Mircom

TX3 Series

UL LISTED TX3-CX CARD ACCESS SYSTEMS

Installation Manual

Mircom UL Listed TX3-CX Card Access System Installation and Operation Manual v.2

Mircom
25 Interchange Way
Vaughan, Ontario
L4K 5W3
905.660.4655
Fax:905.660.4113

Contents

List of Figures

1 Welcome

This manual provides information about the installation and operation of the TX3-CX Card Access System, and must be read in its entirety before beginning any installation work.

Installation must be performed by a qualified technician and must adhere to the standards and special notices set by the local regulatory bodies.

Note:	**Mircom periodically updates panel firmware and Configurator Software to add features and correct any minor inconsistencies. For information about the latest firmware or software visit the Mircom website at www.mircom.com.**

Warning:	**The Card Access System must be grounded by a qualified electrician. An improperly grounded unit can result in equipment malfunction and electrical shock.**

This chapter explains

- Introducing the TX3-CX Card Access System
- Applications
- Installer Responsibilities
- Network Setup
- About this Manual
- Contact Us

1.1 Introducing the TX3-CX Card Access System

The TX3-CX Card Access System is part of the Mircom suite of products that provide building ready monitoring, control and integrated security solutions for use in the high end multi-tenant residential market.

The Card Access System addresses the need within today's high end multi-tenant residential market for an easy-to-use tenant access system and an easy-to-use configuration utility.

This manual provides the technician with information about the installation and configuration of the Card Access System and explains how to configure various components for a new system, including the modification of an existing system.

1.2 Applications

Mircom's Card Access System consists of a controller, two card readers and configuration software. The controller can accept at the same time, a combination of card readers with different formats to control two access points or doors. The Card Access System can set elevator usage if elevator controls are used.

A number of different card readers are supported, such as the TX3-CX-REC Wiegand wireless receiver, all of which are configurable using the Configurator software.

Note: Only the 26-bit Wiegand SIA standard format is evaluated to UL 294.

The Card Access System can be used in a stand-alone or networked environment using a standard RS-485, daisy chain peer-to-peer network arrangement.

This network can consist of only the card access controller or a combination of Touch Screens, Lobby Control Units, Elevator Restriction Units and Card Access Units. Up to 63 units can be networked on any RS-485 network or subnetwork. Valid RS-485 network addresses range from 1 to 63. One of the networked units with a real time clock, such as Touch Screen, Lobby Control or Card Access must have their network address set to 1.

If an Ethernet network is used, you can connect more than 63 units to your system. If you use an Ethernet network with RS-485 subnetworks, each RS-485 subnetwork can have 63 devices connected to it.

1.2.1 Wiegand interface

The Wiegand interface is a wiring standard for card readers for establishing the connections between a card reader and the Card Access System. This interface is a serial interface requiring 7 to 10 conductors for communications between the reader and the controller. This interface also supplies 12V power to the reader.

The Wiegand compatible access card has 26 bits of information embedded onto the card. The card reader reads and registers the card information and sends it back to the controller in a serial bit stream.

1.2.2 Card Access System

Note: Only the 26-bit Wiegand SIA standard format is evaluated to UL 294.

The Mircom Card Access System supports a proprietary 37-bit encoding technology and a 26-bit SIA standard format, and consists of a maximum of 63 card access controllers networked together. Each card access controller can have two card readers. The Card Access System provides an optional battery backup and a real time clock.

The Card Access System integrates with the TX3 Telephone Access system by utilizing a common network for both Telephone Access and Card Access Systems.

A PC provides configuration and on-line monitoring of the Card Access System and the Telephone Access System status. Once the system is configured, the PC is not required.

1.3 Installer Responsibilities

The installation and setup must be done by a qualified technician. The technician is responsible for installing all of the system components, connecting all of the input and output wiring for the appropriate door entry systems, and ensuring that the wiring adheres to the requirements of the system for proper operation using the Configurator software.

1.4 Network Setup

The Card Access System can consist of either stand-alone card access controllers or networked card access controllers. Networked card access controllers can communicate over an RS-485 network, an Ethernet TCP/IP network, or a combination of an Ethernet network with RS-485 subnetworks. All card access controllers can communicate over RS-485. To communicate over an Ethernet network you need at least one IP-enabled card access controller (called a Master Node).

The TX3 Configurator software can connect to any of these network configurations. How you connect to the network (that is, through TCP/IP, USB, a modem, or the COM port) determines what devices you can configure on the network using the TX3 Configurator. The different network configurations are explained in the rest of this section.

Figure 1 shows a basic Card Access System with one card access controller and two card readers. The maximum distance between the card access controller and the card readers is 500 feet.

Figure 1. Basic Card Access System

Figure 2 shows a network with two card access controllers connected to an RS-485 network. The Card Access System can have up to 63 card access controllers networked together. If you connect to any device on the RS-485 network (using USB, a modem, or a COM port), you can also connect to and configure any other device on the RS-485 network using the TX3 Configurator software.

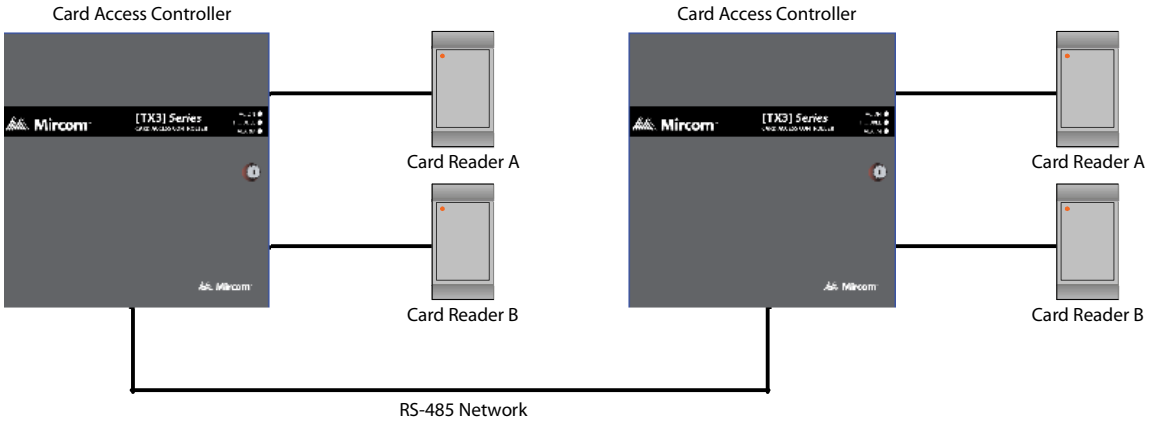


Figure 2. Card Access System using an RS-485 network

Figure 3 shows a configuration with card access controllers connected to an Ethernet TCP/IP network. This configuration removes the 63 device limitation that you have on an RS-485 network. The devices connected to an Ethernet TCP/IP network are called Master Nodes. If you connect to the TCP/IP network with the TX3 Configurator, you can connect to and configure any of the Master Nodes

on the Ethernet TCP/IP network. If you connect directly to one of the Master Nodes using USB, a modem, or a COM port, you will be able to configure that device but not any other device.

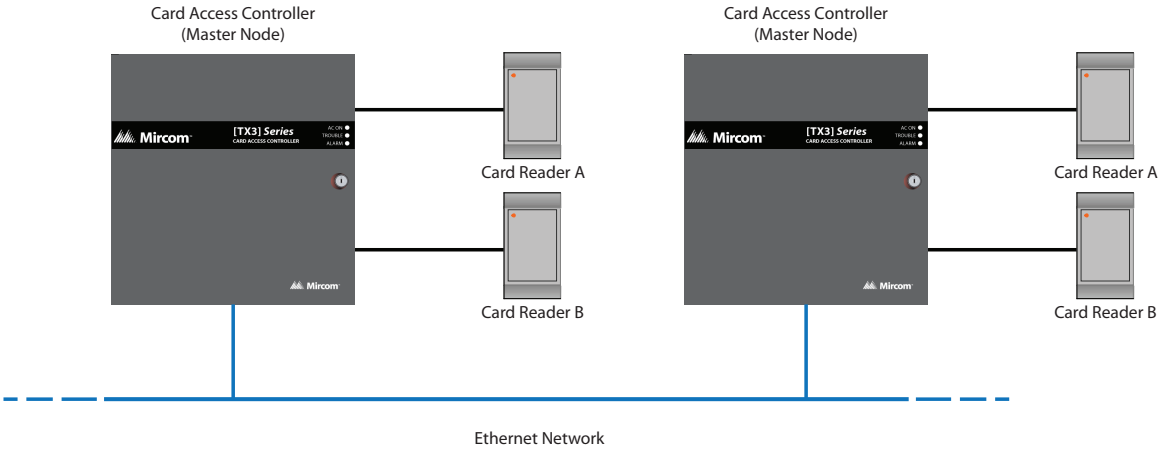


Figure 3. Card Access System using an Ethernet TCP/IP network

Notes: In order for a panel to be a Master Node:

- It must be IP capable. Panels that are IP capable have "-A", "-B", or "-C" at the end of their model names.
- It must have a TX3-IP IP Module installed if it is a Touch Screen.

Figure 4 shows a Card Access System using an Ethernet network with RS-485 subnetworks. The card access controllers connecting to a Master Node's RS-485 subnetwork are Slave Nodes to the Master Node. Each RS-485 subnetwork can have up to 63 controllers connected to it; you can still have more than 63 Master Nodes connected to the Ethernet network.

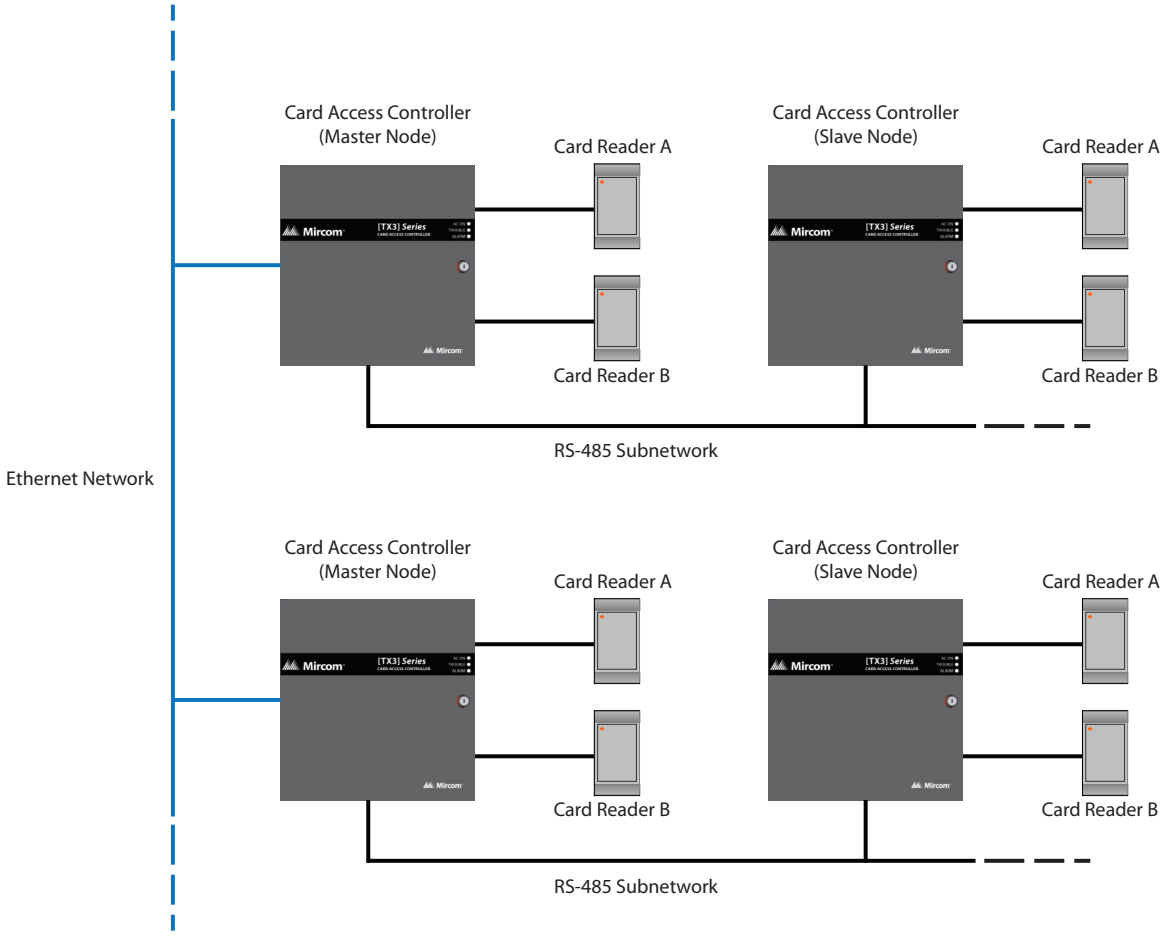


Figure 4. Card Access System using both Ethernet and RS-485 networks

If you connect to the Ethernet TCP/IP network with the TX3 Configurator, you can configure any of the nodes in the system. If you connect directly to a controller using USB, a modem, or a COM port, you will only be able to configure devices that are on the same RS-485 subnetwork as that device.

Note: There can only be one Master Node on an RS-485 subnetwork. That is, you cannot connect one RS-485 subnetwork to another RS-485 subnetwork. However, if you want to connect to a Touch Screen panel remotely over the Internet (for instance, to

configure Touch Screen options such as color and themes), the Touch Screen panel must be set as an Master Node even if there is no slave panel connected to it.

1.5 About this Manual

This manual covers the following models:

- TX3-CX-2-A Two Door Card Access Controller (includes 1 card access controller board and 1 power transformer)
- TX3-CX-4-A Four Door Card Access Controller (includes 2 card access controller boards, 1 TX3-IP IP Module, and 2 power transformers)
- TX3-CX-6-A Six Door Card Access Controller (includes 3 card access controller boards, 1 TX3-IP IP Module, and 3 power transformers)
- TX3-CX-8-A Eight Door Card Access Controller (includes 4 card access controller boards, 1 TX3-IP IP Module, and 4 power transformers)
- TX3-IP IP Module (allows a card access controller to connect to an Ethernet TCP/IP network as a Master Node)
- TX3-USB-AD Kit (converts RS-485 signals to USB)
- TX3-MDM Modem Module (not permitted in UL 294 applications)

1.6 Contact Us

1.6.1 Canada and USA

Toll Free: 1-888-660-4655

Local: 905-660-4655

Fax: 905-660-4113

1.6.2 Website

http://www.mircom.com

2 Configurable Features

This chapter describes all the configurable features and their modes of operation, and provides you with detailed information to let you configure the system using the Configurator software.

