the following steps to mount the unit:

1. Press the four plastic standoffs through the mounting holes at back of the cabinet.
2. Secure the cabinet to the wall in the desired location. Use appropriate wall anchors when securing the cabinet to drywall, plaster, concrete, brick or other surfaces.
3. Press the circuit board into the plastic standoffs to secure the module to the cabinet.

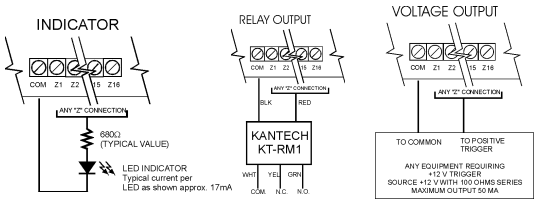
Once the unit is mounted, wiring may be started.

2.3 Installation and Wiring

Before beginning to wire the unit, ensure that all power (AC transformer and battery) is disconnected from the controller.

Perform the following steps to complete wiring:

1. Connect the four Combus wires to the KT-PC4216. Connect the red, black, yellow and green Combus wires to the RED, BLK, YEL and GRN terminals, respectively.
2. Complete all output wiring as illustrated on this page:



3. Connect the external tamper switch, if used.

***Note**: Current is drawn from the Combus. May require a KT-PC4204 power supply module if drawing too much current from the Combus.*

Consult the wiring diagrams for further information.

2.4 Applying Power

After all wiring is completed, apply power to the **KT-300**. Connect the battery leads to the battery, then connect the AC transformer.

***Note**: Do not connect the power until all wiring is complete.*

3. Assigning the Module

Follow the instructions below for assigning and programming your KT-PC4216 module.

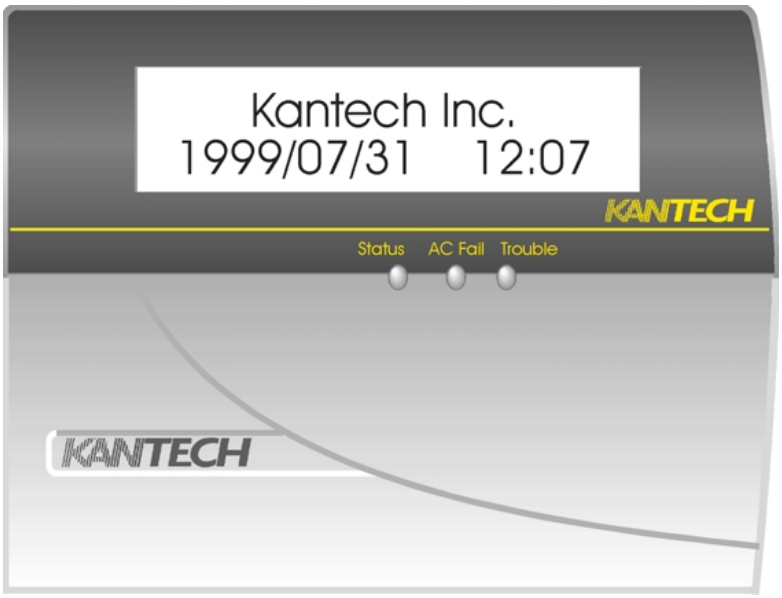
Follow these steps to assign the module(s):

1. Establish communication between the PC and the controller,
2. Remove the tamper switch wire (or only the wire if tamper switch is not used),
3. A serial number should be displayed on the screen. In the same window where the serial number is located, you should see the type of module and on which controller it is connected,
4. From the software, select the functionality of the module and enter the serial number in the appropriate field (see your software reference manual under controller definition -- assign modules for more details).

***Note:** Don't forget to reconnect the tamper switch (or the wire, if there is no tamper switch).*

***Note:** If you are using a KT-PC4204 in "repower" mode on the same loop, do not use the first relay of the KT-PC4216.*

KT-LCD4501 - LCD Time & Date Display Module



Introduction

The **KT-LCD4501** module is an LCD with integrated keypad which presents date and time via a 32-character liquid crystal display.

1. Specifications

- Connects to control panel via 4-wire Combus
- Current draw: 50mA (from Combus)
- Inputs' status (green), AC Fail (red) and Trouble (yellow) status lights

2. Installation

2.1 Unpacking

The KT-LCD4501 package includes the following parts/items:

- One KT-LCD4501 keypad
- Four mounting screws

2.2 Mounting

The keypad should be mounted where it is accessible to designated points of entry/exit. Once a dry and secure location is selected, perform the following steps to mount the keypad:

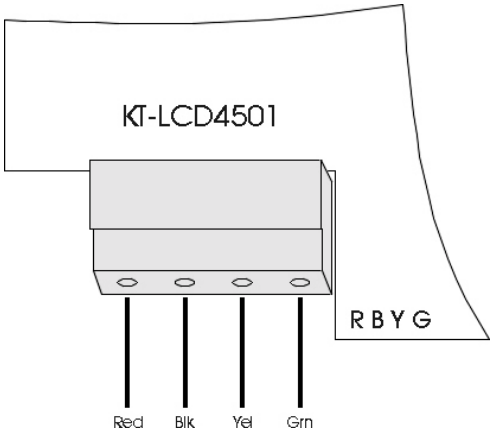
1. Remove the keypad backplate by loosening the screw located at the base of the unit.
2. Secure the keypad's backplate to the wall in the desired location. Use the included screws.

Before mounting the keypad to its backplate, complete keypad wiring.

2.3 Wiring

Before beginning to wire the unit, ensure that all power (AC transformer and battery) is disconnected from the control panel. To complete keypad wiring, connect the four Combus wires (red, black, yellow and green) to the keypad terminals (R B Y G).

Consult the diagram below:



3.4 Applying Power

Once all wiring is complete, apply power to the controller. Connect the battery leads to the battery, then connect the AC transformer.

Note: *Do not connect the power until all wiring is complete.*

3. Assigning the Keypad

Once all wiring is complete, the module must be assigned to the system. To assign the module, perform the following steps:

1. Establish communication between the computer and the controller,
2. Press the pound key (#) on each keypad,
3. A serial number should be displayed on the screen. In the same window where the serial number is displayed, you should see the type of module and on which controller it is connected,
4. From the software, select the functionality of the KT-LCD4501 and enter the serial number in the appropriate field.

SECTION 10

KT-300 Compatible products

This section introduces the various products that are compatible with the KT-300 door controller.

ioProx

Multi-Function Proximity Readers

With 4 new **IoProx** readers to choose from, you will find one that's right for your application! Their attractive, compact and weatherized design makes them suitable for installation in various indoor and outdoor environments.

The **IoProx** reader electronics are vandal and weather resistant and are encapsulated in epoxy potting. All readers have an integrated piezo buzzer and bicolor LED indicating system/reader status. Optional tamper switch and command button modules are available.

P400

P300

UNSHIELDED Cable

The **IoProx** readers can be installed using #22AWG UNSHIELDED cable to a distance of up to 1000' (300m) from the controller. Using this type of cable significantly reduces installation costs.

Integrated Command Buttons (P200XSF and P400XSF)

An optional integrated command button module can be added to the P200 and P400 models. The two buttons are form C contacts that can be used to arm/disarm an alarm panel, that can be connected to a buzzer to serve as a doorbell, etc.

Voltage Requirements

The readers accept a voltage of 5 to 14 VDC and can be used with virtually any controller on the market. This will allow a system to be upgraded simply by changing the readers and cards, without needing to recable.

P200

P100

Easy Installation

The **IoProx** readers' small size provides flexibility for mounting: they can be installed on walls, door mullions, or single and double gang boxes.

Read Range

The read range increases with reader size. Depending on the model selected and the environmental conditions, the read range varies from up to 4in. (P100XSF) to up to 6in. (P400XSF).

XSF Security

XSF format is only compatible with Kantech software products. The readers recognize over 137 billion unique codes. Using Kantech's XSF cards (eXtended Secure Format) provides increased security and absolute guarantee against card duplication. The readers are also available in standard 26 bit Wiegand format.

ShadowProx Readers

MOTOROLA

SH-X1

SH-X4

The **SH-X1, SH-X2** & **SH-X4** proximity readers are the next generation of the popular ***ShadowProx™*** line of proximity readers, cards, and tags. Sleek and contemporary styling allows for installation in the most prestigious locations.

Following the practical tradition of the ***ShadowProx™*** line, these units are mountable on door mullions (SH-X1), on walls, on single gang electrical boxes (SH-X2) or on a single or double gang electrical box, as well as any flat surface (SH-X4). For added style and convenience, they are more compact and will enhance both the interior and exterior decor of any professional environment.

SH-X2

Single Piece Construction Proximity Reader, the **SH-2KP** proximity reader is designed in format and finishing suitable for installation in the most prestigious locations. The single piece construction also provides for faster installation and more reliability.

