PTI SECURITY SYSTEMS

APEX Access Device

Installation and Operation Manual

www.ptisecurity.com *800.331.6224*

S E C U R I T Y , A C C E S S : C O N T R O L

Revised May 2012

ETL LISTED

Thank you for purchasing the APEX Access Device. While every effort has been made to ensure the accuracy of the information in this document, PTI Security Systems assumes no liability for any inaccuracies contained herein. We reserve the right to change the information contained herein at any time and without notice.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio TV technician for help.

This Class B digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

© 2012 PTI Security Systems

All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, or translated into any language in any form, by any means, without written permission of PTI Security Systems.

This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instruction manual, may cause interference to radio communications. It has been tested and found to comply with the limits for a Class A computing device pursuant to Subpart J of Part 15 of FCC rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference in which case the user, at his/her own expense, will be required to take whatever measures may be required to correct the interference.

With the RS485 communication scheme, a keypad can be located as far as 4000 feet from the controller, which is why shielded twisted pair cable with ground wire is required for optimal operation. Voltage drop across long lengths of wire must also be considered. The farther the device is from the controller, the larger the gauge of wire that must be used. Refer to the Voltage Drop Calculation QuickDoc for more information. This document is available on our web site at *www.ptiaccess.com/downloads*.

THE SYSTEM WILL NOT OPERATE PROPERLY IF THE VOLTAGE IS BELOW 12VDC. Extreme care should be taken when choosing a power supply voltage and current rating. Long distance runs may require a remote power supply to be installed in line with an RB5 relay to ensure proper operation.

CONTENTS

TECHNICAL SPECIFICATIONS

Power Supply:

Voltage:	12 – 24VDC or 12 – 18VAC
Current Consumption:	300mA Maximum

Relay Outputs (resistive load):

Maximum Switching Voltage:	30VAC/DC
Maximum Switching Current:	AC: 10A (NO) / 3A (NC)
	DC: 5A (NO) / 3A (NC)
Maximum Switching Capacity:	1250VA (NO)
	375VA (NC)
Minimum Permissible Load:	10mA at 5VDC
Contact Resistance:	100 mΩ Maximum
Life Expectancy:	
Mechanical:	10,000,000 operations
Electrical:	200,000 operations minimum
	(at maximum rated load)

Inputs:

Dry Contact Type ONLY.

Do NOT apply voltage to any of the inputs.

Dry Contact Specifications:

Contact Resistance:	500 mΩ Maximum
Current Capacity:	100mA at 5VDC Minimum

Environmental:

Ambient Temperature:	-40°C to +80°C (-40°F to 176°F)
Ambient Humidity:	0% to 100% (see note)

Note: The humidity inside the housing for any APEX device cannot exceed 100% and must be noncondensing.

INSTALLATION

Mounting Options

The APEX Access Device controls entry to or exit from a secured area. It works in conjunction with a controller and control software. The APEX can be used to control gate access, building access, room access, elevator access, etc. It is designed for ease of use and flexibility. Both the keypad and the large LCD are backlit for easy visibility day and night. Mounting height for devices will vary with local code regarding handicap access, emergency and fire access, and other regulations.

Before installing the APEX, determine where and how the device will be installed as the mounting location will be determined by how the device is to be used. If it is to be used for drive up access, it must be installed where it can be accessed from a vehicle's driver door. If it is to be used for walk up access, it must be installed where it is easily accessible to a person on foot.

Drive Up Accessibility

When the APEX will be positioned for drive up accessibility, the device must be mounted within easy reach of the driver of an automobile or light truck. Most such applications use gooseneck stands that are located on an island between the entry and exit gates, or to the left side of the gate if a single gate is used. Local building codes may set a minimum and maximum height for devices that are accessible by vehicle. Figure 1 shows possible mounting locations when used for vehicle access.

Walk Up Accessibility

When the APEX is used for walk up access, it can be mounted on a stand or attached to a wall. It can be surface mounted so that it protrudes from the wall or it can be flush mounted using the optional flush mounting kit.