For details on using the Configurator, see LT-995 TX3 Configuration and Administration Manual.

This chapter explains

- Inputs
- Correlations
- Access Criteria
- Timers
- Schedules
- Holidays
- System Status

2.1 Inputs

Each card access controller has eight inputs to accommodate the following special functions:

- Request to exit for reader A or B
- Door sense for reader A or B
- General purpose

2.1.1 Request to exit for reader A or B

When this input is active, the system unlocks the lock and the handicap lock for either reader A or B. In addition, the **Unlock time** timer starts. When the **Unlock time** timer expires or the door contact associated with this card reader becomes active, the doors lock.

The input is associated with the ‘request to exit’ function.

2.1.2 Door sense for reader A or B

When the door is open this input is active and when the door is closed the input is inactive. This input:

- senses if the door ever opened after it was unlocked as a result of access being granted. If the door did not open even though the door was unlocked for the programmed time duration, it is reported to the Configurator if configured.
- senses a forced entry. If the door is locked and the door contact input becomes active, the forced entry alarm activates. This can be changed by selecting **Disable forced entry alarm**.
- senses if the door is held open. This happens when the door is unlocked and the door contact becomes active but does not get inactivated before the **Unlock time** timer or the **Extended unlock time** timer expires. At this time the **Door held open warning** timer starts. If the door is still open when this timer expires, a **Door held open warning** is reported to the Configurator.

  When the **Door held open warning** timer expires, the **Door held open alarm** timer starts. When the **Door held open alarm** timer expires, a door held open alarm is reported to the Configurator.

  If the door closes during the time when the **Door held open warning** timer or the **Door held open alarm** timer are active, the warning or alarm is cancelled, and the **Door open warning restored** or **Door open alarm restored** event is reported to the Configurator.

2.2 Correlations

The correlations function lets you establish specific relationships between panel inputs (events) and outputs (actions), such as turning on a light when a door opens. Correlations also allow you to specify these relationships to a schedule, such as allowing access only during certain days and times of the week. A maximum of 32 correlations is allowed.

2.2.1 Assigning events to access points

Assigning events to access points associates the access point with the event. The Configurator lets you assign input events by labelling the following access points:

- Reader A
- Reader B
- Inputs 1 to 8

2.2.2 Events

Events are defined by the following inputs and reader states:

- Access is granted (*from Reader A or B*)
- Access is denied (*from Reader A or B*)
- Forced entry alarm (*from Reader A or B*)
- Door held open alarm (*from Reader A or B*)
- Door not open (*from Reader A or B*)
- Input is active (*from Inputs 1 to 8*)
- Unlock mode is on (*from Reader A or B*)
- Unlock mode is off (*from Reader A or B*)
- High security is on (*from Reader A or B*)
- High security is off (*from Reader A or B*)

2.2.3 Actions

An action is defined by the type of action that occurs for a specific event and consists of the following:

- Turn ON output
- Turn OFF output
- Turn ON high security
- Turn OFF high security

2.2.4 Panels

Correlations can be applied to either one of the panels on your system, all of the panels on your system, to a custom group of panels on your system (for TCP/IP networks only), and across all panels on the network. They can occur on the local panel, distributed panels or different types of panels (Card Access and Telephone Access) on the network.

Note: Correlation signals cannot be transmitted by Touch Screen Master Nodes. If you plan on setting up correlations either all of the panels on your network or a custom group of panels, consult LT-995 for instructions on selecting the **Route IP Correlations** checkbox.

2.2.5 Output

Actions are applied to an output on the panel(s) selected. This option specifies which output.

2.2.6 Duration

The duration of the action is specified in minutes and seconds, or indefinitely.

2.2.7 Schedule

The schedule lets you specify when correlated events take effect.

2.3 Access Criteria

If connected to a PC, the Configurator software monitors the functional state of inputs from all panels and devices, and senses the status of connected components. Outputs are programmed for specific functionality, such as specific delay and on/off times.

Granting access depends on different criteria, such as security precautions and the access privileges granted the card holder. To prevent unauthorized access the controller has various configurable features for determining the conditions and type of access.

Access requirements are a function of schedule, holidays, security precautions and access privileges. The parameters are configurable and allow for very detailed system operation. For example access privileges may have dependencies and consequently may be more suitable to run as a scheduled task.

The Configurator software lets you define and configure the various modes of operation for managing access, defining inputs and assigning outputs. In order to effectively use the Configurator you must understand these configurable features.

The following features are configurable:

- Lock / Unlock
- High security
- PC decision required
- Facility code
- Card + PIN
- Anti-passback
- Temporary card
- Interlock
- Access Level
- Controller options
- Access point options
- Card options

2.3.1 Lock / Unlock

An access point has one of the following lock status modes:

Lock Mode. When in lock mode the door is normally locked. Any valid access card unlocks the door for the duration of a specified time interval according to:

- door unlock time
- extended unlock time

During this mode the red LED on the card reader associated with this access point becomes active and turns green for the duration the door is unlocked.

Unlock Mode. When in unlock mode the door is unlocked. The green led on the reader associated with this access point stays lit. During this mode the door sense is not monitored for the following:

- door did not open
- door held open warning
- force entry alarm

2.3.1.1 Changing the lock/unlock mode

The lock/unlock mode is changed in one of the following three ways:

- an administrator using the Configurator can send a command to change the lock mode
- an access card with lock/unlock privileges, if swiped twice in succession, toggles between lock and unlock mode
- a schedule associated with the lock/unlock mode - when the associated schedule is active, it changes to unlock mode and when the schedule is inactive, it changes back to lock mode

Whenever the mode is changed from lock to unlock or from unlock to lock, the beeper on the reader associated with this access point sends a distinct beep indicating the mode is changed.

2.3.2 High security

The high security mode grants access to cards with the high security privilege. This mode is changed as follows.

- if the access point is configured as high security then it is in high security mode by default unless changed by the PC or card with high security privilege
- if an access card with high security privilege is swiped four times in succession, the mode toggles between high security on to high security off

- the Configurator software can change the mode from high security on to high security off or from high security off to high security on
- an event correlated with a response to turn on or off the high security mode

The high security mode locks all doors in the unlocked mode.

Whenever the high security mode changes, the beeper on the reader associated with this access point sends a distinct beep.

2.3.3 PC decision required

During this mode the decision to grant access is transferred to an attendant. Using the PC the attendant grants or denies access. Only valid cards assigned with the PC decision requirement are able to make this type of access request.

2.3.4 Facility code mode

Access cards consist of two codes; facility code and card code. The facility code mode is designed for new installations where access cards are not programmed into the database. When the facility code mode is enabled, cards with same facility code are granted access.

The facility code can be set to any number. If a number is not chosen, it will automatically default to “0” as a placeholder.

In this mode, the door is unlocked for the same period of time that as that of the standard door unlock timer. This mode is configured for each access point.

2.3.5 Card + PIN

This mode provides another level of security during certain parts of the day. During this mode not only a valid card is required for access but also a PIN code. The PIN code is 1 to 4 digits long and is programmed for each card. 0 is not a valid PIN code.

There is a schedule associated with this mode. When the schedule is enabled, the mode is on and when the schedule is disabled, the mode is off.

This feature requires a card reader with a keypad.

2.3.6 Anti-passback

This mode prevents unauthorised users from getting access. During the anti-passback period if a valid card is used at an access point, it cannot be re-used at the same access point until the pre-programmed anti-passback timer expires. After expiration of the timer, the user regains access.

2.3.7 Temporary card

This type of card can be created by placing a usage counter on the card. Each time the card is used, the usage counter is reduced by one. When the usage number reaches zero, access is denied.

A usage counter of 255 indicates there is no restriction on use.

2.3.8 Interlock

This mode is typically used in a double door application to prevent unauthorised access. During this mode the user presents the card at both doors. The second door unlocks after presenting the card, if the first door is locked and closed.

If enabled door B cannot be unlocked until door A is locked and closed. Door A cannot be unlocked until door B is locked and closed.

2.3.9 Access level

Creating an access level lets you define where and when to use a card, and set elevator usage if elevator controls are used.

A maximum of 128 access levels are defined for each controller. A schedule is associated with each access level for all the access points on the controller as indicated by the following example.

Access level ID = 1

- for reader A schedule = Always
- for reader B schedule = Never

Access level ID = 2

- for reader A schedule = Office hours
- for reader B schedule = Always

If a card is assigned an access level 1 it means the user can have access to reader A at all times but will not have access to reader B at any time.

If a card is assigned an access level 2 it means the user can have access to reader A during the office hours and will have access to reader B all the time.

The option for elevator control exists for each access level. If elevator control is enabled for a specific access level then swiping a card with that access level will turn on the associated elevator relays. Which relays are activated can be specified individually for each access level. Up to 16 elevator relays can be activated for each access level. If more than 16 relays are assigned to a specific access level only the first 16 will be activated.

2.3.10 Controller options

The following controller options are configurable:

Card format. The following card formats are supported.

Note: Only the first format listed here (26-bit Wiegand SIA standard format) is evaluated to UL 294. The other formats listed here cannot be used in UL 294 applications.

- 26-bit Wiegand SIA
- 32-bit CSN
- 34-bit Awid
- 35-bit HID corporate 1000
- 35-bit Indala
- 36-bit HID Simplex
- 36-bit Keyscan C15001
- 37-bit Cansec
- 37-bit HID 10304
- 37-bit Mircom
- 39-bit Kantech XSF
- 50-bit RBH

Send real time logs. If enabled, only the real time logs are sent to the PC.

Interlock feature. If enabled, door B cannot be unlocked until door A is locked and closed. Door A cannot be unlocked until door B is locked and closed.

Facility code. Facility code is set to any value is used in the facility code mode. The default is 0.

2.3.11 Access point options

The following access point options are configurable:

Auto relock. Enabling this option locks the door when the door closes before the door open timer or extended door timer expires. Disabling this option locks the door, but only after the expiration of door open timer or extended door open timer.

Deduct usage count. For cards designated as “temporary” (that is, the usage counter option is enabled and set to a value below 255), this option decreases the usage counter by one every time this card is used at the access point. When the usage counter reaches zero, the card deactivates.

Disable forced entry alarm. If this option is enabled, the forced entry alarm does not activate even if the door is opened without permission. Instead, access is granted. This is usually used on access points where there is no request to exit (RTE) device.

Note:	If you select this option, then you should also select **Report request to exit** so that every time access is granted, it is reported in the Online Events.

Ignore card facility code. This option is enabled by default meaning that only card number will be processed. If this option is unchecked, then for every card, card number and facility code will be processed to grant access.

PC decision required. When enabled granting access is transferred to the PC from the controller. For this option to work the PC needs to be on all the time with an attendant. Use this option when the building has a security desk or a concierge.

First person In. Configuring the access point for the lock/unlock schedule, causes the door to remain locked at the start of the unlock schedule, until the first valid card with this privilege is presented to the card reader. The door continues to remain unlocked for the remainder of the unlock schedule.

RTE bypass DC. Enable this option if there is a mechanical egress device installed on the door. In this situation, the door is unlocked manually, and the TX3 system does not unlock the door. If the door is opened, the system updates the door status and the LED on the reader turns green. The door contact is bypassed and so there is no forced entry alarm.

High security. When enabled only access cards with the high security privilege are able to open the door.

Report request to exit. This option logs and monitors events and system status. When enabled any requests to exit are logged and reported to the Configurator. Since the person exiting is not known, only the time and date and the request itself is logged and reported.

Report door not opened. When enabled this option logs and reports events when access is granted but the door remains closed.

Report unknown format. When enabled this option logs and reports access attempts with a card with an unknown format.

Facility code mode. Enabling this mode grants access to cards based on only their facility code. This allows nonprogrammed cards to have complete building access. Use only when necessary.

Inhibit ID. When enabled the card code is not sent to the PC. This feature is used for logging and reporting purposes.

Timed Anti-passback. When enabled access is not permitted at the same access point for a specific amount of time specified by the anti-passback timer.

2.3.12 Card options

Access cards are configured for the following features:

Usage counter. The usage counter is used for temporary cards. The usage counter can be given any value from 1 to 255. Using 255 means there is no restriction on usage. If any other value is used it means the card is only usable for that number of times.

Status. The status of the access card is marked as:

- Active
- Inactive

Inactive cards are not granted access. Active cards are granted access provided all the other conditions like schedule and privilege are met.

Access level. Select the access level for the card. Access levels are configurable on the basis of privilege. Up to 128 access levels can be defined for the system.

PIN. The PIN code is a 1 to 4 digit numerical value used during the card + PIN schedule. 0 is not accepted.

Ignore anti-passback. When this option is enabled the card holder is not restricted by the timed anti-passback mode.

Lock/Unlock privilege. When this option is enabled the user has the privilege of unlocking the door by presenting the card to the reader twice in succession.

High security privilege. When this option enabled only access cards with this privilege are able to open the door.

Extended unlock time. When this option is enabled the door opens for the extended unlock time (see section 2.4.3 on page 23). This option is normally given to seniors and persons with disabilities.

Handicap. When this option is enabled the output designated as accessible is activated along with the main door.

First person in. This option works in conjunction with scheduled unlock modes only. If the First person in setting is enabled, only a card with the First person in privilege can start the unlock mode.

2.4 Timers

The following types of timers are associated with the Card Access System operation:

- Unlock time
- Extended unlock time
- Anti-passback
- Door held open warning
- Door held open alarm

2.4.1 Timer schedule

Events are scheduled as Always, Never, or administrator defined. Timed access adheres to a schedule as follows:

Auto-unlock schedule. When enabled the door remains unlocked during the schedule.

PIN required schedule. Card access requires the use of a PIN during the schedule.

2.4.2 Unlock time

The door unlock timer starts when the door unlocks. When the timer expires the door locks. The main door unlock timer is programmable from 0 to 300 seconds. The default is 10 seconds.

2.4.3 Extended unlock time

This extended unlock timer mode is used for cards with the extended unlock feature enabled. The timer starts when the door unlocks. When the extended unlock timer expires the door locks. The timer resets when the main door sense is programmed to be inactive. The extended unlock timer is programmable from 10 to 300 seconds. The default is 15 seconds.

2.4.4 Anti-passback

The anti-passback timer starts when access is granted. In this mode the user cannot re-enter this door until the anti-passback timer expires. When the timer expires the user has access. The anti-passback timer is programmable from 0 to 900 seconds. The default is 300 seconds.

2.4.5 Door held open warning

The door held open warning timer starts when access is granted. When the door unlock timer expires and the door does not close during this interval a ‘door held open’ warning is issued to the PC and the common trouble status becomes active. If the door closes during this interval, the timer resets and no warning report is sent to the PC.