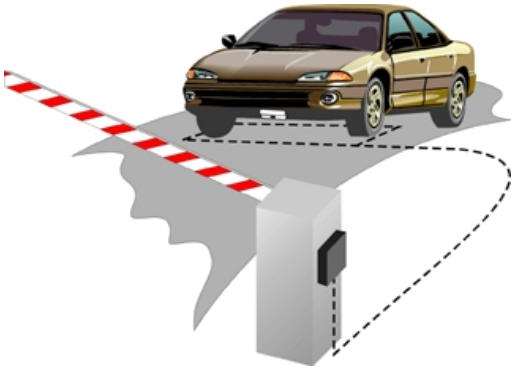
SHADOW PROX

SH-2KP

SHV-60E Vehicle Reader

The ***ShadowProx*** VID system provides automatic identification of cars, trucks, buses, fork lifts or other vehicles approaching a gate or controlled roadway. Upon reading the vehicle's tag, the system will either activate the gate, overhead door mechanism or deny access depending on the vehicle's access level. The system provides managers with new abilities for recording and tracking the flow of vehicles, crates, containers, etc. in and out of access areas.

Operation



Each vehicle is equipped with a rugged SH-V159 vehicle tag. The tag can be read at speeds up to 40 km (25mph). When the vehicle proceeds over the buried antenna, the tag's unique identification is transmitted to the access control system. For higher security application, adding an additional ***ShadowProx*** reader for the driver's own card would record both vehicle and driver ID before opening the gate.

Two types of installations

The tag can be installed under the vehicle for detection by a buried cable antenna or, on the side of the vehicle, to work with a standard SH-X5 reader mounted on a wall or post. For practical reasons, there is a choice to be made of either undercarriage or side mounted tags.

Buried antenna

Typically, a cable totalling 53 meters (175 feet), including leading length of 7.6m (25') to connect to the **SH-V60E** is buried in loops under the road surface over an area of 1.8m (6 feet) by 46cm (18"). The cable is wired to the **SH-V60E** reader electronics housing located in a dry heated environment. The **SH-V60E** can be located at a maximum distance of 30m (100') from the buried loop. From there the **SH-V60E** is wired to the KT-300 using regular reader cable. The tags can be read at a distance of up to 81cm (32") from the road.

Side mounted reader

A SH-X5 extended range reader is installed against a wall or on a post located as close as possible to the vehicle's side where the tags will be mounted. Because the SH-V159 is an active tag, the read range can be up to 2.4 meters (8 feet). The reader is wired to the KT-300 controller in the usual way.

HID Readers

MiniProx

The **MiniProx**™ reader boasts a new slim design for a low-profile appearance. The attractive new design allows the Mini-Prox to be mounted indoors and match any decor.

ThinLine II

The **ThinLine II**™ reader provides the same performance and reliability as the MiniProx but with a low profile appearance. Housed in an industry standard switch plate, the ThinLine is an attractive addition to any installation.

ProxPro with keypad

The **ProxPro**™ reader combines all of the electronics usually found in two separate packages into a single, architecturally attractive enclosure that mounts to a standard single-gang box. With its inherently weatherproof design, the reader is easily mounted either indoors or out. Integrated keypad option (KP) is available on this reader.

ProxPro

The long read range of the **MaxiProx**™ reader provides a significant user advantage by minimizing or eliminating the effort required to present an access control card. This makes the reader ideal for installations incorporating parking control, or where special consideration is needed to facilitate access.

MaxiProx

ProxPoint

The **ProxPoint**™ proximity reader is so small and inconspicuous, you hardly know it's there. In addition to its small, attractive design, all of reader electronics are epoxy-potted making it ideal for both indoor and outdoor applications. The **ProxPoint**™ reader is priced to fit the tightest of budgets. The **ProxPoint**™ reader is sealed in a rugged, weatherized polycarbonate enclosure designed to withstand harsh environments as well as provide a high degree of vandal resistance. This allows reliable performance anywhere.

POLARIS™ Polaris Reader

Polaris 2KP

The POL -2 and POL-2KP magnetic stripe readers are the new generation of the POLARIS series. Packed with new features, the POLARIS-2 series provides the right combination of quality and reliability.

Bidirectional card reading

A card can be swiped through the reader in both directions and the reader's microprocessor automatically detects and rejects read errors. This prevents improper data being sent to the access control system.

Integrated keypad (POL-2KP)

With an integrated 6-touch membrane keypad, the Polaris-2KP helps bring down the cost of your installations. The high quality lexan membrane is rated for 1 million duty cycles. The Polaris-2 keypad also provides a special "star" button used to trigger the arming or disarming of most alarm panels.

4 configurable outputs

Configurable outputs provide flexibility for the installer. Wiegand 26 bits, Wiegand 34 bits, ABA clock & data and ABA-Wiegand outputs can be programmed easily in the field without special programming cards or tools. These configurable outputs make the Polaris-2 series compatible with most access control systems on the market.

Wireless Transmitters

Extra long read range of up to 25 meters or more

The **WLS** series transmitters and outdoor receiver provide extra long read range using wireless technology in the 304MHz range. Ideal for parking and garage entrance applications. The read range can be extended by installing the power antenna remotely.

- Available in KSF (Kantech Secure Format) and Wiegand 26 bit format,
- Typical read range of up to 25 meters (80 feet),
- Receiver powered directly from the controller.

WLS-5401

WLS-3710

WLS-3700

BC-301 Bar Code Reader

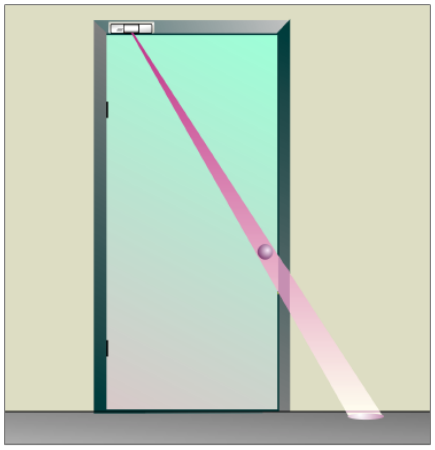
Fully waterproof, its tough cast aluminium shell is treated with black polymer coating for extra durability. Reads most common bar code formats, including :Code 39, Interleaved 2 of 5, UPC/EAN, Codebar. Bi-color LED. Use this reader with your EntraPass to read just about any existing bar codes cards supplied by the end user.

BC-301

T-REX Exit Detector

First of Kind ! The **T-REX** creates a new standard and provides a complete solution to exit detection and door surveillance for access control applications. Outstanding innovations such as X-Y Targeting™ and DSP implement to make the **T-REX** the fastest and most reliable exit detector on the market.

T-REX



X-Y Targeting™ targets a specific area of detection.

While some exit detectors on the market offer adjustments of detection pattern with masking or horizontal alignment, the T-Rex is the first detector to offer vertical detection targeting using two adjustable louvers located in the detection chamber. The installer can "trim" the detection area by adjusting these louvers from 90º down to a minute 5º. Horizontal adjustment is provided by rotation of the lens. Added security: These two adjustments allow the installer to mount the detector in a way that the detector will not "hit" the floor along the doorjamb. This new and exclusive feature prevents attempts to circumvent the door supervision by sliding objects underneath the door that would otherwise be detected by sensors mounted in the traditional way.

DSP prevents false alarms and broken noses !

Kantech's T-Rex utilizes infrared detection coupled with DSP (Digital Signal Processing) sampling specifically designed for access control applications. There is a substantial operation difference between a common infrared intrusion motion detector and the T-Rex. An intrusion detector operates at low sensitivity levels and is looking for the positive presence of a human. An exit detector must detect an extremely fast movement of a hand (the target) about to push the door or turn the door handle. Contrary to intrusion applications, a failure to detect in an exit application will actually cause a false alarm or worse a broken nose !

PB-EXIT Exit Button

The **PB-EXIT** exit button is a spring loaded, momentary square exit button mounted on a stainless steel plate. The SPDT contacts switch when the button is depressed and returns when released. The contacts are UL listed with a 10AMP capacity. This button could be used for momentary release of fail-safe or fail-secure electric locks. It may also be used to input an exit signal to the access control system. In some areas, local building or fire safety regulations may limit the use of exit buttons and it is recommended to consult or get approval prior to installing exit buttons.

PB-EXIT

Optional Expansion Modules

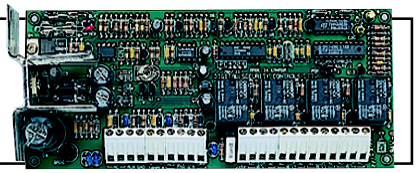
The Combus terminals on the **KT-300** controller are used to connect expansion modules to add more inputs, outputs, relays and LCD keypads. The four Combus terminals of the main panel must be connected to the four Combus terminals or wires of all modules.

There are 4 expansion modules that can be connected to **KT-300s** Combus (more specifications of each of these modules can be found in the KT-300 installation manual).

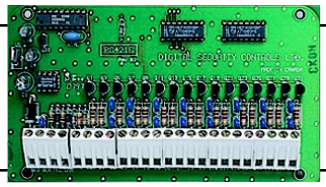
KT-PC4108

The **KT-PC4108** module is a zone input module that adds up to 8 fully programmable zones to the **KT-300** controller.