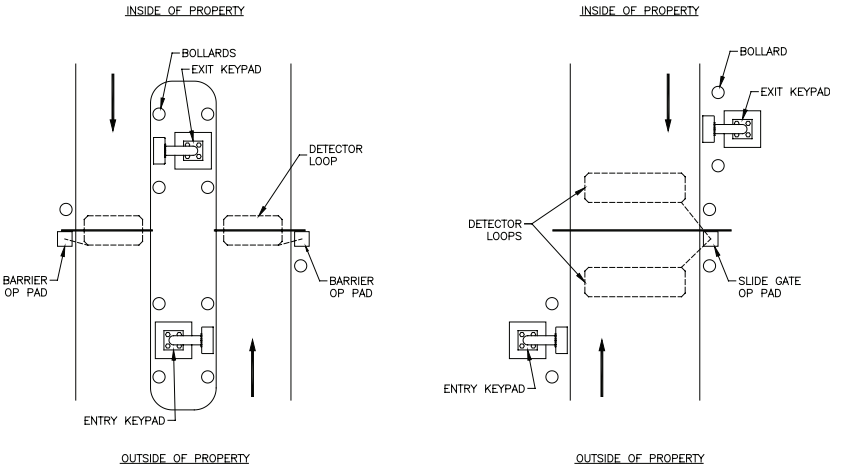


Figure 1

ADA Guidelines for Access Control

The Americans with Disabilities Act of 1990 (ADA) prohibits discrimination in and ensures equal access to employment, government services, public accommodations, transportation, and commercial facilities for persons with disabilities. Some of the guidelines and requirements from this law can be applied to access control. Because many local municipalities have much stricter standards than the ADA, we strongly recommend that owners, builders, and installers consult a qualified expert in local, state, and federal interpretations of ADA and similar laws. For more information about the ADA, visit the ADA web site at *www.ada.gov* or the Department of Justice ADA web site at *www.usdoj.gov/crt/ada/* or call the ADA Information Line at (800) 514-0301. Many communities have adopted the Americans with Disabilities Act (ADA) as the standard for locating devices that the general public will use.

Recommendations for Sites

The ADA and other similar laws are open to some degree of interpretation by local authorities and courts. It is in your best interest to familiarize yourself with the complete requirements for ADA and other similar local laws. Most important, however, is to work to provide reasonable access to your services by persons of all abilities. Below are some recommendations that may help.

- Contact a local inspector or architect who can provide assistance in designing the access to your facility with respect to ADA and other similar laws
- Visit the ADA web site or call the information line listed above
- Provide adequate, well-lit signs (written, picture, and Braille)
- Design hallways with adequate room for wheelchairs
- Provide adequate access to all keypads, access devices, and elevator controls as provided for in ADA
- Use keypads with proximity cards or key fobs and audible signals to provide greater access flexibility

ADA Mounting Requirements

1. Keypads should be mounted so that the top of the number touchpad is no more than 48 inches above the finished floor with no obstructions in locations where wheelchair access is available only from the front. Keypads can be placed higher if a wall mount gooseneck allows closer access to the keypad.

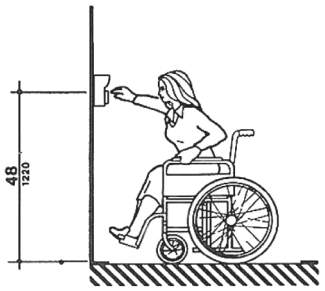


Figure 2a

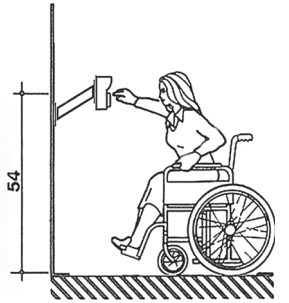


Figure 2b

2. Keypads should be mounted so that the top of the number touchpad is no more than 54 inches above the finished floor with no obstructions in locations where the wheelchair has sideways access.

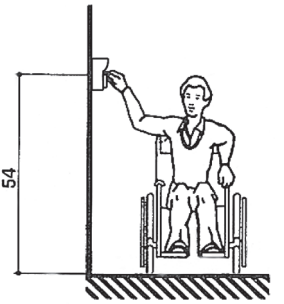


Figure 3

3. Keypads should be mounted so as not to protrude more than 4 inches from the wall. If mounted in a bollard or pylon, it may protrude up to 12 inches. Items mounted higher on the wall or ceiling must be 80 inches or higher above the finished floor.

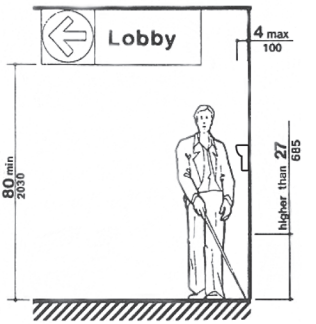


Figure 4

4. Computer keyboards and other office equipment should be placed on desks between 28” – 34” tall with no more than 20 inches in reach depth for obstructed front access or 24 inches in reach depth for obstructed side reach access. In the first figure below, if X < 20” then Y = 48”. When X = 20” – 25”, then Y = 44”. X should always be ≤ 25”.