The door held open warning timer is programmable from 10 to 900 seconds. The default is 30 seconds

2.4.6 Door held open alarm

The door held open alarm timer starts when the door held open warning timer expires and the door remains not closed. When this timer expires and the door is still open, a ‘door held open alarm’ is issued to the PC and the common alarm status becomes active. The door held open alarm timer is programmable from 10 to 900 seconds. The default is 60 seconds

2.5 Schedules

Schedules let you set up a timetable to establish when certain actions are permitted to occur, such as door access. These schedules are designated and listed by name in the Configurator software, and are available for selection wherever it is necessary to invoke access permission.

The system can store up to 64 schedules. Each schedule consists of eight periods with each period consisting of

- Start time and end time in hours: minutes format
- Days of the week and Holiday selection

Each schedule has an ID and a label to identify the schedule for use in the Configurator software.

If the current time and day satisfies any one of the eight periods in a schedule, the schedule is considered to be active; otherwise, it is inactive.

By default the following two schedules cannot be edited:

- 'Always' schedule
- 'Never' schedule

Schedules are used for the following:

- Timer schedule
- Correlations
- Auto-unlock

- PIN required schedule
- Access levels

2.6 Holidays

Up to 128 holidays can be entered in the system. Each holiday consists of the following:

- start time/date
- end time/date

If a holiday falls on the same date each year it can also be programmed as an annual event.

Each holiday has a holiday ID and label to identify the holiday for use in the Configurator software.

By default, New Year (January 1) is already programmed into the system.

2.7 System Status

The controller monitors inputs for trouble and alarm conditions.

2.7.1 Common trouble

The common trouble indicator is active when any of the following inputs receive a trouble condition:

- Any supervised input
- Power (AC and battery)
- Door held open warning

The common trouble status clears only if all the above inputs are back in normal state. When the common trouble status is active, the common trouble led flashes at a slow rate.

2.7.2 Common alarm

The common alarm status is active when any of the following inputs receive an alarm condition:

- forced entry alarm
- door held open alarm

The common alarm status clears only if all the above inputs are back in normal state. When the common alarm status is active, the common alarm led flashes at a fast rate.

3 Mechanical Installation

This chapter describes the installation and setup of the controller and card reader.

This chapter explains

- Grounding the Card Access System
- The TX3-CX-2-A Enclosure
- The TX3-CX-4-A, TX3-CX-6-A, TX3-CX-8-A Enclosure
- Mounting all Enclosures
- Installing the TX3-PS24-5A Power Supply Enclosure for TX3-CX-4-A, TX3-CX-6-A, TX3-CX-8-A (not permitted in UL 294 applications)

3.1 Grounding the Card Access System

Grounding reduces the risk of electrical shock by providing an alternate escape route for the electrical current. The Card Access System is equipped with a 16 gauge electrical wire attached to the panel chassis ground terminal. The ground terminal is shown in figure 6.

Note: Do not disconnect this wire.

Attach the end of the supplied wire to a suitable grounding wire 16 gauge or thicker. Attach the other end to the cold water ground.

3.2 The TX3-CX-2-A Enclosure

The TX3-CX-2-A enclosure mounts with four screws as shown in figure 5. The back cover is 12 inches wide by 14 inches long. The top two mounting holes are 10 inches apart.

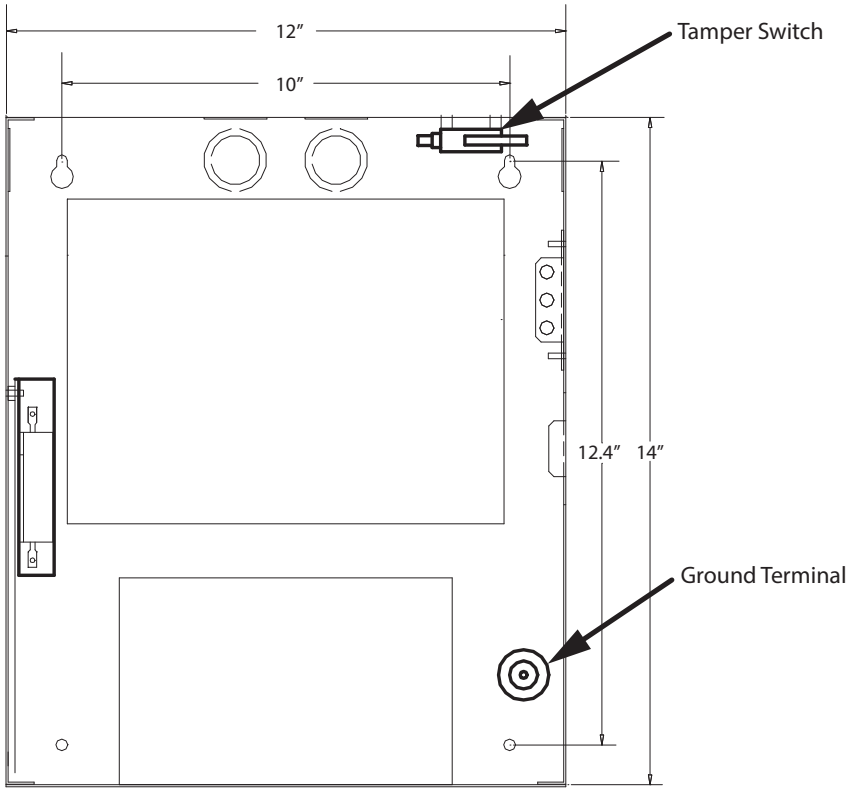


Figure 5. Enclosure dimensions for TX3-CX-2-A

3.3 The TX3-CX-4-A, TX3-CX-6-A, TX3-CX-8-A Enclosure

The TX3-CX-4-A, TX3-CX-6-A, and TX3-CX-8-A enclosures mount with four screws as shown in Figure 6.

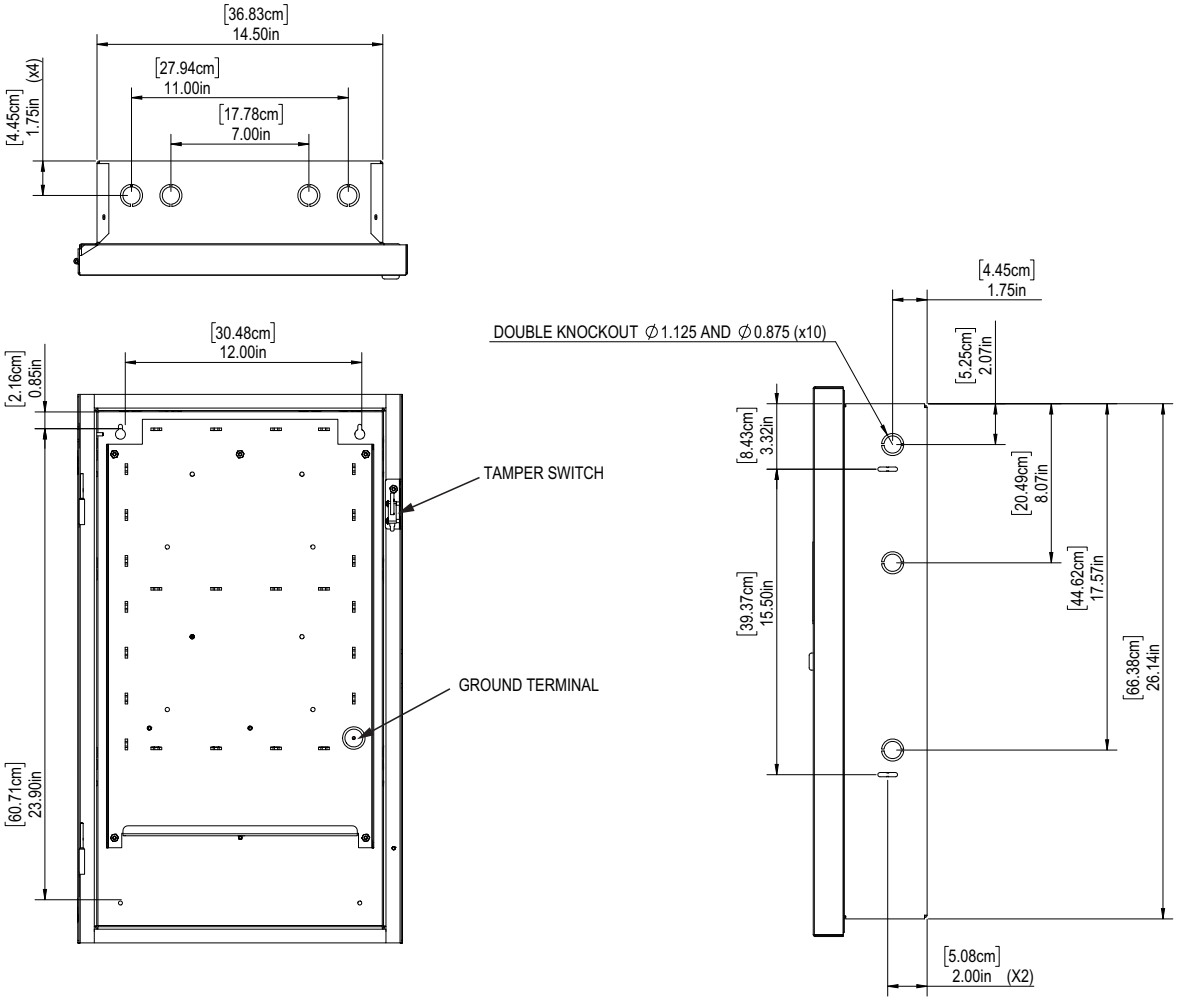


Figure 6. Enclosure dimensions for TX3-CX-4-A, TX3-CX-6-A, TX3-CX-8-A

3.3.1 Mounting of Card Access Controller Boards

Figure 7 shows how the card access controller boards are mounted in the TX3-CX-4-A, TX3-CX-6-A, TX3-CX-8-A enclosure. Up to 4 card access controller boards can be mounted in the enclosure. The card access controller boards are mounted in two layers using standoffs. A ribbon cable connects the LEDs on the door to the P7 LED port on the boards.

Note: In the TX3-CX-4-A, TX3-CX-6-A, TX3-CX-8-A enclosure, the card access controller boards are turned so that the power connection is on the top and the P7 LED display port is on the left.

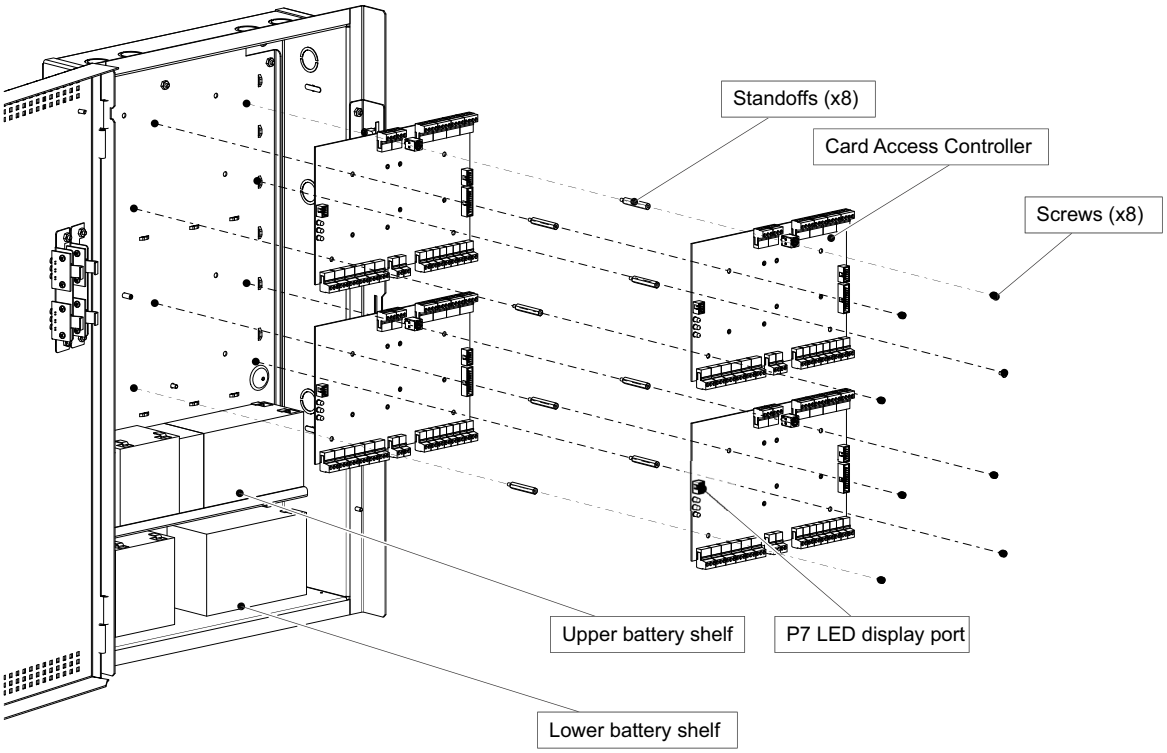


Figure 7. Installation of the controllers in the TX3-CX-4-A, TX3-CX-6-A, TX3-CX-8-A enclosure

3.4 Mounting all Enclosures

To mount the enclosure

1. Find a suitable location for the enclosure beside a wall stud.
2. Using the enclosure as a template, mark the top two mounting holes as shown in figures 5 and 6.

3. Place the screws halfway into the wall in the position shown using a suitable screw.
4. Hang the box onto the two screws.
5. Screw the other two screws at the bottom of the enclosure.
6. Tighten all four screws into place.

3.5 Installing the TX3-PS24-5A Power Supply Enclosure for TX3-CX-4-A, TX3-CX-6-A, TX3-CX-8-A (not permitted in UL 294 applications)

Note: The TX3-PS24-5A power supply is not evaluated to UL 294.

The TX3-PS24-5A external power supply is a 156 W, 24 V single output switching power supply encased inside a metal enclosure. A voltage selectable switch is located on the side of the power supply and is factory set to 115 V but can be switched to 230 V.

To set the voltage on the Switching Power Supply

1. Ensure that the TX3 unit is off and that all power is disconnected.

Warning: The power must be turned off before the switching power supply is accessed. Failure to due so may result in damage to the equipment or electric shock that can lead to death.

2. Open the switching power supply box using the key for the TX3 unit. The switching power supply unit is secured inside the box by metal guides and two screws on either side of the terminal block. Unscrew and remove the screws on both sides of the terminal block.