The **KT-PC4204** module is an output module with four programmable relays. This module can be used to repower the Combus. The KT-PC4204 is also used for elevator control or other purposes.



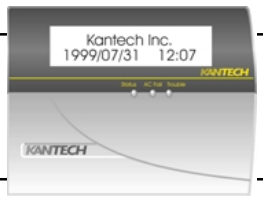
KT-PC4204



KT-PC4216

The **KT-PC4216** module is an open collector to 12 VDC 16-zone output module. Can be used for elevator access control (may require additional hardware) or other purposes.

The **KT-LCD4501** module is an LCD with integrated keypad which presents date and time via a 32-character liquid crystal display and is used for time and attendance functions.



KT-LCD4501

Modules Housing Cabinet

Measurements: 16.8" H x 10.4" W x 4.1" D

Color: Black

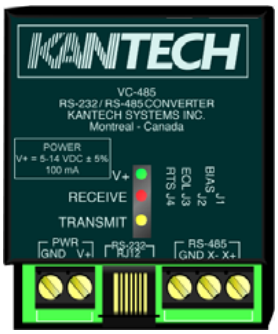
Kantech part no.: KT-4051CAB

Cabinet will hold either:

a) One (1) KT-PC4204 power supply/relay module with room for batteries and one (1) KT-PC4108/KT-PC4216.

b) Three (3) KT-PC4216/KT-PC4108. modules

KT-4051CAB



VC-485_F

VC-485 Multifunction communication interface

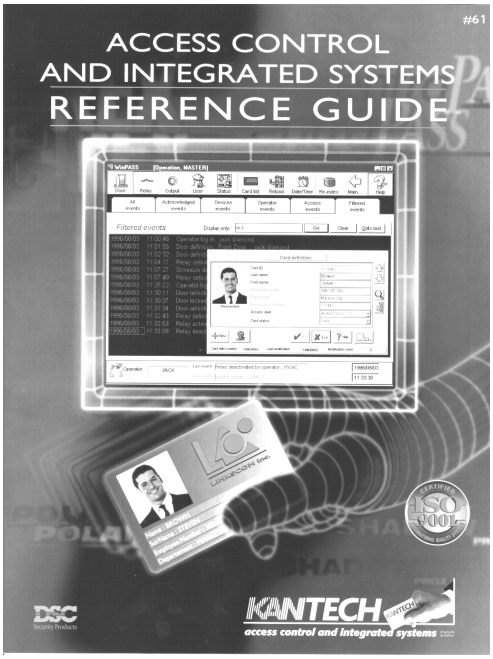
The **VC-485** is a protocol converter from RS232 to RS485. Its primary use is to convert the RS232 communication of the host computer to the RS485, KT-200 communication bus. Maximum length is 1200 meters (4,000 feet) using Ethernet grade 3, 2 twisted pair cable. The **VC-485** can also be used as a repeaters by installing two units, back to back, to increase the maximum length of the communication bus.

Revision C is a 5 VDC powered
Revision F is a 12 VDC powered

Reference Guide

Get your own free copy of our comprehensive **Access Control Reference Guide**. The Guide, which has been touted as one of the industry's finest publications, provides specifications and descriptions for all of Kantech's award-winning products. Furthermore, this guide also includes a multitude of valuable reference material that contributes to industry training and education.

Please call today at **1-888-KANTECH (1-888-526-8324)** for your free copy of the Reference Guide. Also, make sure you visit our extensive Web site at **www.kantech.com** for on-line documentation or to download a free working demo of our latest software products.



Reference Guide #61

SECTION 11

Compatibility with KT-200

This section regroups all the topics that are related to the KT-200 door controller. Within this section you will find:

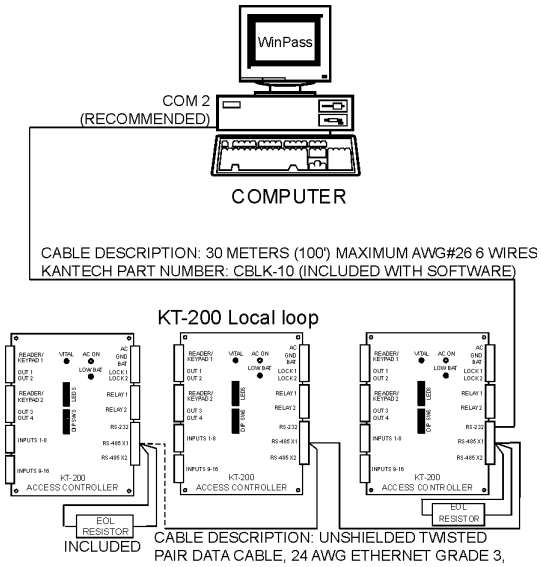
- The KT-200 installation procedure,
- The system specifications when using KT-200 door controllers, and
- A list of products that are only compatible with the KT-200 door controller.

Introduction - Section 1

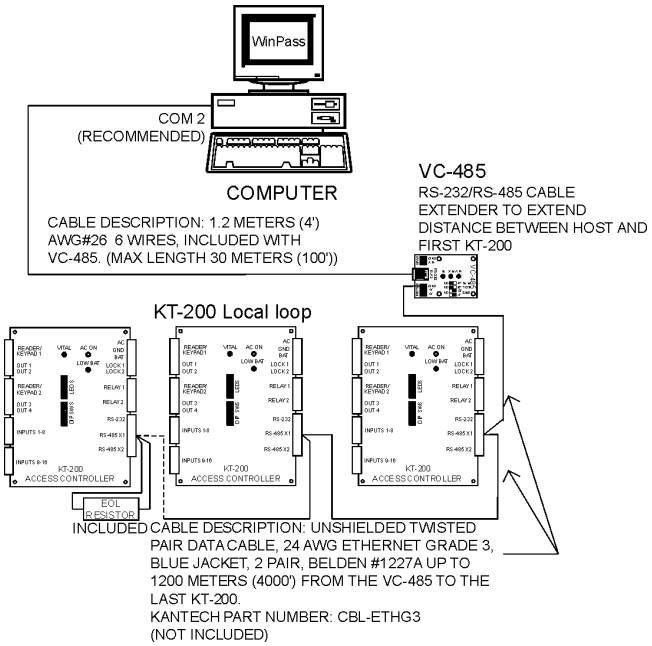
Important Note:

If you are using KT-200 controllers and more information applies to the KT-200 controller on a specific subject, the phrase "**SEE SECTION 11 IF YOU ARE USING KT-200 CONTROLLERS**" will be displayed within the subject.

WinPass Architecture (RS-232)



WinPass Architecture with Optional VC-485 Line Extender



System Specifications

Features	Specifications
Number of cards (on-line)	8,000
Number of cards (off-line)	3,000
Card families or site codes	No limit
Door controllers KT-200	32
Card readers	64
Keypads	64
Monitored inputs	512
Door lock outputs	64
Dry contacts Form "C" relays (with REB-8)	64 (512)
Auxiliary outputs for reader LEDs and door alarms	128
Card user access levels	250
Schedules of 4 time zones each	100
Holidays	366
Operator workstations	1
System operator passwords	No limit
Operator security levels	1 fixed / 8 prog.
Concurrent operator languages	2
Number of printers	Windows limit

Using ExpressSetUp - Section 2

For steps 1, 2, 4, 5 & 6, refer to Section 2 - Using ExpressSetUp.

3) You can modify the door names. Select (check box) the doors (readers) on which Anti-Passback is required (see Controller Definition Section for more on Anti-Passback). Specify the type of Anti-Passback (soft or hard). Specify if you will be **using REB-8 relay expansion boards or not**.

ExpressSetUp associates the door contact for the first door of a controller to input 1 and the second door contact to input 9. The request-to-exit button or detector (REX) is associated to input 2 for door 1 and to input 10 for door 2.

Login the System - Section 2

You should also verify that the Communication Port and Address DIP Switch are correct in the Configure Controller (MORE) window. The Communication Port must be the same as the port selected in Workstation and the controller Address setting (from 1 to 16) must be the same as the physical address set by the controller's DIP switch setting.

Defining Controllers - Section 3

The KT-200 controllers are polled and identified by their individual addresses configured by the on-board dipswitches. All readers and zone inputs are connected to the controllers, as well as the door strikes, output relays, and auxiliary outputs.

Programming Relays - Section 3

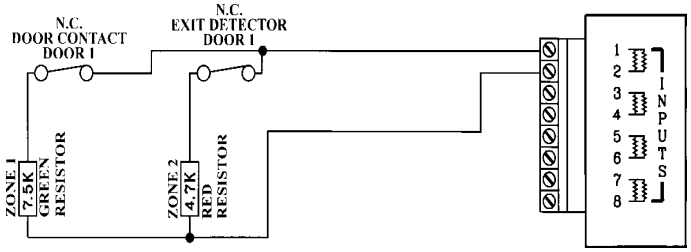
If extra relays are required, up to 14 more may be added (for a total of 16) by adding REB-8 relay expansion boards.