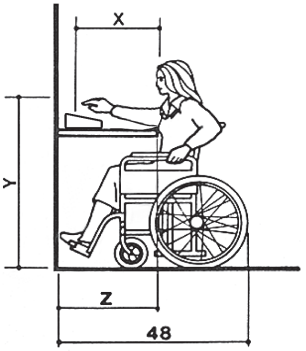


Figure 5a

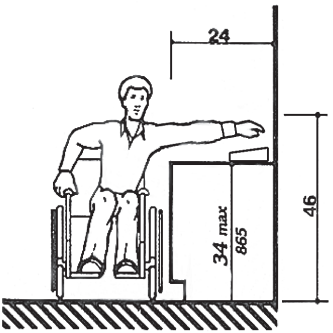


Figure 5b

All information contained herein is from the ADA web site and the Department of Justice Code of Federal Regulations Excerpt CFR Part 36 ADA Standards for Accessible Design revised July 1, 1994. PTI Security Systems is not liable for the information contained in this document and we strongly recommend that installers, owners, and builders work with qualified experts in the local, state, and federal interpretations of ADA and other similar laws. Refer to the ADA Standards for Accessible Design and Federal regulations for more specific information and requirements.

Mounting Access Devices

The proper mounting height for the APEX varies with the application. There are several options for mounting access devices: surface mount, flush mount, box mount, and wall mount. These can be attached to a wall or installed at an entrance using a gooseneck or bollard.

Once it has been determined where to install the keypad, the location and purpose of the device should be noted on a site security wiring plan that is kept in a safe location for future maintenance and service purposes.

Surface Mount

Surface mounting of keypads is generally used in conjunction with door strikes and elevators. Mounting height is generally 48” – 58” from the finished floor to the center of the ‘5’ button on the touchpad. The actual location of the wall-mounted APEX may be affected by local building codes.

The type of fasteners required will depend on the material used to construct the wall. If the APEX is installed on an exterior wall, make sure the contact point between the housing and the wall is sealed with some form of silicone sealant rated for outdoor use to prevent moisture and insects from getting into the housing.

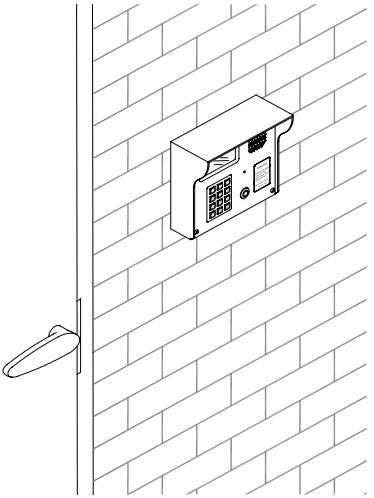


Figure 6

Flush Mount

A flush mount box allows the keypad to be set into hollow walls and is generally used in interior installations. The flush mount box must be ordered separately. Mounting height is generally 48” – 58” from the finished floor to the center of the ‘5’ button on the touchpad. If the flush mount kit must be used outdoors, a gasket is required for the face plate. Refer to Figure 8 for the mounting details of the flush mount adapter. The actual placement of the APEX device and the wiring methods to it may be affected by local building codes.

An elevator flush mount is available that is made of brushed stainless steel for mounting inside elevator cars. This model does not include an intercom.