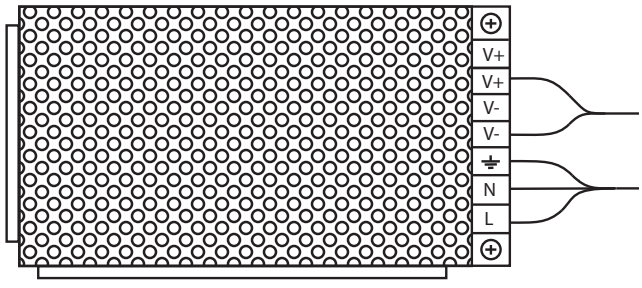


Figure 8. Inside the TX3-PS24-5A enclosure

3. Lift the switching power supply unit out of its box to access the red voltage selection switch.

4. Switch the voltage selection switch to the required voltage level. Place a flathead screwdriver in between one of the holes in the chassis to access the switch. By default it is set to 115 Volts.

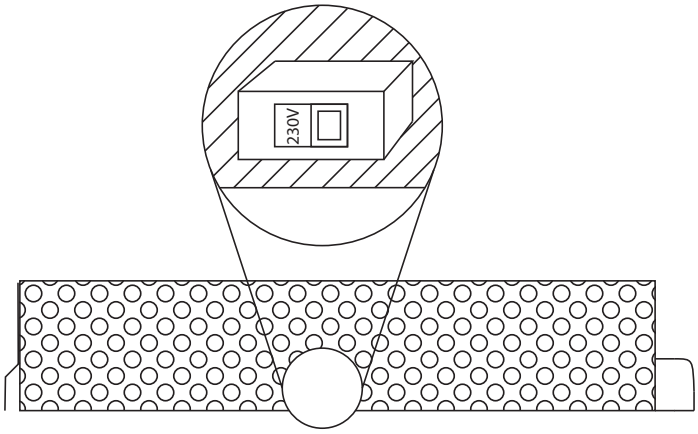


Figure 9. TX3-PS24-5A voltage selection switch

5. Place the switching power supply back into the box using the metal guides to position it and then replace the screws on both sides of the terminal block to secure it into the box.
6. Reconnect the power.

The external power supply connects to the building power AC power supply. It is recommended that the unit is powered by its own dedicated electrical outlet to protect it from excessive power surges and current fluctuations.

Note: Install the power supply outside the Touch Screen enclosure.

Overall dimensions: height: 7 23/32” (196 mm),
width: 9 53/64” (250 mm), depth: 2 37/64” (66 mm)

Knockout dimensions: 1 1/8” (29 mm) and 7/8” (22 mm)

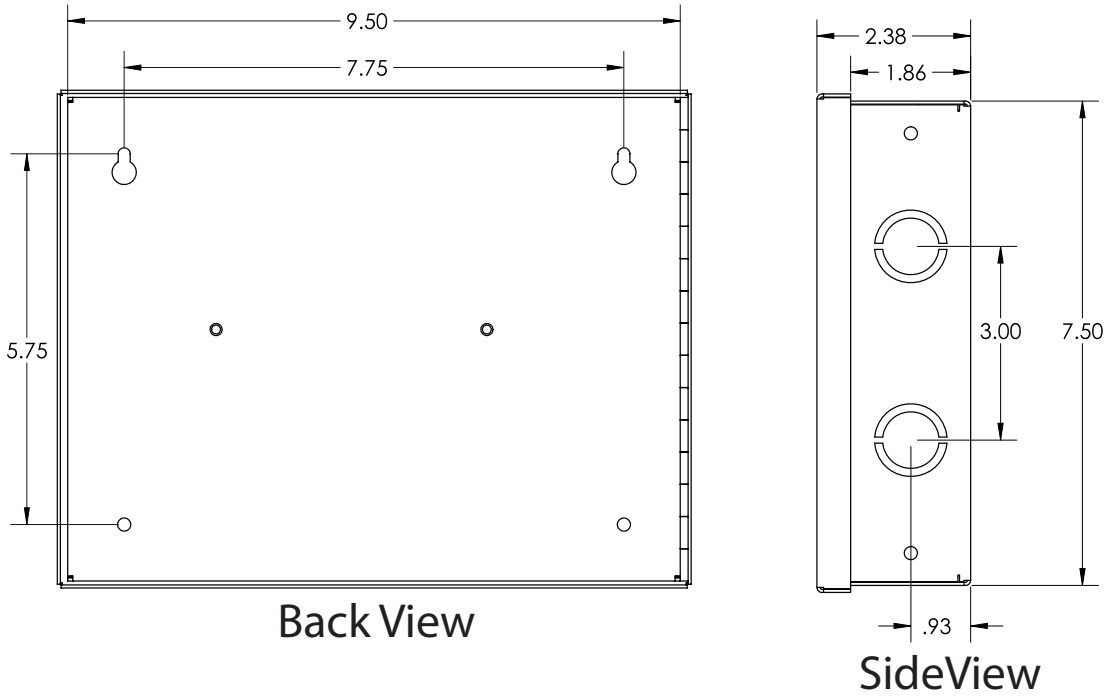


Figure 10. TX3-PS24-5A enclosure dimensions

To surface mount TX3-PS24-5A

You need:

- 4 fasteners appropriate for the wall that you are mounting the enclosure on.

1. Find a suitable location for the power supply enclosure, such as over a wall stud.
2. Using the enclosure as a template, mark the two top mounting hole locations as indicated in Figure 10. Ensure that at least one side is over a wall stud.
3. Remove the enclosure and place two wall fasteners halfway into the marked hole locations.
4. Place the enclosure onto the fasteners and lower it so that the fasteners fit in the narrow part of the keyholes.
5. Screw the other two fasteners into the two remaining holes.
6. Tighten all four fasteners into place.

Note: The enclosure can also be mounted directly onto the drywall using anchors.

4 Setup of the Card Access Controller

This chapter describes the installation and setup of the controller and card reader.

This chapter explains

- Controller Board Description
- Optional Components
- Power Supply Connection
- TX3-PS24-5A Power Supply (not permitted in UL 294 applications)
- RS-485
- USB Port
- Inputs
- Outputs
- Card Readers
- Setting DIP Switches SW2
- Setting Jumpers
- Turning on the Controller
- Updating Firmware
- Beginning Configuration

4.1 Controller Board Description

The Card Access System controls access points according to how the inputs and outputs are defined and correlated with each other. Inputs and outputs are defined by how the access and control points are wired with the controller.

Before you begin you must establish how you want the outputs to behave as a function of the inputs. For a complete description of correlation and the modes of operation see section 2 on page 13.

Keep a record of the wiring for configuration purposes.

4.1.1 Controller Panel LEDs

There are three status LEDs on the front of the Card Reader Panel:

AC ON LED. `AC ON LED` illuminates steady green when AC power is present.

Trouble LED. `Trouble LED` flashes amber at a slow rate when there is a common trouble condition in the system. Trouble consists of:

- any supervised input
- AC power/low battery
- door held open warning

Alarm LED. `Alarm LED` flashes red at a fast flash rate when there is a forced entry or the door held open alarm timer expires.

4.1.2 Controller Board Components

The card access controller consists of the following terminals:

- 8 inputs
- 8 outputs (6 relay contact outputs and 2 outputs providing 12 VDC)
- connections for two card readers (noted as Reader A and Reader B)
- power supply
- RS-485 connector
- USB, IP Module, and Modem board connectors

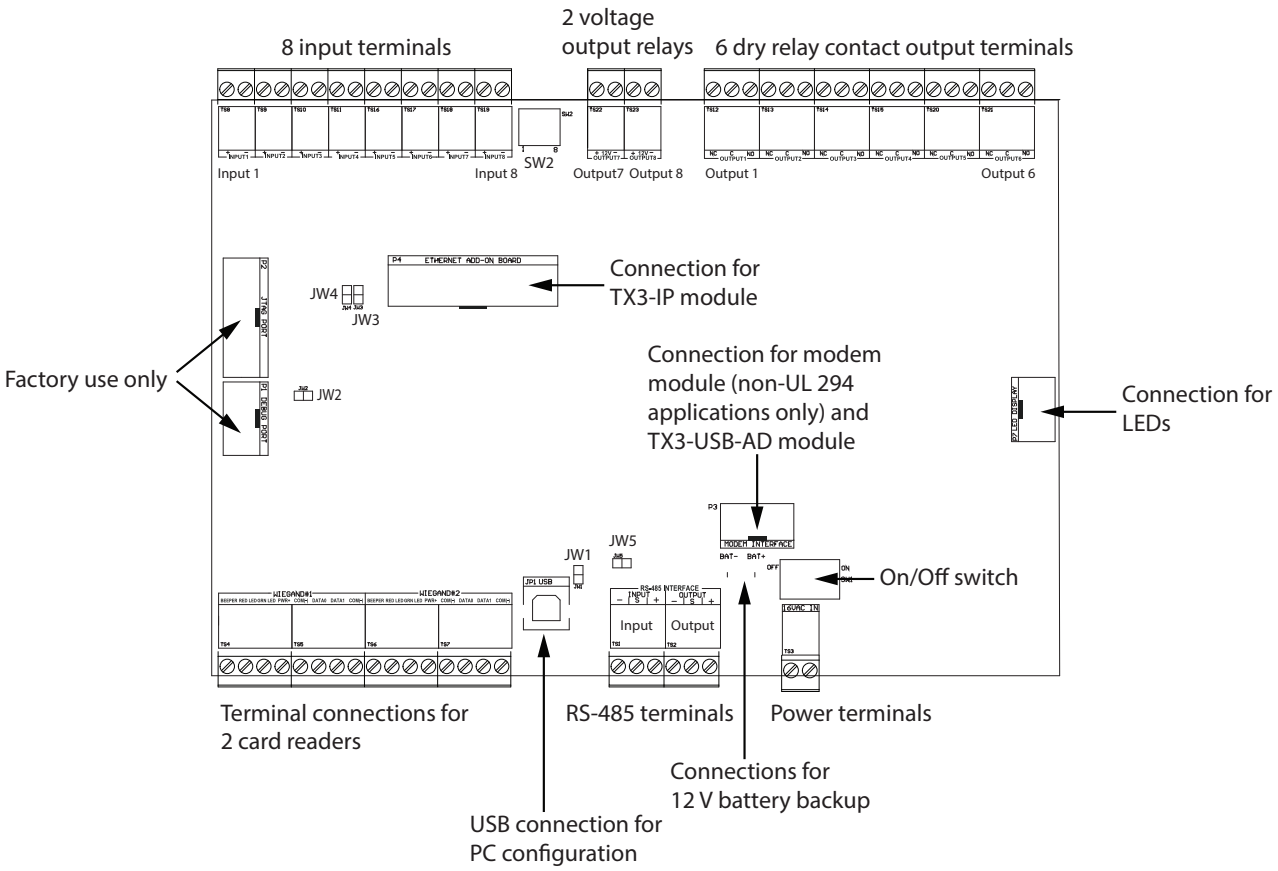


Figure 11. Controller board connection locations

Note:	In TX3-CX-4-A, TX3-CX-6-A, and TX3-CX-8-A, the card access controller boards are turned so that the power connection is on the top and the LED display port is on the left.

4.2 Optional Components

Install the following optional components as required:

- Tamper switch
- TX3-IP Module
- TX3-USB-AD Kit
- Battery Backup
- TX3-MDM Modem Module (not permitted in UL 294 applications)

4.2.1 Tamper switch

The tamper switch is located as shown in figures 5 and 6. Connect the tamper switch wire to the general purpose input and correlate the opening of the cover to a specific output (action). For a complete description of correlations see section 2 on page 13.

4.2.2 TX3-IP Module

The TX3-IP Module kit comes with the IP Module which allows a card access controller to connect to an Ethernet TCP/IP network as a Master Node.

To install the TX3-IP Modem Module

1. Screw the four spacers to the controller board mounting holes.
2. Connect the ribbon cable to the **P4** Ethernet add-on connector on the controller board.
3. Place the IP Module board over the spacers, and then fasten into place using the four screws provided.
4. Connect the IP Module board to your Ethernet network using the RJ45 connector on the IP Module and an Ethernet cable.

For more information see the TX3-IP IP Module Installation Instructions LT-1161.

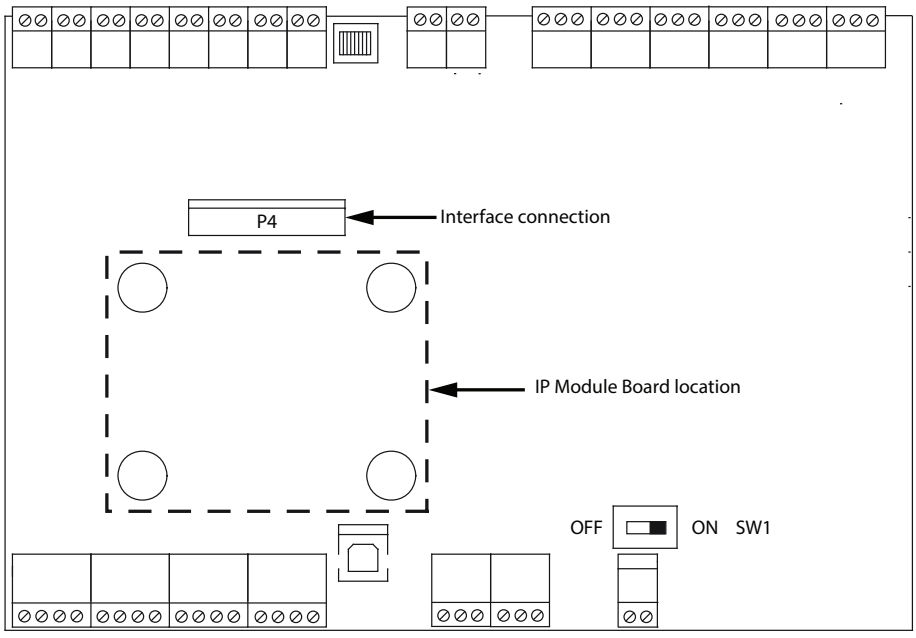


Figure 12. IP module board location

4.2.3 TX3-USB-AD Kit

The TX3-USB-AD Kit converts RS-485 signals to USB.

To install the TX3-USB-AD Module

1. Connect the ribbon cable to the **P3** connector on the card access controller.
2. Place the module over the connector position with the four spacers.
3. Align and fasten into place with the four screws.
4. Observe the correct polarity and connect the wires from the RS-485 connector on the TX3-USB-AD module to the RS-485 to USB adapter (GC-AT-820) as shown.

Note: Use 22 AWG twisted shielded pair for the RS-485 wire.