Note: The REB-8 relay expansion board may be used only with the KT-200.

Monitoring Inputs - Section 3

KT-200

WinPass can monitor 16 inputs per KT-200. Typically, 4 inputs per KT-200 are reserved for the doors (a door contact, T.REX request-to-exit detector for door 1 and, a door contact, T.REX request-to-exit detector for door 2). The following diagram shows how inputs are connected to a KT-200.



Programming Outputs - Section 3

KT-200

In addition to having two form C relays on each KT-200, four open-collector auxiliary outputs have also been provided. These outputs are typically used to activate the reader's LED on an access granted/ and the piezo alarm buzzer on a T.REX request-to-exit detector door alarm *(please refer to the output definition in section 5).*

Controller Definition - Section 5

Input Connection

Configure one or two REB-8 relay expansion boards with the KT-200 controller.

Door Definition - Section 5

Door address

COM2:01:01

The door address is a physical address consisting of the serial port, the physical address of the controller ***(Dip switch of the KT-200)***, and the physical address of the door (1 or 2). The door address cannot be modified unless the controller serial port setting is modified at which time the door address is automatically changed by the system.

Door Contact Input

Input 1 is reserved for door 1 and Input 9 for door 2 by default for the KT-200.

REX Input

Input 2 and Input 10 are reserved for REX on door 1 and REX on door 2 for the KT-200.

Input Definition - Section 5

Input Address

COM2:01:01

The input address is a physical address consisting of the serial port, the physical address of the controller ***(Dip switch for the KT-200)***, and the physical address of the input (1 to 16).

Output Definition - Section 5

Output Address

COM2:01:01

The output address is a physical address consisting of the serial port, the physical address of the controller ***(Dip switch for the KT-200)***, and the physical address of the input (1 to 4).

Relay Definition - Section 5

Relay Address

COM2:01:01

The relay address is a physical address consisting of the serial port, the physical address of the controller ***(Dip switch on the KT-200)***, and the physical address of the relay (1 to 16).

Workstation Configuration - Section 5

Port Settings

Enter the value according to the DIP switch settings on the KT-200 door controllers. The default value is 9600 baud.

Installers familiar with the installation can use the checklist with the "☑" symbol

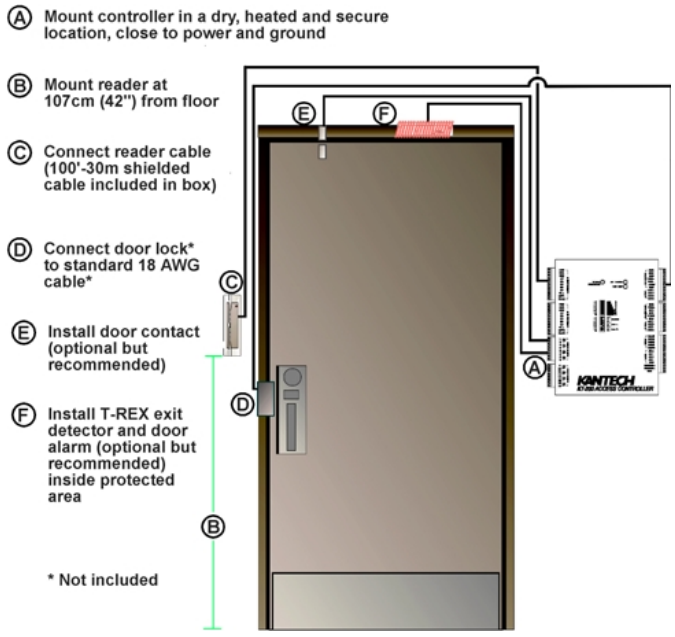
Step 1. Preparing Installation of the KT-200

☑ **Required to install the KT-200:**
- **KT-200 controller**
- **EOLs resistors for inputs**
- **Keys to open KT-200 cabinet**
- **AC Transformer**
- **Two 12 volt batteries**
- **Ground clamp**
- **EPROM**

A visual verification should be made when unpacking the KT-200. Any missing item or damaged component should be reported immediately . Install the associated software EPROM on the KT-200's EPROM socket located directly above the on-board lithium battery. As with every other chip on the pc board, the EPROM alignment notch should be pointing to the top of the pc board.

Step 2. Physical Installation

☑ **Check for ideal location indoors**
☑ **Stay away from electrical or communication devices**



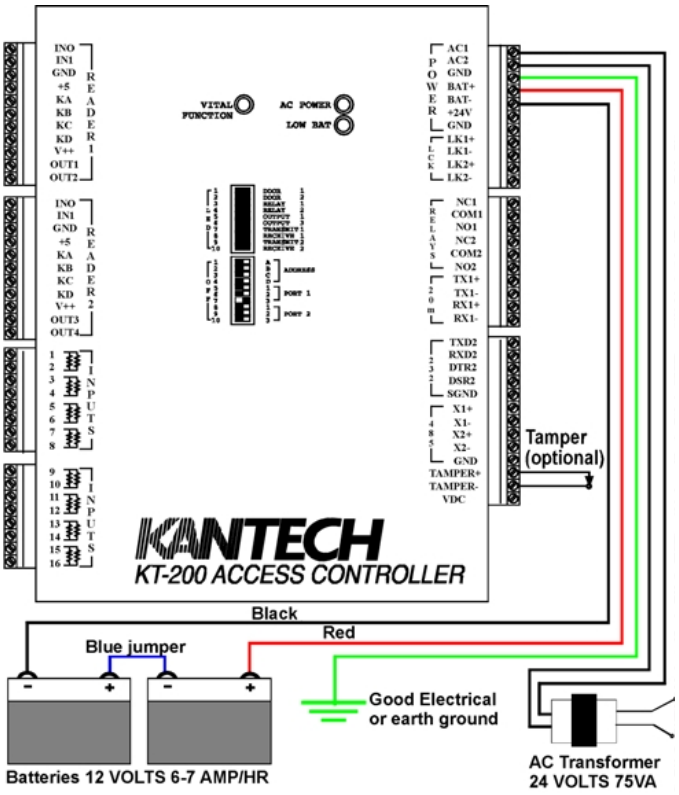
The KT-200 controller cabinet has been designed to be mounted on a wall without any additional enclosures. The cabinet is large enough to accommodate the battery backup supply and the necessary wiring connections for most applications. EMT conduit knockouts are provided in 1/2" and 3/4" on all sides of the cabinet.

The cabinet should be mounted indoors, in a secure location providing normal temperature and humidity levels, leaving 23 cm. (8 inches) clear space around all sides and a minimum of 33 cm. (13 inches) clear space in front of the cabinet. The location should be easily accessible for servicing the equipment and it is recommended that controllers be located near the controlled doors.

The controllers must be located at a minimum distance of 2 meters (6 feet) from any high voltage equipment or wiring, at a minimum distance of 2 meters (6 feet) from electrical equipment susceptible of generating electrical interference, at a minimum distance of 1 meter (3 feet) from telephone equipment or lines and, at a minimum of 8 meters (25 feet) from any transmitting equipment. Finally, physical access by keys on controlled doors must be provided so that the KT-200 can be accessed for servicing in case of malfunctions.

Step 3. Power Requirements

☑ **DO NOT POWER AT THIS POINT!**
☑ **Install 24VAC/75VA transformer**
☑ **Locate batteries in cabinet**
☑ **DO NOT POWER AT THIS POINT!**



The KT-200 controller must be powered by a 24VAC75VA wire-in transformer. The transformer is usually mounted by a licensed electrician on a 4" X 4" electrical box located near the unit.

Power should only be applied to the unit when all connections are completed and tested

When AC power is present, the green LED will be on. After the unit is running, if the AC supply is removed, the battery backup will support normal operation up to 20 hours with two (2) 12 volt gel type batteries of 7 Amp/hour. An internal battery verification will cut the battery power when the battery voltage level falls below 22 volt and the red DC LED indicator will remain on until the battery voltage has dropped below 18 volt.

NOTE: The KT-200 unit will not start on batteries alone. The AC supply must be initially connected.

Step 4. Grounding

☑ **AWG#18 grounding wire to GND**

Since the KT-200 uses high performance communications, proper grounding must be provided to insure proper operation. **An AWG#18 single conductor solid copper wire must be used to ground each controller to a good earth ground as per the local electrical code (be careful about ground loops). The ground clamp should be located below any other ground.** It is also recommended to provide an AWG#18 single conductor copper wire between each controller.

Step 5. Tamper Protection

☑ **Install optional tamper switch on cabinet**

A tamper switch may be installed on the unit to detect an unauthorized opening of the cabinet. The normally closed tamper switch is connected to the TAMPER+ and TAMPER- (last inputs located at the bottom of the right side connector sets.) This input must not be wired to devices outside of the KT-200 cabinet. If the tamper input is not used, install a jumper across the terminals.

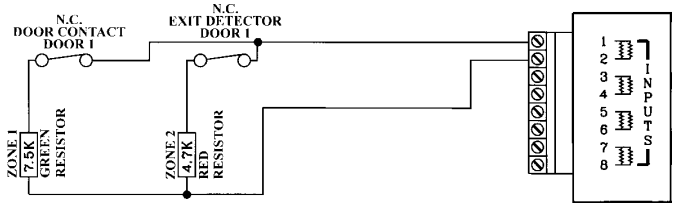
Step 6. Hooking Up Inputs

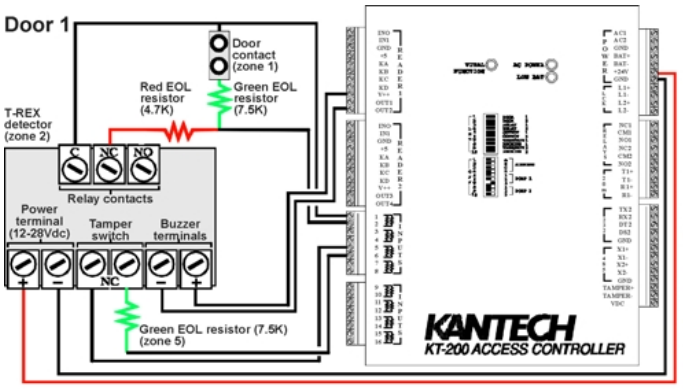
☑ **Check each input loop for EOL's**
☑ **Connect devices to inputs 1 to 16**
☑ **Only one open contact per loop!**
☑ **Green resistor for odd inputs (1,3,5,7...)**
☑ **Red resistor for even inputs (2,4,6,8...)**

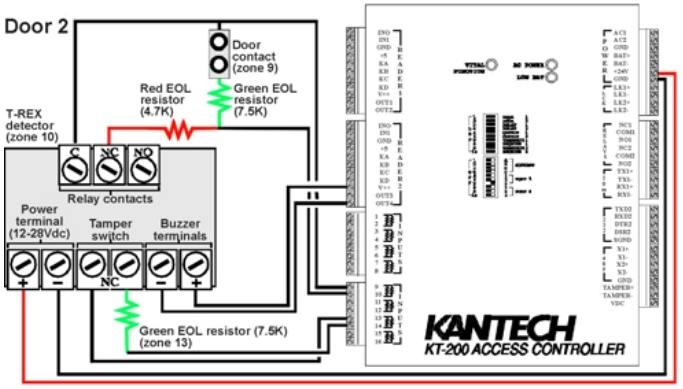
The KT-200 has the capability of monitoring 16 input points. To reduce cabling, the 16 points are grouped under 8 sets of terminals identified 1 to 16. (Installing in series with the monitored device contacts, a 7.5K Ohms (GREEN) resistor for the odd input and a 4.7K Ohms resistor (RED) for the even input, enables the KT-200 to monitor both points on one single cable pair).

To provide line security, resistors must be installed at the monitored device (contact, detector...). The resistors shipped with the KT-200 have been identified with Green for Odd (7.5K) and Red for Even (4.7K).

The maximum distance of one line is 600m (2,000 feet) with AWG#22.







Inputs can be used to monitor open devices such as thermostats but it is not recommended to monitor two open contacts on one input terminal set as such wiring provides reduced line integrity.

If required, it is possible to get enhanced line integrity and 24 hour line supervision by using even resistors (Red 4.7K) with normally open contacts and using the odd resistor (Green 7.5K) as end of line. Only one point per terminal set can be monitored for devices wired in this configuration for a total of 8 inputs per KT-200.

Inputs 1-2 are ideally reserved for the first controlled door contact as input 1 and the associated request-to-exit detector as input 2. Inputs 9-10 are ideally reserved for the second controlled door contact as input 9 and the associated request-to-exit detector as input 10. There is no obligation to follow this rule but such a standard convention makes it easier for servicing.

Unused inputs on the KT-200 should be terminated by EOL resistors or defined as open inputs to reduce useless status reporting of abnormal conditions.

Step 7. Relays & Auxiliary Outputs

☑ **Connect relay to low voltage devices**
☑ **Add external relays for high voltage devices**
☑ **Connect auxiliary outputs to readers & local warning devices**

The KT-200 provides 2 control relays that may be activated or deactivated by schedules or input conditions. The relays are single pole normally open and closed contacts rated at 30VDC/24VAC, 2 amp maximum.

Devices generating high levels of electrical noise or arcing (such as electromagnet coils) should not be directly connected to these output relays as noise or arcing current could be induced into the

KT-200 circuit. Use external switching relays to prevent damage to the KT-200.

Connect outputs OUT1 and OUT3 (from reader terminals) to the reader LEDs to provide visual feedback of access operation. Connect OUT2 and OUT4 to local warning devices that will signal Door alarms.

For example, at door 1, OUT1 could be programmed to:

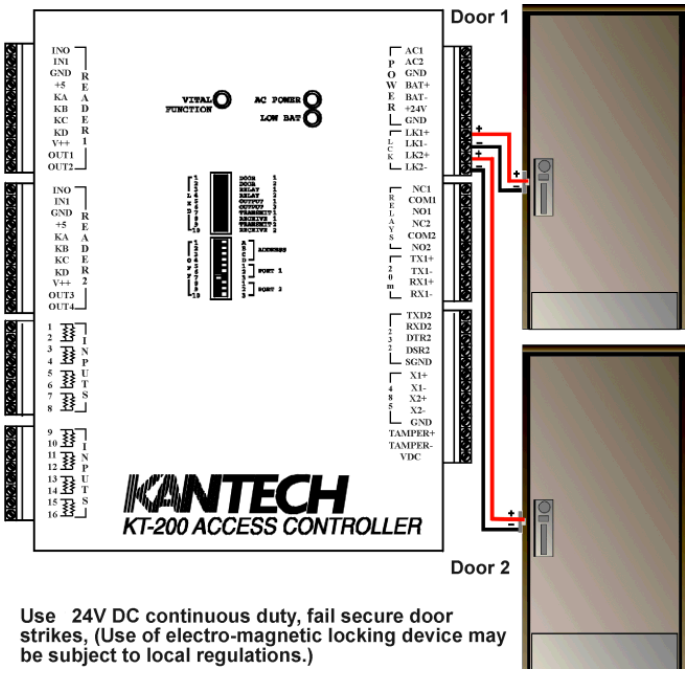
- Be steady red when the door is locked and waiting for a card read
- Turn to green when the door is unlocked
- Flash from red to green when the access is denied.

OUT2 could be programmed to:

- Operate a local warning device when the door has been left open
- Flash a yellow LED on the keypad to indicate wait for PIN input.

Step 8. Door Locking Devices

☑ **Connect door locks to LK+ and LK-**
☑ **Max.250mA at 24DC per output**
☑ **Check local "mag locks" regulations**



Use 24V DC continuous duty, fail secure door strikes, (Use of electro-magnetic locking device may be subject to local regulations.)

The locking device outputs L1+ L1- for door 1 and L2+ L2- for door 2 are located on the bottom of the power connector on the top right side of the KT-200.

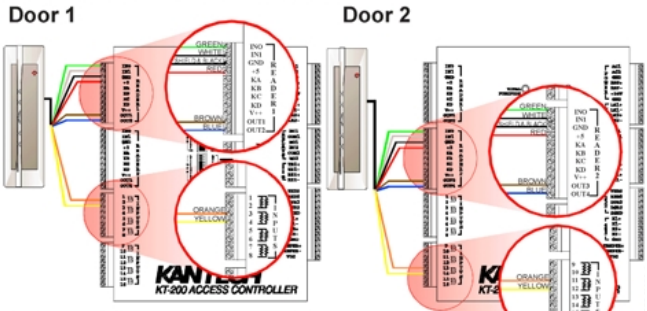
The locking device outputs are controlled according to the end user programmed parameters for allowing access to, or unlocking of doors according to schedules.

These 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 modes (normal or reverse action). The typical maximum DC current for each lock output is 250mA.

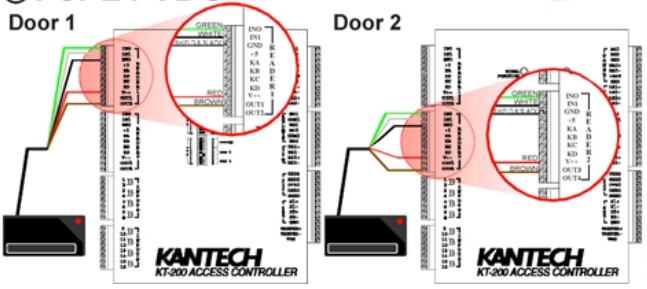
WARNING: Controlled door locks may be governed by regulatory bodies and should always be installed according to local regulations. In most instances, there are strict limitations to installing magnetic (mag locks) or other similar locking devices on doors used for exit.