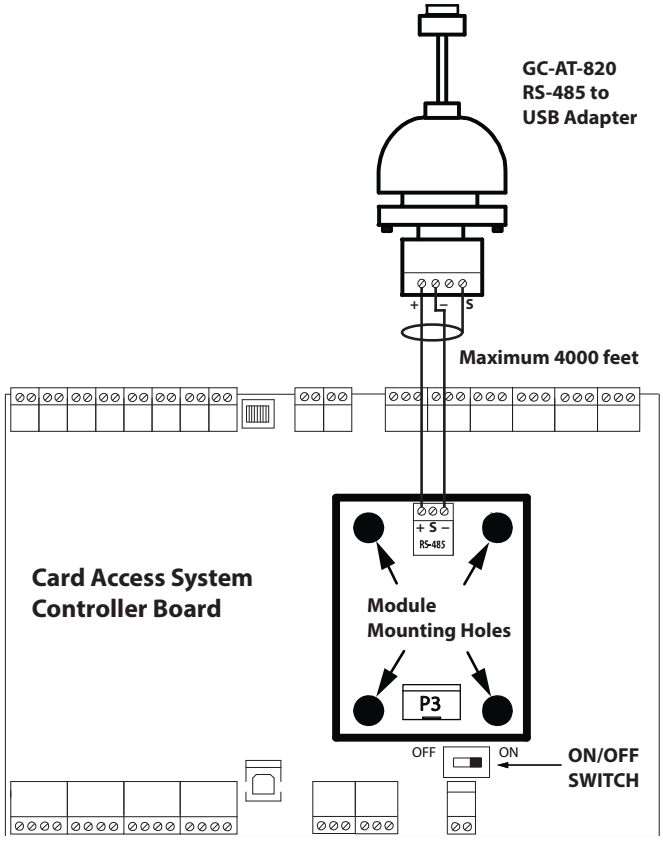


Figure 13. TX3-USB-AD board location

Table 1: RS-485 Add-On Module Jumper Settings

Mode	JW1	JW2
No termination	Open	Open
AC termination 120R + 1nF	Short	Open
No termination	Open	Short
DC termination 120R (Factory Default)	Short	Short

Note: For the main application of TX3-USB-AD, short JW1 and JW2.

For more information see the TX3-USB-AD Kit Installation Instructions LT-6027.

4.2.4 Battery Backup

Battery backup is optional. The batteries fit in the enclosures as shown in section 3.2 on page 27 and section 3.3 on page 28.

Use 12 VDC, 7 Ah sealed lead-acid rechargeable batteries. Use one battery for each card access controller board:

- TX3-CX-2: 1 battery
- TX3-CX-4: 2 batteries
- TX3-CX-6: 3 batteries
- TX3-CX-8: 4 batteries

Connect the battery to the connectors located to the left of the ON/OFF switch SW1 as shown in figure 14.

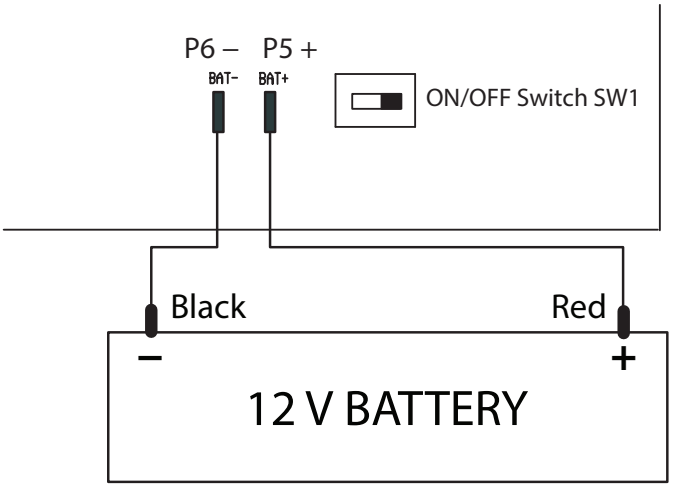


Figure 14. Controller board battery wring

4.2.5 TX3-MDM Modem Module (not permitted in UL 294 applications)

Note: The TX3-MDM Modem Module is not evaluated to UL 294.

The TX3-MDM Modem Module is designed to work only with POTS (plain old telephone system) lines.

The modem module has two telephone connectors, an RJ-11 connector and a terminal block as shown in figure 16. The terminal block tip/ring line is polarity insensitive and reversible.

To install the TX3-MDM Modem Module

1. Connect the ribbon cable to the **P3** connector on the card access controller as shown in figure 15.
2. Place the board over the connector position with the four spacers.
3. Align and fasten into place with the four screws.
4. Connect the telephone line to the RJ-11 or the Tip and Ring connectors as shown in figure 16.

For more information see the TX3-MDM Modem Module Installation Instructions LT-971.

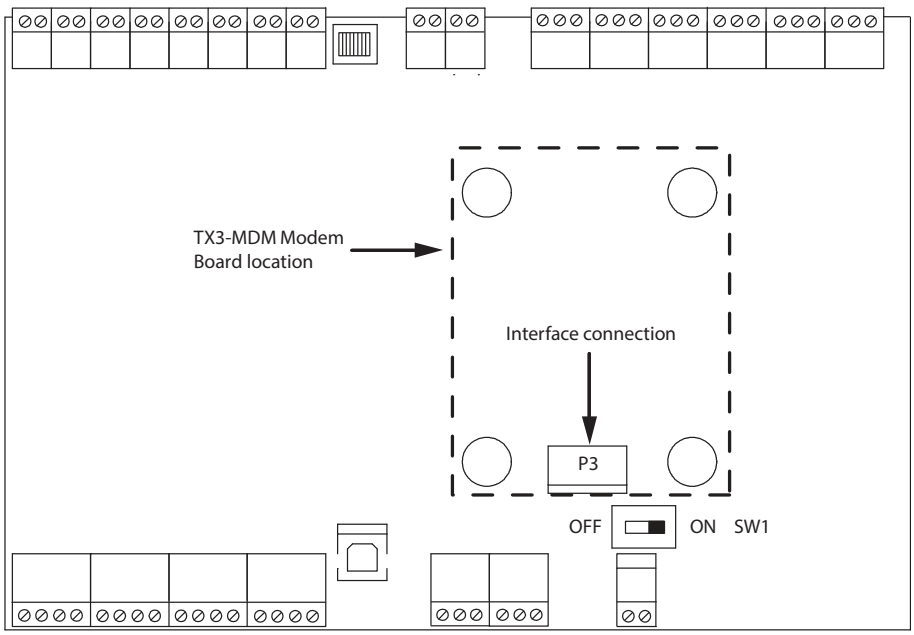


Figure 15. Modem board location

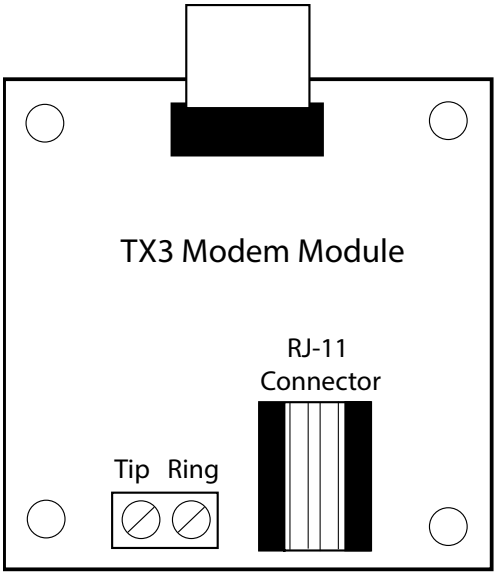


Figure 16. Modem module telephone connectors

4.3 Power Supply Options

Use one or more of the following power supplies that will cover your power needs depending on how many card access controllers you have:

- Direct plug-in Class 2 transformer (Manufactured by Yeo Heung Electronics Co. Ltd., Model No. SEP/P-1640U). One required for each card access controller board, if used for primary operating supply
- UL 294 Listed power supply
- TX3-PS24-5A external power supply (not permitted in UL 294 applications)

4.3.1 Power Supply Connection

The power supply connection on the bottom right of the controller board and receives 16 VAC, 40 VA. Use 18 AWG wiring.

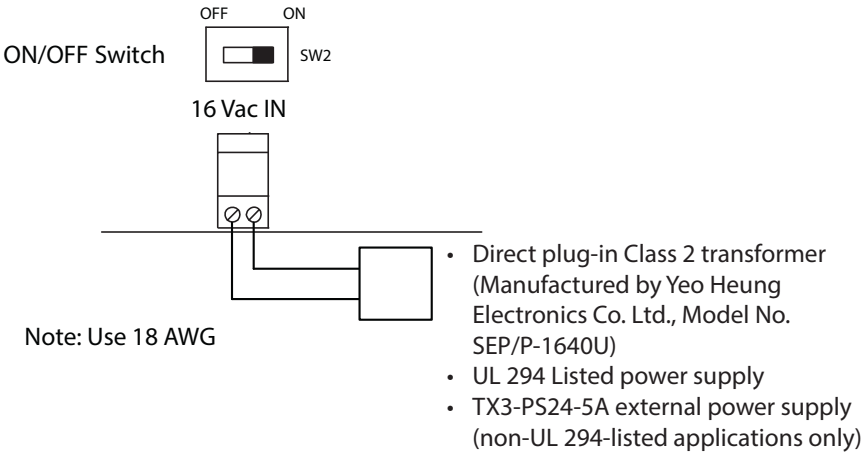


Figure 17. Controller board power supply

4.4 TX3-PS24-5A Power Supply (not permitted in UL 294 applications)

Note: The TX3-PS24-5A power supply is not evaluated to UL 294.

The power supply terminal block is shown in figure 17. It receives 24 VDC from the external TX3-PS24-5A power supply.

The external TX3-PS24-5A power supply connects to the building power AC power supply. A voltage selectable switch is located on the side of the unit and is factory set to 115 V.

For best operation install the external power supply into its own dedicated electrical outlet to protect it from excessive power surges and current fluctuations.

Note: Install the power supply outside the card access enclosure.

4.4.1 Wiring the TX3-PS24-5A Power Supply

The power supply terminals are located at the bottom of the TX3-PS24-5A external power supply as shown in Figure 18.

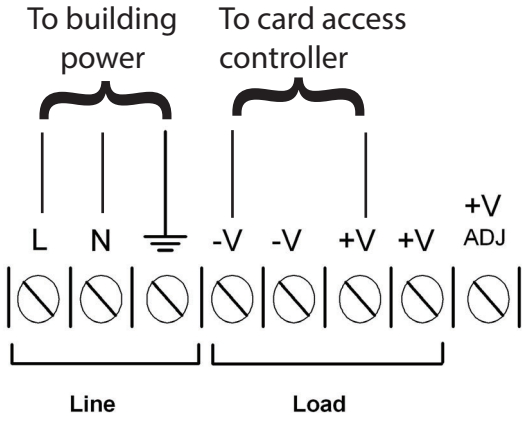


Figure 18. TX3-PS24-5A terminal block wiring

To wire TX3-PS24-5A

1. Turn off the card access controllers.
2. Set the voltage selectable switch on the TX3-PS24-5A power supply to the appropriate voltage. The voltage selectable switch can be set to either 115 V or 230 V. See section 3.5 on page 30.
3. Connect the load power supply wires to the card access controller board panel terminal screws as shown in figure 17.
4. Connect the other end of the load power supply wires to the **Load** terminal screws as shown in figure 18.
5. Connect the building power supply wires to the **Line** terminal screws as shown in figure 18.
6. Turn the power on.

4.5 RS-485

An RS-485 terminal lets you easily connect multiple Telephone and Card Access Controllers across a network. The RS-485 connection is situated at the bottom middle of the main controller board and consists of two separate terminals, each for an input and output.

Connect the RS-485 input terminal to the RS-485 output terminal of another controller. See figures 19, 20, 21 and 22.

You can close JW5 on the first and last controllers instead of using end-of-line 120 Ω resistors.

If there are problems with RS-485 communication, close both JW7 and JW8 on either the first or last controller connected by RS-485.

Note: Use twisted shielded pair grounded at one end.

Recommended cables:

- RS485 cables
  - Belden 3109A RS-485, (4 pr) 22 AWG (7x30) or equivalent
  - Belden 9842 RS-485, (2 pr) 24 AWG (7x32) or equivalent
  - Belden 9841 RS-485, (1 pr) 24 AWG (7x32) or equivalent
- CAT5 Cables
  - Belden 72001E ETHERNET Cat 5e 2 Pair, 24 AWG or equivalent
  - Belden 70006E Cat 5e, 100Mb/s, Quad, AWG 22 (1) or equivalent

Maximum total length:

- 4000 feet (1244 m) for 22 AWG
- 2500 feet (762.5 m) for 24 AWG

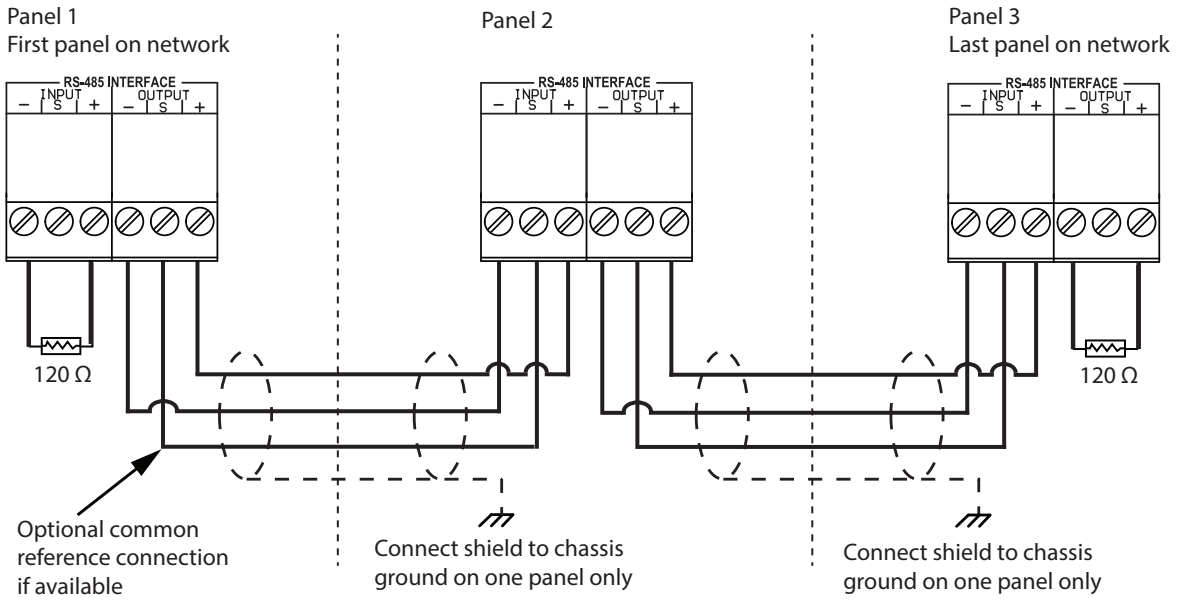
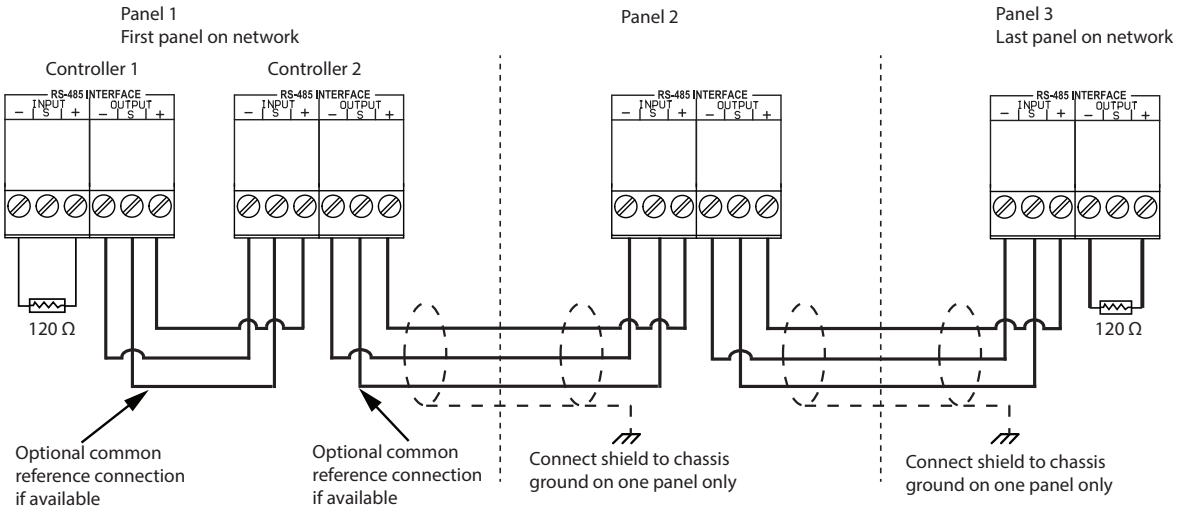


Figure 19. RS-485 Wiring for TX3-CX-2-A



NOTE: WIRES MUST BE TWISTED.