Step 9. Readers and Keypads

Ⓐ For 5 VDC readers



Ⓑ For 24 VDC readers



☑ **Connect door locks LK1 and LK2**
☑ **Max. 250mA at 24 VDC per outputs**
☑ **Check local "mag-lock" regulations**

READER CONNECTION TERMINAL

WARNING: Connecting the red wire lead (or power lead) of a 5VDC reader to the 24VDC terminal may damage the reader. See reader installation procedure for proper power connection.

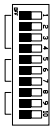
A KT-200 can control 2 readers and/or 2 keypads. These can be installed on one door to control both entry and exit or on two separate doors operating independently to control access in one direction only. The keypad can operate a door by itself or be used in conjunction with a card reader for PIN confirmation.

Using the proper cable, the readers/keypads may be located up to a distance of 150 meters (500 feet) from the KT-200. Auxiliary outputs provide access operation visual and/or audible feedback at the controlled door . Outputs OUT1 & OUT2 are used for the first door and OUT3 & OUT4 for the second door.

The 5VDC power and V++(24DC) power can also be used to power low current audible devices usually located at the controlled door.

Step 10. Dip Switch Settings

OFF ON



- ☑ **Dips 1 to 5 for controller address**
- ☑ **Dip 6 & 7 comm speed with other KT-200s**

Controller Address	DIP 1	DIP 2	DIP 3	DIP 4	DIP 5
1	OFF	OFF	OFF	OFF	OFF
2	ON	OFF	OFF	OFF	OFF
3	OFF	ON	OFF	OFF	OFF
4	ON	ON	OFF	OFF	OFF
5	OFF	OFF	ON	OFF	OFF
6	ON	OFF	ON	OFF	OFF
7	OFF	ON	ON	OFF	OFF
8	ON	ON	ON	OFF	OFF
9	OFF	OFF	OFF	ON	OFF
10	ON	OFF	OFF	ON	OFF
11	OFF	ON	OFF	ON	OFF
12	ON	ON	OFF	ON	OFF
13	OFF	OFF	ON	ON	OFF
14	ON	OFF	ON	ON	OFF
15	OFF	ON	ON	ON	OFF
16	ON	ON	ON	ON	OFF
17	OFF	OFF	OFF	OFF	ON
18	ON	OFF	OFF	OFF	ON
19	OFF	ON	OFF	OFF	ON
20	ON	ON	OFF	OFF	ON
21	OFF	OFF	ON	OFF	ON
22	ON	OFF	ON	OFF	ON
23	OFF	ON	ON	OFF	ON
24	ON	ON	ON	OFF	ON
25	OFF	OFF	OFF	ON	ON
26	ON	OFF	OFF	ON	ON
27	OFF	ON	OFF	ON	ON
28	ON	ON	OFF	ON	ON
29	OFF	OFF	ON	ON	ON
30	ON	OFF	ON	ON	ON
31	OFF	ON	ON	ON	ON
32	ON	ON	ON	ON	ON

The 10 DIP switches are located in the middle of the KT-200 controller circuit board. The top 5 switches (1 to 5) configure the KT-200's address and dip switches 6 & 7 set the communication PORT-1 baud rate.

The factory default baud rate is set at 9,600 baud (Dip6 OFF, dip7 ON), DIP switches 8 & 9 set the controller with or without a VC-485. Please refer to the following tables to set the DIP switches on the KT-200 controller. Press down the dip switch on the right side to set ON and on the left side to set OFF.

Please note that the dip switch settings will only become effective after resetting the controller by powering it off or pressing the SW3 reset switch located on the bottom left of the controller PCB.

RS-485 Bus Speed	DIP 6	DIP 7
1200 baud	OFF	OFF
2400 baud	ON	OFF
9600 baud	OFF	ON
19200 baud	ON	ON

	DIP 8	DIP 9
Controller #1 without VC-485	ON	ON
Controller #1 with VC-485	OFF	OFF

Dip Switch #10 is always OFF.

Setting up a Local System Without a VC-485

1) Set J3 to the DOWN position (RS-232 mode) on the KT-200.
2) Set dipswitches 8 and 9 to ON on the KT-200 that will be connected to the Host (this sets up the KT-200 as a master controller without modem).
3) Set dip switch 1 to ON. Press RESET. Set dipswitch 1 to OFF. Press RESET again (this procedure initializes the KT-200 as a master controller with modem).
4) Verify that dip switches 6 & 7 (9600 by default) are properly set for the correct baud rate with the other KT-200s.
5) Verify that the communications cable connected to the Workstation and the Controller is properly wired and connected.

Setting up local System with VC-485

1) Verify the wiring between the KT-200 and the VC-485.
2) Verify the wiring between the VC-485 and the Workstation.
3) Verify if both LEDs are illuminated on the VC-485.
4) If only the yellow is on, the host is trying to communicate with the controller.
5) If only the red is on (or flashes), the controller is trying to communicating with the PC host. If controllers are not communicate, verify that the RS-485 bus wiring is correct. That is X+ and X- and the ground is properly connected between the KT-200 and the VC-485. If one wire is not properly connected, the KT-200 may be communicating in degraded mode.

Step 11. Jumper Settings

Jumper default values are set at the factory and should only be modified for special applications. Since new settings become valid only after resetting the power, make sure that all power has been removed from the KT-200 controller before changing jumper settings. All other jumpers on the controller board should be left as set by the factory.

JUMPER #	NAME	LOCATION	DEFAULT SETTING	ALTERNATE SETTING
J2	Network Port-1 communications protocol	Middle right next to comm chips.	Down for RS-485 to other KT-200s	DO NOT USE
J3	DO NOT USE	Below J2	DOWN (RS-232)	DO NOT USE
J4	DO NOT USE	Below dip switch	DOWN	DO NOT USE
J8	Watchdog	Bottom middle	UP for watchdog	DO NOT USE
J9	Non volatile RAM battery	Bottom middle on top of J8	Up for non volatile memory protection	Down to erase non-volatile memory

Step 12. Connecting the KT-200 to the RS-485 Bus

☑ **Connect RS-485 cable to X1+ and X1-**
☑ **Yellow RS485 EOL on last KT-200**

Controllers are linked together using their communication PORT-1 RS-485 communication protocol. The communication loop originates at the workstation computer.

The workstation communicates with the local first controller in RS-232 protocol on the controller's RS-232 port (TX2, RX2).

The RS-485 protocol will easily operate at high baud rates (up to 19,200), its immunity to interference is very high and maximum communication loop length with the appropriate cable is 1,200 meters (4000 feet).

The RS485 communication loop originates from the first controller or the VC-485 converter and runs sequentially to each KT-200 controller as a single communication line. Connecting several KT-200 at a single point is not acceptable nor are "Y" or "spider web" type networks.

The line must continue to each KT-200 and terminate with the yellow 120 Ohms end of line resistor at the last KT-200 on the loop. This method insures that the line is balanced and that both conductors are the same length. The RS485 communication loop should be wired with Ethernet grade 3 double pair network cable (see cable specifications).

The RS485 loop can operate at 9,600 or 19,200 baud under normal conditions. Intermittent communication problems or erratic operation may require to slow down the network. Varying the network speed does not perceptibly change the operation speed of the system.

The network speed must be changed at each KT-200 on the loop by setting DIP switches 6 and 7 as indicated previously. For the change to take effect, the controller must be reset using the SW3 push button switch located on the bottom left side of the controller circuit board.

Also, the system baud rate must be set from the operator's microcomputer.

KT-200 Technical Specifications

AC power	24 VAC, 75 VA, class 2 transformer
Battery backup	2 gel type batteries 12V 7Ah
Cabinet measurements (H.W.D)	15-5/8" x 13-3/4" x 3-15/16"
Conduit knockouts	EMT 1/2" and 3/4"
Weight	6kg (13.8 lbs)
Operating temperatures	From 2°C to 40°C (35°F to 110°F)
Humidity	90° non-condensing humidity
Processor	Z80- 6MHz, with "watchdog"
Reader technologies	Proximity, Wiegand, magnetic, bar code, keypads and others
Reader maximum distance	150 meters (500 feet) from KT-200
P.I.N. confirmation	At each reader with keypad
Inputs	16 inputs, NO/NC, with EOL's
Maximum points wiring	600 meters (2,000 feet) - AWG#22
Door strike power supplied by controller	27VDC @ 125mA (per strike)
Auxiliary outputs	27 VDC @ 50mA (open collector)
Control relays	2 relays, 30VDC, 24VAC, 2A max.
Tamper switch input	Normally closed
Communications ports	RS232 and RS485
Communication speeds	From 300 to 19,200 baud
Internal memory and clock	Maintained by a lithium battery
Network Autonomy	Distributed data and processing

KT-200 Electrical Specifications

VOLTAGE OUTPUTS	TYPICAL	MAX	ABSOLUTE COMBINED MAX
LOCK 1 (+24/27 VDC) LOCK 2 (+24/27 VDC)	125mA 125mA	**500mA**	**1A**
READER 1 V++ (+24/27 VDC) READER 2 V++ (+24/27 VDC)	75mA 75mA	**500mA**	
+24 V AUXILIARY POWER	250mA	**500mA**	
READER 1 5V (+5 VDC) READER 2 5V (+5 VDC)	50mA 50mA	**500mA**	**500mA**

OPEN COLLECTOR OUTPUTS	TYPICAL	MAX	NOTES
OUT 1	20mA	**50mA**	Outputs are Open-Collector to Ground, current limited by a 47 Ohm series resistor. Current is drawn from above outputs (5V or 24V) and must be included in their respective calculation.
OUT 2	20mA	**50mA**	
OUT 3	20mA	**50mA**	
OUT 4	20mA	**50mA**	

Walk Through Testing

Once the software Quick setup has been done, a walk through test is necessary to ensure all controller and reader connections are working and that the system will operate correctly.