Figure 20. RS-485 Wiring for TX3-CX-4-A

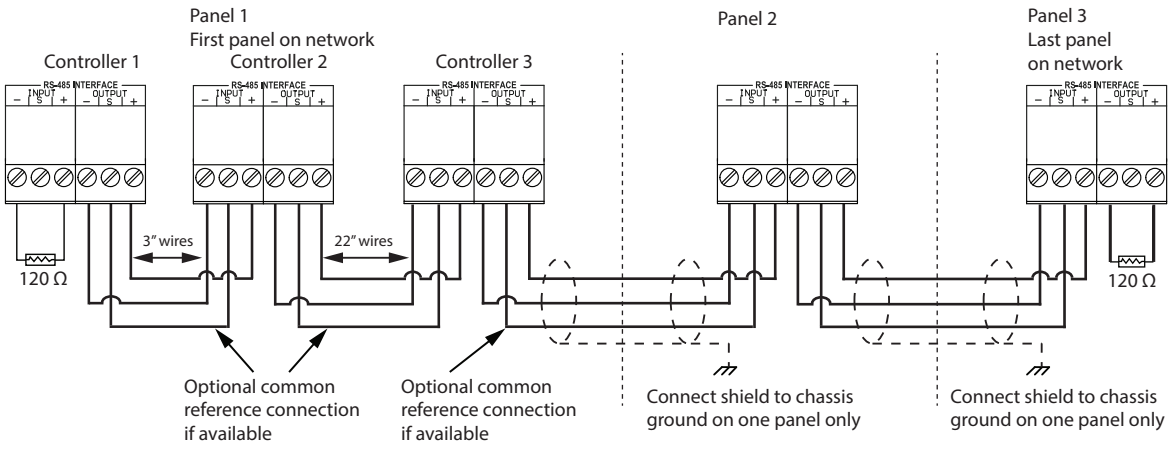


Figure 21. RS--485 Wiring for TX3-CX-6-A

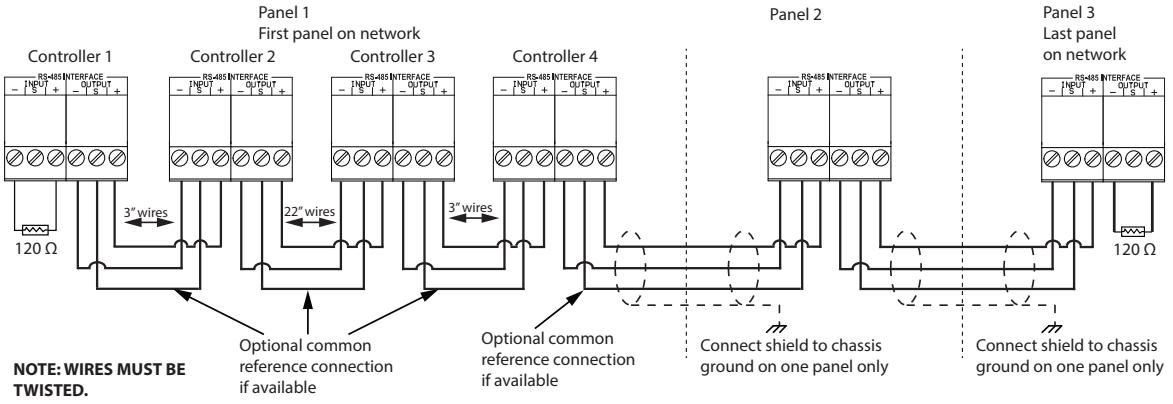


Figure 22. RS-485 Wiring for TX3-CX-8-A

4.6 USB Port

The USB port provides a connection to a PC, for configuring the Card Access System and downloading any new firmware.

4.7 Inputs

Each card access controller has eight inputs to accommodate the different types of configurable functions associated with the inputs. For additional details and a complete description of the different types of configurable functions see section 2 on page 13.

After the installation and setup is complete, the functional state of all inputs and circuit supervision types must be configured using the Configurator software. During configuration you will also establish correlations between inputs and outputs.

Depending on the device each input is configured according to:

- type of input function
- active state
- supervision requirement
- alarm delay

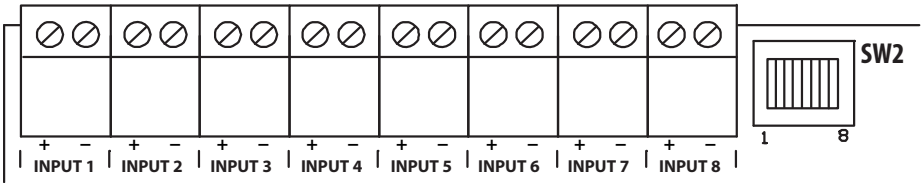


Figure 23. Controller board input terminals

4.7.1 Inputs 1 to 8

Inputs 1 to 8 are programmable inputs. Configure each input for one of the following actions. Figure 24 shows a sample connection.

- Request to Exit (reader A)
- Request to Exit (reader B)
- Door sense (reader A)
- Door sense (reader B)
- General purpose input

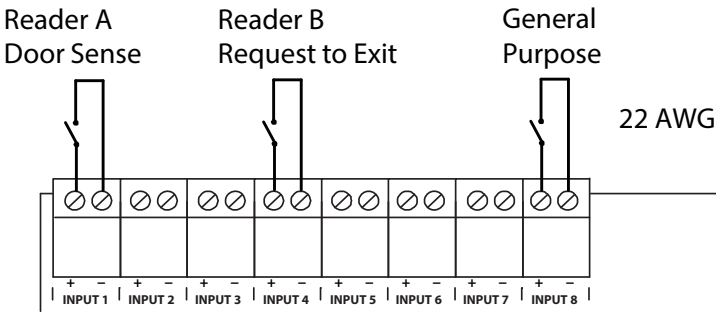


Figure 24. Input terminal sample connections

4.7.2 Request to Exit

Activation of this input unlocks the door and starts the door unlock timer.

4.7.3 Door sense

When the door is open this input is active and when the door is closed the input is inactive.

4.7.4 General purpose input

The general purpose input is mainly used for establishing a correlation with a specific output. When a general purpose input becomes active it is considered as an event that correlates to either turn on or off a general purpose output, or to turn on or off the high security mode. Other correlated events include different functions such as forced entry, auto relock or interlock.

4.7.5 Active state

An active state is when the input circuit is considered active and is configured as one of the following:

- open
- short (default)

There are some restrictions in configuring the active state depending on what kind of supervision is required.

If the input is not supervised the input is either ‘open’ or ‘closed’. If the input is supervised for ‘open’ the active state cannot be ‘open’.

If the input is supervised for both ‘open’ and ‘short’ the active state cannot be ‘open’.

4.7.6 Supervision requirement

Each input is configured for a specific type of supervision depending on your particular installation requirements as follows:

- no supervision
- supervise for open
- supervise for short
- supervise for both open and short

Note: Set the Circuit Supervision in the Configurator software to match the supervision type in your installation.

4.7.6.1 No Supervision

When inputs are configured with no supervision, the active state is either ‘open’ or ‘short’ as programmed.

4.7.6.2 Supervised for open

When configured as supervised for open, the active state is ‘closed’ (short). Open supervision uses a single 47K ohm resistor.

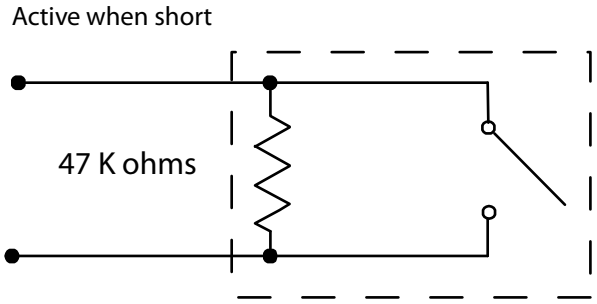


Figure 25. Input - supervised for open

Note: The active state cannot be an open state.

4.7.6.3 Supervised for short

When configured as supervised for short, the active state is open. A single 47K ohm resistor is required for short supervision.

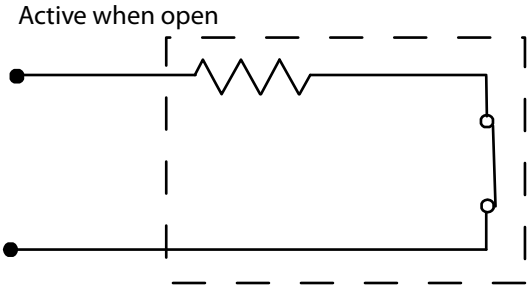


Figure 26. Input - supervised for short

Note: The active state cannot be a short state.

4.7.6.4 Supervise for open and short

When configured as supervise for both ‘open’ and ‘short’, the active state cannot be open, therefore the active state is closed.

Two 22K ohm resistors are required for supervision.

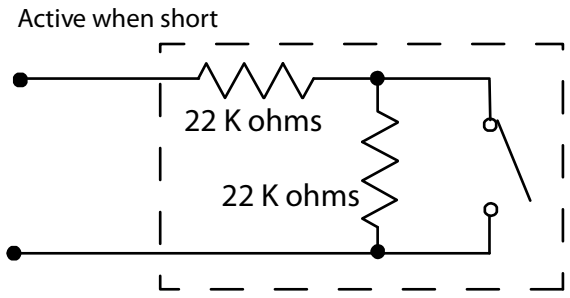


Figure 27. Input - supervised for open and short

Note: The active state cannot be an open state.

4.7.7 Alarm Delay

Alarm delay is a Configurator defined parameter that specifies the amount of time before an input raises an alarm condition. For more information see section 2 on page 13.

4.8 Outputs

There are 8 outputs located on the top right hand corner of the card access controller as shown in figure 11.

Each output is wired for a specific function or for an active state. Determine the functional requirements for the device and connect the outputs accordingly. For additional details and a complete description of the different types of configurable functions see section 2 on page 13.

After the installation and setup is complete, the functional state of all outputs must be configured using the Configurator software.

4.8.1 Specific functions

Each output is wired for the following specific functions:

- Lock for Reader A or B
- Handicap lock for Reader A or B
- General purpose output

Lock for reader A or B. This output assigns the main access door to either reader A or reader B. When access is granted at the designated reader, this output unlocks the door.

Handicap lock for reader A or B. This output controls the handicap access door. Access is granted to cards with handicap privileges.

General purpose output. The general purpose output is for all other types of outputs, such as turning on a light.

4.8.2 Active state

Outputs require active states. Each output is configured for the active state to indicate one of the following:

- energized
- de-energized

4.8.3 Outputs 1 to 6

Outputs 1 to 6 are relay contact programmable outputs with the following characteristics. Figure 28 shows a sample connection.

- normally open (NO)
- normally closed (NC) available
- 125 VAC, 2 A, 0.6 pf (dry contact)
  Or
- 30 VDC, 1 A, 0.6 pf (dry contact)

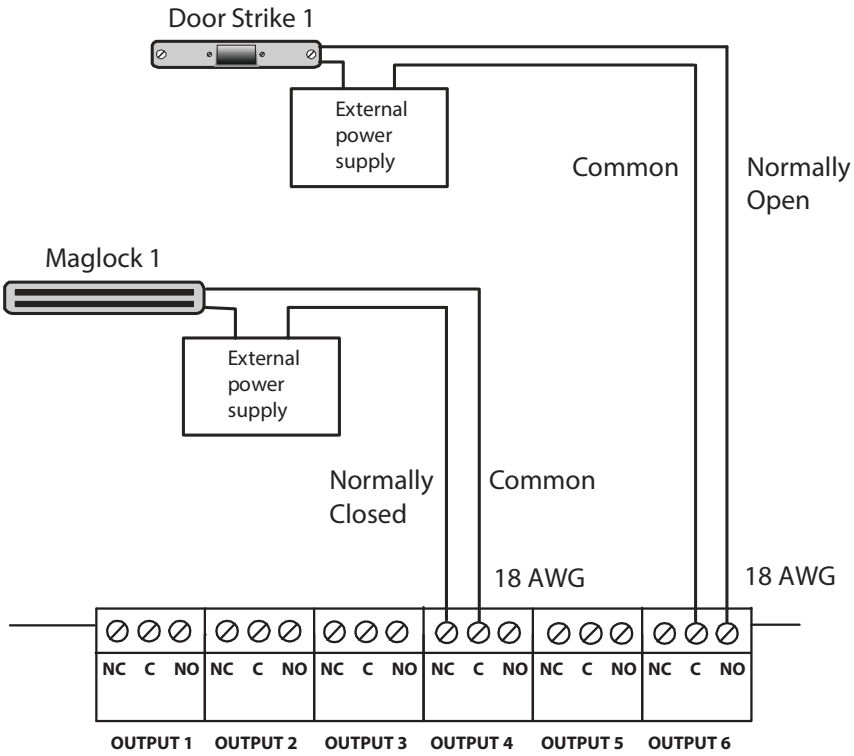


Figure 28. Controller output terminal sample connections

4.8.4 Outputs 7 and 8

Outputs 7 and 8 are programmable and provide a combined output of 1 A. Each individual output is capable of providing:

- 12 VDC / 700 mA maximum

Note: Outputs 7 and 8 are capable of providing a maximum output of 700 mA each, for a combined output of 1 A. For example, if output 7 provides 700 mA, then output 8 provides 300 mA.

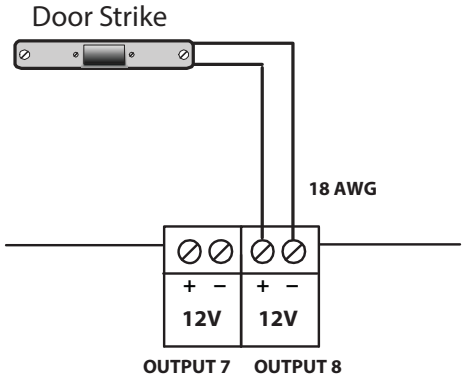


Figure 29. Outputs 7 and 8 sample connections

Figure 29 shows a door strike activated and powered by output 8.

4.9 Card Readers

The card readers are part of the Mircom Card Access package. The cards are produced by Mircom.The controller supports two card readers.

4.9.1 Card Reader Requirements

Mircom provides several multi protocol proximity card readers.

Third party card readers must meet the following minimum requirements in order to be compatible with Mircom's Card Access System:

- must support the 26 bit standard SIA protocol
- standard Wiegand interface
- LED status indicator
- warning or alarm buzzer
- 12 Volt operation
- maximum 500 feet distance from the card reader and the controller
- use 20 AWG wire for 500 feet and use 22 AWG for 250 feet

4.9.2 Card Reader Connection

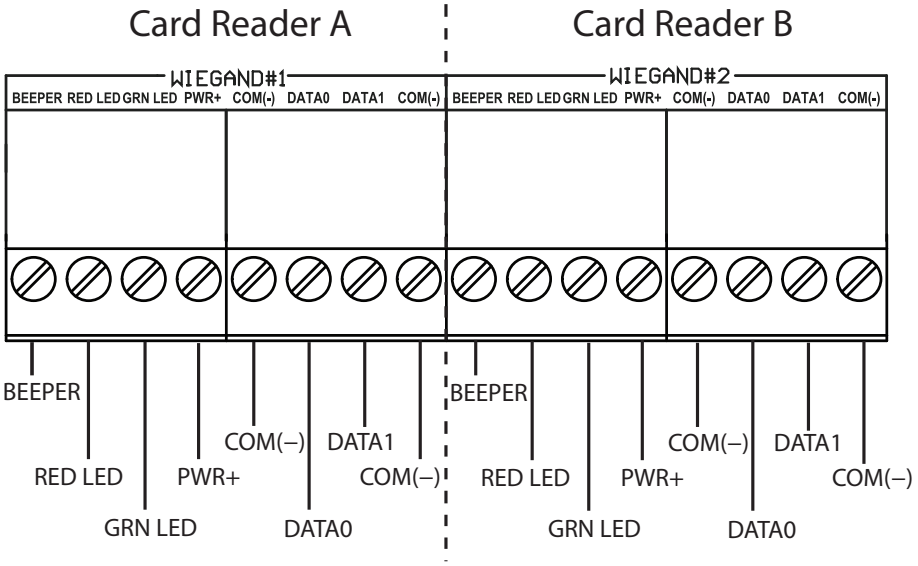


Figure 30. Controller board card reader connectors

Connect the readers to the terminals shown in figure 30.

Table 2: Connections for the TX3-P300-HA and TX3-P500-HA readers

Color	Terminal
Blue	BEEPER
Orange	RED LED
Brown	GRN LED
Red	PWR+
Green	DATA0
White	DATA1
Black	COM(−)

Card readers supplied by Mircom require a foil shielded multiple conductor stranded cable, at least 22 AWG. For example, use Belden 9535 or a similar cable.

The black wire can be connected to either COM (−) connector on the terminal block.

For other brands of card readers, follow the instructions in the manual for the card reader.

Note: Some card readers treat the green and red LED connections differently. You might need to switch the green and red LED connections for the LED to work properly. This note applies to both single line LED and dual line LED readers.

4.9.3 Card Reader Status LEDs

There are three status LEDs on the card reader:

Green LED. Illuminates steady green when door is unlocked.

Red LED. Illuminates steady red when door is locked.

Orange LED. Illuminates steady orange until a card is used for the first time. Normal illumination returns upon subsequent use. (*on some models only*)

4.9.4 Card Reader Beeper

The beeper indicates specific events at different beep rates as follows:

Card Presented. One short beep.

Access Granted. Two short beeps.

Access Denied. One short beep and one long beep.

Mode of Operation Changed. Three short beeps indicate a change in the on or off state for the high security or the unlock mode.

Alarm. Continuous short beeps.

4.10 Setting DIP Switches SW2

The DIP switches on SW2 are used to set the card access controller address on the RS-485 network and determine how the card access controller gets its IP address (on IP enabled controllers only). Valid addresses are 1 to 63. DIP switches 1 to 6 are used for binary addressing with DIP switch 1 being the least significant bit. DIP switch SW2 is found at the top central portion of the card access controller board, see figure 11.

See section 5 on page 59 for the DIP switch settings for RS-485 network addressing.

Note: DIP Switch 7 is not used and should remain at the default setting (OFF).

Note: DIP Switch 8 determines how the IP address is assigned to the IP Module for IP enabled card access controllers.

- **DIP Switch 8 OFF (default):** The IP address is assigned using a DHCP server. This is the factory default setting.
- **DIP Switch 8 ON:** The IP address is assigned using the Configurator software.

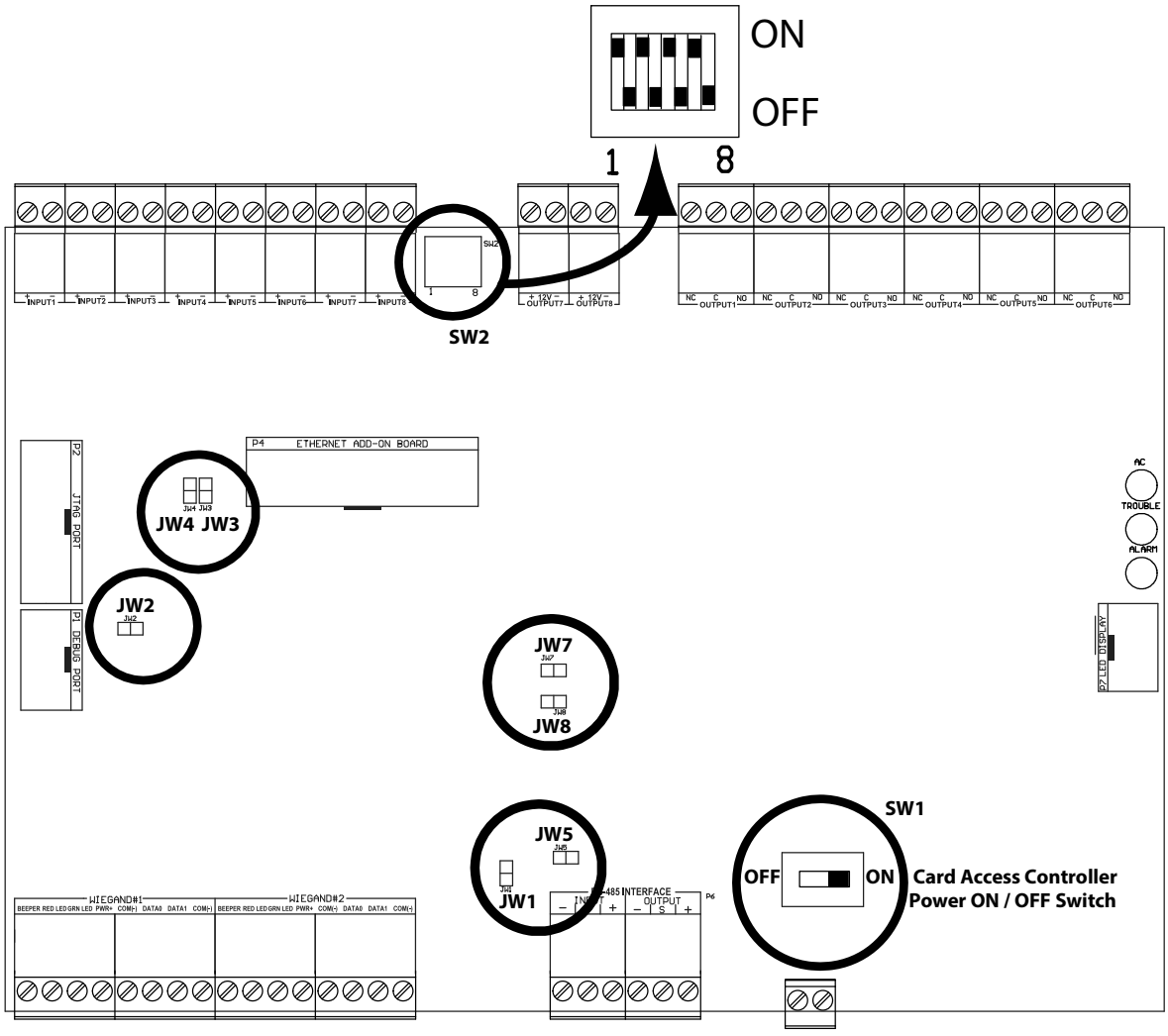


Figure 31. Location of jumpers JW1 to JW8 and switches SW1 and SW2

4.11 Setting Jumpers

There are seven pre-set jumpers on the controller board as follows (refer to figure 31):

JW1. JW1 is used for updating firmware and is always open by default.

JW2. JW2 is used for updating firmware and is open by default. See section 4.13 on page 56.

JW3 and JW4. JW3 and JW4 are not used and are open by default.

JW5. JW5 is open by default. Close JW5 on the first and last controllers instead of using end-of-line 120 Ω resistors for RS-485.

JW7 and JW8. If there are problems with RS-485 communication, close both JW7 and JW8 on either the first or last controller connected by RS-485. By default, JW7 and JW8 are open.

4.12 Turning on the Controller

Before you turn on the controller ensure that the all connections adhere with the correct operation of the devices. For example, a magnetic lock requires power in the default state.

Once the controller is turned on, you must begin the configuration. For detailed information on how to configure the controller see LT-995 Configuration and Administration Guide.

4.12.1 Default Configuration Values

Once the controller is on, it operates according to its preset default configuration values. When the Configurator software first starts, it uses the default values and adopts these values as its initial settings.

The default configuration values are adopted only when the following situations occur:

- turning the system on for the first time
- memory corruption
- program upgrade

4.13 Updating Firmware

You can update the firmware on your panel with the TX3 Configurator software by using one of the following methods.

- Firmware Upgrade Wizard
- Network Firmware Upgrade

The Firmware Upgrade Wizard can be used to update only one panel at a time. It will work on any panel.

The Network Firmware Upgrade procedure can update more than one panel at the same time. In order to use the Network Firmware Upgrade, all of the panels must already have firmware that supports this feature installed on them.

Refer to LT-995, TX3 Configuration and Administrator Manual, for instructions on how to perform both of these firmware upgrade methods. LT-995 can be found on the TX3 Configurator Software installation CD, the USB flash drive, or on the Mircom website.

4.13.1 Firmware Version Control

The firmware version number is accessible from the Configurator software and changes whenever there is a major, minor or revision update.

The following convention is used whenever there is a major, minor or revision change:

Initial release. Version 1.00.0

Major change. Version 2.00.0

Minor change. Version 2.01.0

Revision changes. Version 2.01.1

4.14 Beginning Configuration

The card access controller is now configurable using the following connections.

- USB connection
- Ethernet connection
- COM port connection
- Modem connection

For a complete description of the configuration and on how establish a connection to the card access controller using a USB, Ethernet, COM port or modem connection, see the following documentation:

- LT-995 Configuration and Administration Guide
- LT-973 TX3 Configurator Quick Start

Verify the following:

- Ensure that the controller and all connected devices and components are fully operational.
- Ensure the controller DIP Switches (SW2) are set with a unique network address.
- Ensure the Configurator software is set with the correct controller network address.
- Ensure that your PC and the Configurator are set with the correct date and time.

To start the configuration

1. Connect the PC to the controller using the USB port.
2. Launch the Configurator and click `Connect`. Once connected the connection icon appears in the Configurator tool bar.
3. Configure the Card Access System using the instructions in the Configurator Software Program or the LT-995 Configuration and Administration Guide.