Proceed with this walk test before making any software changes or modifications.

1) Present a card to every reader.

2) At the WinPass Workstation, when the card is presented to a reader, at the bottom of the event monitoring screen, a "Card unknown" event should appear displaying the door name and card number.

- If a "Card unknown" event does not appear, verify that the reader is properly connected.
- Does the LED on the reader flash to indicate a card unknown read?
- Does the reader have the proper operating voltage at its terminals? If not, an auxiliary power supply may be used. However, both the power supply and reader grounds must be connected to the KT-200 ground.

3) Open every door to create "Door forced open alarms".

- If no "Door forced open alarms" occur, verify that the door contact is properly wired to the KT-200 with the proper end of line resistor.
- Verify whether you are using a normally open or normally closed door contact.

4) Activate every request-to-exit to detector. Verify that a "Request-to-exit granted" occurs.

- If no "Request-to-exit granted" messages appear, verify that the request-to-exit button is properly wired to a KT-200 input with the proper end of line resistor.

KT-200 FCC Compliance Notice

This equipment does not exceed Class A limits per radio noise emissions for digital apparatus, set out in the Radio Interference Regulation of the Canadian Department of Communications. Operation in a residential area may cause unacceptable interference to radio and TV reception requiring the owner or operator to take whatever steps are necessary to correct the interference.

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 1.5 of the FCC Rules and CSA 108.3. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

KT-200 CE Compliance Notice

Toroid installation:

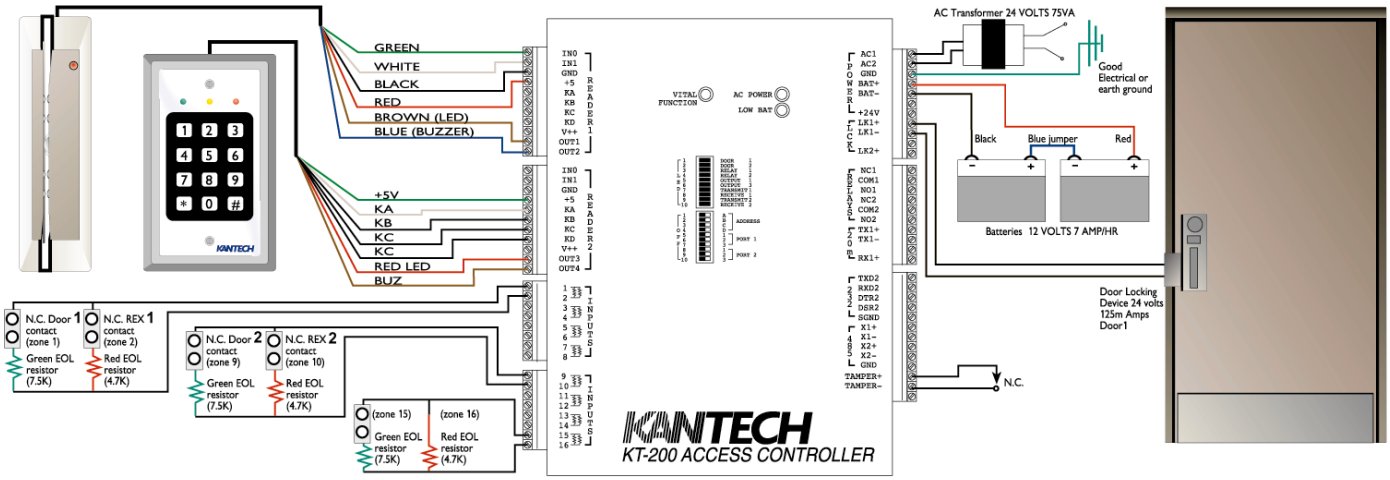
All wires connected to the KT-200 controller must be wrapped around a toroid three times, to conform with CE standards.

Note:

A) The toroids must be located in the KT-200 controller cabinet.

B) Several wires may be wrapped around one given toroid.

Typical Component Connection to KT-200



KT-200 Compatible Products

These products are ***only compatible with the KT-200 controller***, to see other compatible products, please refer to Section 8 of this document.

Keypads

The **KP-500 digital keypad** is specifically designed as a cost effective solution for access control systems requiring the use of a keypad. The brushed stainless steel plate assures a pleasant durable finish. The one piece design is rugged and compact, ideal for high traffic indoor use.

KP-500

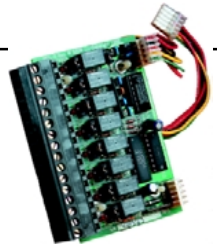
The **KP-2500** is a solid stainless steel weatherproof keypad combining outstanding appearance with tremendous resistance to abuse. The keypad contains no moving parts and uses a proprietary piezo electric technology ensuring that the keypad will perform reliably in even the most demanding environments. The one piece design is rugged and compact, ideal for high traffic indoor and outdoor use.

KP-2500

The **KP-3000** is a cast stainless steel weatherproof keypad combining outstanding appearance with tremendous resistance to abuse. The **KP-3000** is delivered in two parts: the keypad surface mounts on any material including narrow-style aluminium door frames; the electronic decoder circuit is usually located in the door controller.