5 RS-485 Addresses

Table 3: SW2 DIP Switch Settings for RS-485 Network Addressing

ADDRESS	SWITCH 1	SWITCH 2	SWITCH 3	SWITCH 4	SWITCH 5	SWITCH 6
1	ON	OFF	OFF	OFF	OFF	OFF
2	OFF	ON	OFF	OFF	OFF	OFF
3	ON	ON	OFF	OFF	OFF	OFF
4	OFF	OFF	ON	OFF	OFF	OFF
5	ON	OFF	ON	OFF	OFF	OFF
6	OFF	ON	ON	OFF	OFF	OFF
7	ON	ON	ON	OFF	OFF	OFF
8	OFF	OFF	OFF	ON	OFF	OFF
9	ON	OFF	OFF	ON	OFF	OFF
10	OFF	ON	OFF	ON	OFF	OFF
11	ON	ON	OFF	ON	OFF	OFF
12	OFF	OFF	ON	ON	OFF	OFF
13	ON	OFF	ON	ON	OFF	OFF
14	OFF	ON	ON	ON	OFF	OFF
15	ON	ON	ON	ON	OFF	OFF
16	OFF	OFF	OFF	OFF	ON	OFF
17	ON	OFF	OFF	OFF	ON	OFF
18	OFF	ON	OFF	OFF	ON	OFF
19	ON	ON	OFF	OFF	ON	OFF
20	OFF	OFF	ON	OFF	ON	OFF
21	ON	OFF	ON	OFF	ON	OFF
22	OFF	ON	ON	OFF	ON	OFF
23	ON	ON	ON	OFF	ON	OFF
24	OFF	OFF	OFF	ON	ON	OFF
25	ON	OFF	OFF	ON	ON	OFF
26	OFF	ON	OFF	ON	ON	OFF

Table 3: SW2 DIP Switch Settings for RS-485 Network Addressing (Continued)

ADDRESS	SWITCH 1	SWITCH 2	SWITCH 3	SWITCH 4	SWITCH 5	SWITCH 6
27	ON	ON	OFF	ON	ON	OFF
28	OFF	OFF	ON	ON	ON	OFF
29	ON	OFF	ON	ON	ON	OFF
30	OFF	ON	ON	ON	ON	OFF
31	ON	ON	ON	ON	ON	OFF
32	OFF	OFF	OFF	OFF	OFF	ON
33	ON	OFF	OFF	OFF	OFF	ON
34	OFF	ON	OFF	OFF	OFF	ON
35	ON	ON	OFF	OFF	OFF	ON
36	OFF	OFF	ON	OFF	OFF	ON
37	ON	OFF	ON	OFF	OFF	ON
38	OFF	ON	ON	OFF	OFF	ON
39	ON	ON	ON	OFF	OFF	ON
40	OFF	OFF	OFF	ON	OFF	ON
41	ON	OFF	OFF	ON	OFF	ON
42	OFF	ON	OFF	ON	OFF	ON
43	ON	ON	OFF	ON	OFF	ON
44	OFF	OFF	ON	ON	OFF	ON
45	ON	OFF	ON	ON	OFF	ON
46	OFF	ON	ON	ON	OFF	ON
47	ON	ON	ON	ON	OFF	ON
48	OFF	OFF	OFF	OFF	ON	ON
49	ON	OFF	OFF	OFF	ON	ON
50	OFF	ON	OFF	OFF	ON	ON
51	ON	ON	OFF	OFF	ON	ON
52	OFF	OFF	ON	OFF	ON	ON
53	ON	OFF	ON	OFF	ON	ON
54	OFF	ON	ON	OFF	ON	ON
55	ON	ON	ON	OFF	ON	ON
56	OFF	OFF	OFF	ON	ON	ON

Table 3: SW2 DIP Switch Settings for RS-485 Network Addressing (Continued)

ADDRESS	SWITCH 1	SWITCH 2	SWITCH 3	SWITCH 4	SWITCH 5	SWITCH 6
57	ON	OFF	OFF	ON	ON	ON
58	OFF	ON	OFF	ON	ON	ON
59	ON	ON	OFF	ON	ON	ON
60	OFF	OFF	ON	ON	ON	ON
61	ON	OFF	ON	ON	ON	ON
62	OFF	ON	ON	ON	ON	ON
63	ON	ON	ON	ON	ON	ON

6 TX3-CX-2-A Power Supply and Battery Calculations

Use the forms below to determine the required secondary power supply (batteries).

Enter values in the shaded areas.

Table 4: Standby Current

Model	Number		Standby	Total Standby (amperes)
TX3-CX-2	1	X	0.5	= 0.5
Output 7	*	X	(A) **	=
Output 8	*	X	(B) **	=
			Total standby current (add above currents)	= **(C)**

* Enter **1** if a maglock is used, otherwise enter **0**.

** Enter the current draws for output 7 and output 8. Consult the device manufacturer's specifications for this information.

The total current from output 7 and output 8 should not exceed 1 A.

6.1 Total Door Open Time Per Hour

Enter values in the shaded areas.

Table 5: Total Door Open Time Per Hour

Door open timer (seconds)		Approximate number of times the door is unlocked per hour		Total door open time per hour (hours)
	X		/3600	= **(D)**

6.2 Total Current for Door Lock

Enter values in the shaded areas.

Table 6: Total Current for Door Lock

Total door open time per hour (from Table 5)		Number of hours the panel must run on batteries		Standby for outputs 7 and 8 (from Table 4)	Total current for door lock (Ah)
(D)	X		X	**(A + B)**	= **(E)**

6.3 Battery Capacity Requirement

Enter values in the shaded areas.

Table 7: Battery Capacity Requirements

Total standby current (from Table 4)		Number of hours the panel must run on batteries (this must be the same value as in Table 6)		Total current for door lock (from Table 6)	Battery capacity requirement (Ah)
(C)	X		+	**(E)**	= **(F)**

6.4 Battery Selection

Enter values in the shaded areas.

Table 8: Battery Selection

Battery capacity requirement (from Table 7)			The Ah rating of the battery required
(F)	X	**1.2**	= _____ Ah

7 Specifications

Standards						
UL 294 7th Edition						
UL 294, 7th Ed. Access Control Performance Levels						
	TX3-CX-2	**TX3-CX-4**	**TX3-CX-6**	**TX3-CX-8**	**TX3-USB-AD**	**TX3-IP**
Access Control Line Security	I	I	I	I	I	I
Destructive Attack	I	I	I	I	I	I
Endurance	IV	IV	IV	IV	IV	IV
Standby Power	IV	IV	IV	IV	IV	IV

Primary Operating Supply

- Manufactured by Yeo Heung Electronics Co. Ltd., Model No. SEP/P-1640U (includes outlet mounting tab - one required for each card access controller board, if used for primary operating supply). Primary rated 120 VAC, 60 Hz, 0.48 A, Secondary rated 16.5 VAC, 40 VA, UL Listed Class 2.
- UL 294 Listed power supply

NOTE: The TX3-PS24-5A power supply is not evaluated to UL 294 and is not permitted for use in UL 294 applications.

Secondary Operating Supply

12 VDC, 7 Ah sealed lead-acid rechargeable battery (provides 4 h battery standby time - one required for each card access controller board)

Electrical Ratings
TX3-CX-2 • 16.5 VAC, 0.5 A (no load), 2.2 A (full load) **TX3-CX-4** • 16.5 VAC, 1 A (no load), 4.4 A (full load) **TX3-CX-6** • 16.5 VAC, 1.5 A (no load), 6.6 A (full load) **TX3-CX-8** • 16.5 VAC,2 A (no load), 8.8 A (full load) **TX3-USB-AD (optional)** • Powered by the card access controller through the interface connection P3, rated 5 V, 60 mA. **TX3-IP (optional)** • Powered by the card access controller through the interface connection P4, rated 3.3 V, 120 mA.
Connections
• 1 USB port for configuration • 1 RS-485 port • 2 Wiegand connections: 12 VDC regulated voltage output, 100 mA each (200 mA total max.) • 8 programmable inputs • Outputs 1-6 are rated at: 125 VAC, 2 A, 0.6 pf (dry contact) Or 30 VDC, 1 A, 0.6 pf (dry contact) • Outputs 7-8 are programmable and provide a combined output of 1 A. Each individual output is capable of providing: 12 VDC / 700 mA maximum For example, if output 7 provides 700 mA, then output 8 provides 300 mA.
Operating Temperature
0°C (32°F) to 49°C (120°F) up to 93% relative humidity Indoor use only

Warranty & Warning Information

WARNING!

Please read this document **CAREFULLY**, as it contains important warnings, life-safety, and practical information about all products manufactured by the Mircom Group of Companies, including Mircom and Secutron branded products, which shall include without limitation all fire alarm, nurse call, building automation and access control and card access products (hereinafter individually or collectively, as applicable, referred to as "**Mircom System**").

NOTE TO ALL READERS:

1. **Nature of Warnings.** The within warnings are communicated to the reader out of an abundance of caution and create no legal obligation for Mircom Group of Companies, whatsoever. Without limiting the generality of the foregoing, this document shall NOT be construed as in any way altering the rights and obligations of the parties, governed by the legal documents that apply in any given circumstance.

2. **Application.** The warnings contained in this document apply to all Mircom System and shall be read in conjunction with:

   a. the product manual for the specific Mircom System that applies in given circumstances;

   b. legal documents that apply to the purchase and sale of a Mircom System, which may include the company's standard terms and conditions and warranty statements;

   c. other information about the Mircom System or the parties' rights and obligations as may be application to a given circumstance.

3. **Security and Insurance.** Regardless of its capabilities, no Mircom System is a substitute for property or life insurance. Nor is the system a substitute for property owners, renters, or other occupants to act prudently to prevent or minimize the harmful effects of an emergency situation. Building automation systems produced by the Mircom Group of Companies are not to be used as a fire, alarm, or life-safety system.

NOTE TO INSTALLERS:

All Mircom Systems have been carefully designed to be as effective as possible. However, there are circumstances where they may not provide protection. Some reasons for system failure include the following. As the only individual in contact with system users, please bring each item in this warning to the attention

of the users of this Mircom System. Failure to properly inform system end-users of the circumstances in which the system might fail may result in over-reliance upon the system. As a result, it is imperative that you properly inform each customer for whom you install the system of the possible forms of failure:

4. **Inadequate Installation.** All Mircom Systems must be installed in accordance with all the applicable codes and standards in order to provide adequate protection. National standards require an inspection and approval to be conducted by the local authority having jurisdiction following the initial installation of the system and following any changes to the system. Such inspections ensure installation has been carried out properly.

5. **Inadequate Testing.** Most problems that would prevent an alarm a Mircom System from operating as intended can be discovered by regular testing and maintenance. The complete system should be tested by the local authority having jurisdiction immediately after a fire, storm, earthquake, accident, or any kind of construction activity inside or outside the premises. The testing should include all sensing devices, keypads, consoles, alarm indicating devices and any other operational devices that are part of the system.

NOTE TO USERS:

All Mircom Systems have been carefully designed to be as effective as possible. However, there are circumstances where they may not provide protection. Some reasons for system failure include the following. The end user can minimize the occurrence of any of the following by proper training, testing and maintenance of the Mircom Systems:

6. **Inadequate Testing and Maintenance.** It is imperative that the systems be periodically tested and subjected to preventative maintenance. Best practices and local authority having jurisdiction determine the frequency and type of testing that is required at a minimum. Mircom System may not function properly, and the occurrence of other system failures identified below may not be minimized, if the periodic testing and maintenance of Mircom Systems is not completed with diligence and as required.

7. **Improper Operation.** It is important that all system users be trained in the correct operation of the alarm system and that they know how to respond when the system indicates an alarm. A Mircom System may not function as intended during an emergency situation where the user is unable to operate a panic or emergency switch by reason of permanent or temporary physical disability, inability to reach the device in time, unfamiliarity with the correct operation, or related circumstances.

8. **Insufficient Time.** There may be circumstances when a Mircom System will operate as intended, yet the occupants will not be protected from the emergency due to their inability to respond to the warnings in a timely manner. If the system is monitored, the response may not occur in time enough to protect the occupants or their belongings.

9. **Carelessness or Safety Hazards.** Moreover, smoke detectors may not provide timely warning of fires caused by carelessness or safety hazards such as smoking in bed, violent explosions, escaping gas, improper storage of flammable materials, overloaded electrical circuits or children playing with matches or arson.

10. **Power Failure.** Some Mircom System components require adequate electrical power supply to operate. Examples include: smoke detectors, beacons, HVAC, and lighting controllers. If a device operates only by AC power, any interruption, however brief, will render that device inoperative while it does not have power. Power interruptions of any length are often accompanied by voltage fluctuations which may damage Mircom Systems or other electronic equipment. After a power interruption has occurred, immediately conduct a complete system test to ensure that the system operates as intended.

11. **Battery Failure.** If the Mircom System or any device connected to the system operates from batteries it is possible for the batteries to fail. Even if the batteries have not failed, they must be fully charged, in good condition, and installed correctly. Some Mircom Systems use replaceable batteries, which have a limited life-span. The expected battery life is variable and in part dependent on the device environment, usage and type. Ambient conditions such as high humidity, high or low temperatures, or large temperature fluctuations may reduce the expected battery life. Moreover, some Mircom Systems do not have a battery monitor that would alert the user in the event that the battery is nearing its end of life. Regular testing and replacements are vital for ensuring that the batteries function as expected, whether or not a device has a low-battery monitor.

12. **Physical Obstructions.** Motion sensors that are part of a Mircom System must be kept clear of any obstacles which impede the sensors' ability to detect movement. Signals being communicated by a Mircom System may not reach the receiver if an item (such as metal, water, or concrete) is placed on or near the radio path. Deliberate jamming or other inadvertent radio signal interference can also negatively affect system operation.

13. **Wireless Devices Placement Proximity.** Moreover all wireless devices must be a minimum and maximum distance away from large metal objects, such as refrigerators. You are required to consult the specific Mircom System manual and application guide for any maximum distances required between devices and suggested placement of wireless devices for optimal functioning.

14. **Failure to Trigger Sensors.** Moreover, Mircom Systems may fail to operate as intended if motion, heat, or smoke sensors are not triggered.

a. Sensors in a fire system may fail to be triggered when the fire is in a chimney, walls, roof, or on the other side of closed doors. Smoke and heat detectors may not detect smoke or heat from fires on another level of the residence or building. In this situation the control panel may not alert occupants of a fire.

b. Sensors in a nurse call system may fail to be triggered when movement is occurring outside of the motion sensors' range. For example, if movement is occurring on the other side of closed doors or on another level of the residence or building the motion detector may not be triggered. In this situation the central controller may not register an alarm signal.

15. **Interference with Audible Notification Appliances.** Audible notification appliances may be interfered with by other noise sources such as stereos, radios, televisions, air conditioners, appliances, or passing traffic. Audible notification appliances, however loud, may not be heard by a hearing-impaired person.

16. **Other Impairments.** Alarm notification appliances such as sirens, bells, horns, or strobes may not warn or waken a sleeping occupant if there is an intervening wall or door. It is less likely that the occupants will be alerted or awakened when notification appliances are located on a different level of the residence or premise.

17. **Software Malfunction.** Most Mircom Systems contain software. No warranties are provided as to the software components of any products or stand-alone software products within a Mircom System. For a full statement of the warranties and exclusions and limitations of liability please refer to the company's standard Terms and Conditions and Warranties.

18. **Telephone Lines Malfunction.** Telephone service can cause system failure where telephone lines are relied upon by a Mircom System. Alarms and information coming from a Mircom System may not be transmitted if a phone line is out of service or busy for a certain period of time. Alarms and information may not be transmitted where telephone lines have been compromised by criminal tampering, local construction, storms or earthquakes.

19. **Component Failure.** Although every effort has been made to make this Mircom System as reliable as possible, the system may fail to function as intended due to the failure of a component.

20. **Integrated Products.** Mircom System might not function as intended if it is connected to a non-Mircom product or to a Mircom product that is deemed non-compatible with a particular Mircom System. A list of compatible products can be requested and obtained.

Warranty

Purchase of all Mircom products is governed by:

https://www.mircom.com/product-warranty

https://www.mircom.com/purchase-terms-and-conditions

https://www.mircom.com/software-license-terms-and-conditions

Special Notices

Product Model Number: TX3

Complies With

Federal Communications Commission (FCC):

- CFR 47, Part 15, Subpart B, Class B
- Unintentional Radiators

Industry Canada (IC):

- ICES-003, ISSUE 4, CLASS B
- Verification Authorization - Digital Apparatus

Registration Numbers

FCC (U.S.): 1M8TE00BTX3

IC (Canada): 1156A-TX3