KP-3000

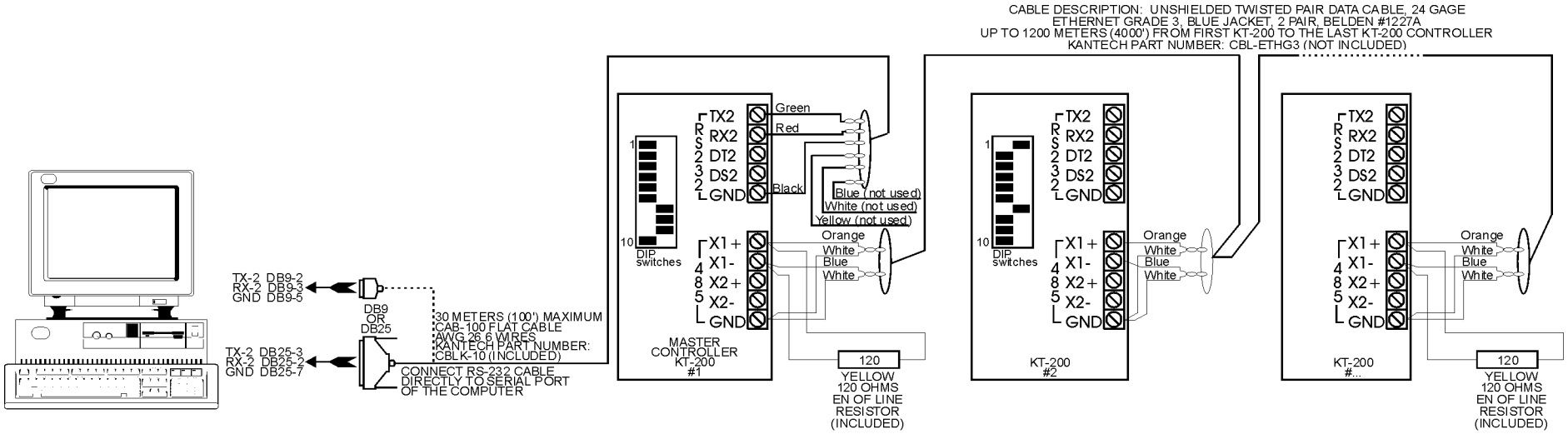
REB-8 - Relay Expansion Board



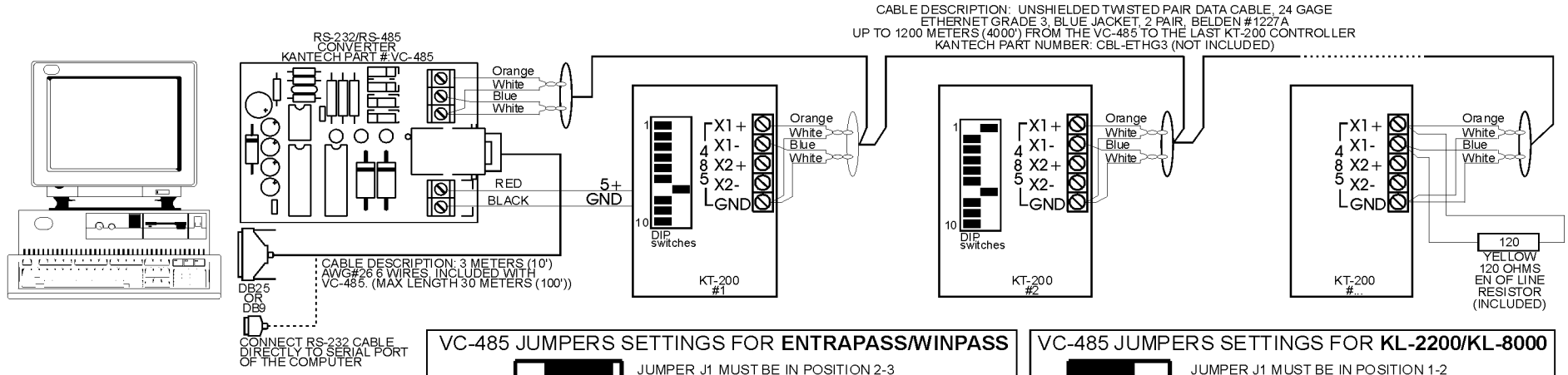
The **REB-8** relay expansion board provides an additional 8 general purpose control relays to the KT-200 door controller. Two **REB-8** can be used to expand up to 16 relays. The **REB-8** can also be used as a cost-efficient alternative for basic elevator control, with up to 16 floors per cab.

REB-8

RS-485 Local Loop Connection Diagram (without VC-485 - WinPass)



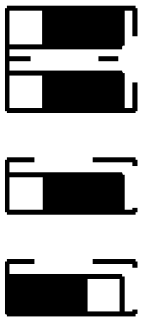
Local RS-485 connection Diagram using VC-485 Line extender



IN SOME CASES IT MAY BE NECESSARY TO LOCATE THE FIRST KT-200 MORE THAN 30 METERS (100') FROM THE COMPUTER.

THE OPTIONAL VC-485 LINE EXTENDER IS A MODULE THAT CONNECTS TO THE PC AND INITIATES THE RS-485 PROTOCOL FROM THE PC RATHER THAN FROM THE FIRST CONTROLLER, PERMITTING A TOTAL LOOP DISTANCE OF 1200 METERS (4000') FROM THE VC-485 TO THE LAST KT-200.

VC-485 JUMPERS SETTINGS FOR **ENTRAPASS/WINPASS**



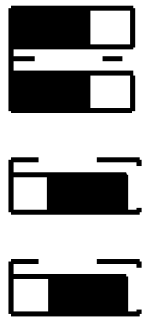
JUMPER J1 MUST BE IN POSITION 2-3
(LINE BIAS ON)

JUMPER J2 MUST BE IN POSITION 2-3
(LINE BIAS ON)

JUMPER J3 MUST BE IN POSITION 2-3
(END OF LINE RESISTOR ON)

JUMPER J4 MUST BE IN POSITION 1-2
(TRANSMIT ON REQUEST TO SEND DISABLE)

VC-485 JUMPERS SETTINGS FOR **KL-2200/KL-8000**



JUMPER J1 MUST BE IN POSITION 1-2
(LINE BIAS OFF)

JUMPER J2 MUST BE IN POSITION 1-2
(LINE BIAS OFF)

JUMPER J3 MUST BE IN POSITION 2-3
(END OF LINE RESISTOR ON)

JUMPER J4 MUST BE IN POSITION 2-3
(TRANSMIT ON REQUEST TO SEND ENABLE)

APPENDIX

This section introduces :

- A list of the most frequently asked questions and,
- A list of “did you know” which can you help you to better understand your system.

Frequently Asked Questions

Why can't I modify or view the DBF database files and tables?

Though the databases appear with DBF file extensions, there are checksums for every database item that must match with those within the WinPass software otherwise a database corruption will occur. This is to prevent unauthorized tampering.

How do I configure the Baud Rate in WinPass ?

In WinPass, clicking the "Port Setting" radio button in the Workstation screen of the Configuration menu can configure the baud rate at which a COM port will communicate with the controllers. Select the port to be used by WinPass, and select the baud rate. You must also assign the COM Port that will be used by WinPass to communicate with the door controllers by clicking on "More" in the Controller definition screen of the Configuration menu.

If you are using KT-300 door controllers, the communication speed will be automatically updated. Please note however that if you are using KT-200 door controllers, the communication speed set by default on the controllers is 9600 baud. If you want to set a different communication speed, you will need to change the dip switch settings on your controllers (Refer to the KT-200 compatibility in Section 11 - Step 10 for more details).

Can a camera be activated as a user is granted access in WinPass?

Yes. Relays can be activated upon door events in the latest WinPass version. Clicking on the Events icon in the Door Definition screen, you can select, for each door, specific events to trigger specific relays. You simply have to hook-up your camera to the relay triggered by the "Access Granted" event.

How do I make a user's picture appear on-screen after events in WinPass?

By double-clicking on the event, the "More Info" window will appear. If users have their picture associated to their card on file, the picture of the user who triggered the event will also be displayed. You can select the doors on which cards must be swiped for a picture to appear. If the "More Info" window is left open, information on the following events will be displayed in turn.

FAQs

Did You Know ?

WinPass is capable of saving any report in several different database/spreadsheet formats ?

These files can then be sorted, queried and filtered with a third-party application. This is done by clicking on the "Brief-case" icon in the Report… Preview menu.

That the Card Database "User Definable" fields can be customized ?

In WinPass, simply click and hold the left mouse button over the "User Definable" text and drag the pointer over the text. Type in the new name of this field to change it. It's that simple!

Common names for these fields are: Employee Number, Department, Address, Telephone Number, etc.

You can increase security overnight ?

A schedule can be assigned to the keypad so that it forces the cardholder to enter their PIN value during night hours and only present an access card during the day.

This can be done when using a reader in conjunction with a keypad. Create a schedule that is valid during night hours and assign it to keypad schedule in the Door Definition menu. When defining a new User or modifying an existing User, set the field "Must use PIN" to "Yes" (click on the "More" icon to access the second page of the User menu to find the "MUST use PIN" field) and assign a PIN value (no greater than 65535). This user will then have to present his card AND enter his PIN number during the period which the keypad schedule is valid. When the keypad schedule becomes invalid, only a card will be needed to unlock the door. No PIN confirmation will be required by the system to grant access to the card holder.

The last two relays on the second REB-8 can be programmed to follow …

a) The Door Status (Forced Open, Open too long, etc.)

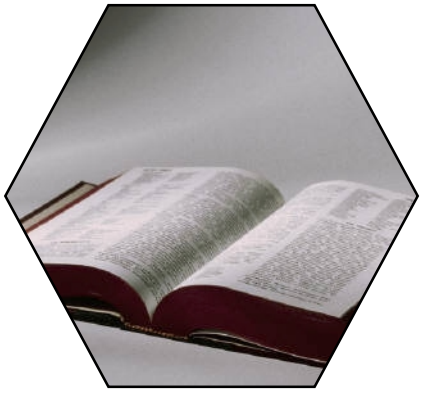
b) Door locked status (locked or unlocked)

c) Relay 1 & 2 status (activated or de-activated)

d) Reader Outputs 1 & 3 (reader LEDs)

e) Reader Outputs 2 & 4 (reader piezos)

These relays can then be used to activate a siren (bell), sign, or other device when a condition is True and deactivate when a condition is False.



INDEX

R

S

T

U

W

KANTECH

ACCESS CONTROL AND INTEGRATED SYSTEMS

WinPass Fax Registration Form

PLEASE TYPE IN CLEAR CAPITAL LETTERS
***** COMPLETE AND RETURN BY FAX AT +1(450) 444-2029 *****
(You can also register by calling see below)

SYSTEM INSTALLER INFORMATION

Name of Installer Company: _____

Address : _____ **City :** _____

State/Province : _____ **Zip/Postal Code :** _____

Country : _____ **Tel :** _____ **Fax :** _____

Kantech Equipment Supplier: _____

Name of Person Registering Software: _____

Signature: _____ **Date:** _____

SITE INFORMATION

Site Name : _____ **City:** _____

System Administrator : _____ **Tel :** _____ **Fax :** _____

Product Serial Number (found on disk #1) : ___ ___ ___ ___ ___ ___ ___ ___

Software Version #: _____ **Revision #:** _____

YOUR SUGGESTIONS AND COMMENTS

What was your first impression of WinPass ?

_____

_____

Your suggestions and comments about WinPass ?

_____

_____

Your suggestions and comments regarding our products ?

_____

_____

Your suggestions and comments regarding our services ?

_____

_____

Other comments ?

_____

_____

For additional information, call Kantech's FREE customer assistance service
Monday to Friday 08:00AM to 8:00PM Eastern Standard Time

Phone: +1(450) 444-2040 • **Fax**: +1(450) 444-2029 • **Web Site**: http://www.kantech.com • **E-mail**: techsupport@kantech.com