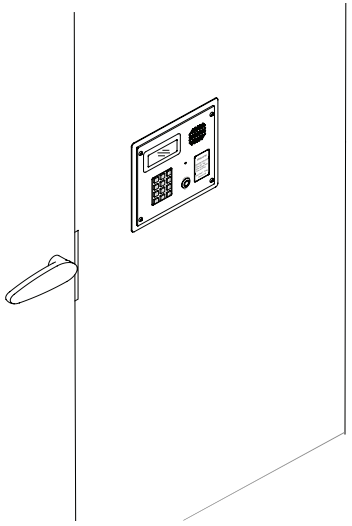


Figure 7

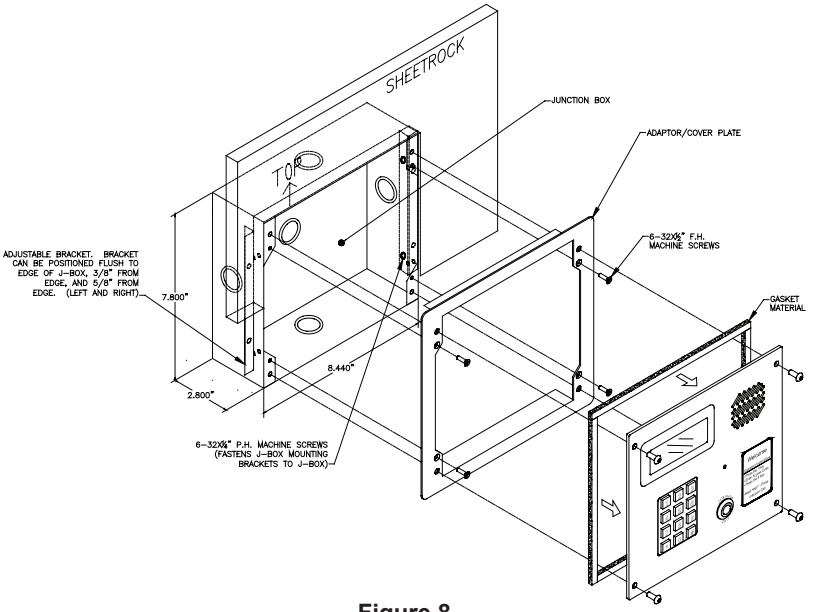


Figure 8

Box Mount

A box mount with no shaded overhang can be ordered for locations that require the keypad to be mounted lower than standard height, such as for handicap access. With a normal APEX mount, a standing person may not be able to see the display. The box mount must be ordered separately. Mounting height varies from 42” – 58” from the finished floor to the center of the ‘5’ button on the touchpad.

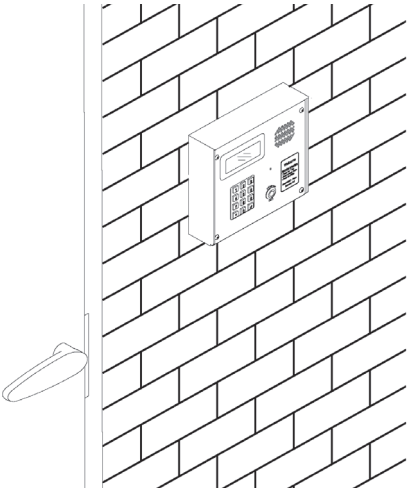


Figure 9

NOTE: Most standard keypad installations will place the ‘5’ button on the touchpad at approximately 50 inches from the finished floor for walk up keypads and 45 inches from the finished driveway for standard vehicle access.

Gooseneck Stand Mount

A gooseneck is commonly used for driveways for vehicle access. These stands are designed at the standard height of 42” (at the center of the APEX) for mounting on concrete pads at the driver side of the site entry or exit area. It can also be used near doors for wheelchair access or when sidewalks and landscaping require a freestanding keypad mount away from the building.

The base plate is equipped with a hole that will accept conduit (¾” maximum) for the electrical wiring to the APEX device. Ensure the conduit is placed properly and the wiring is run through the conduit before mounting the gooseneck stand to the concrete base. The actual location of the gooseneck and the mounting techniques may be affected by local building codes. Generally, the keypad should be protected with concrete bollards that prevent vehicles from hitting the keypad.

There are several different styles of gooseneck stands available. Refer to Figure 10 for the dimensions of two common styles.

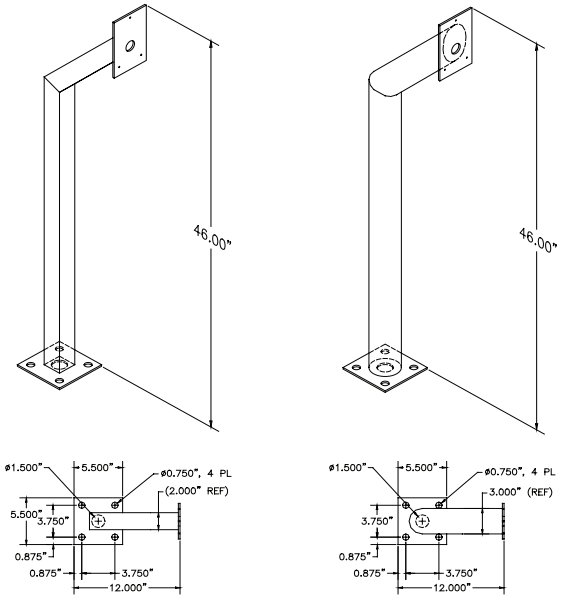


Figure 10

NOTE: Both single and double bollards are mounted on a Schedule 40 10 3/4” diameter pipe with a .365” wall. This pipe is footed in concrete and filled 3/4 of the way with concrete to create a solid barrier. The entire pipe and bollard are then painted to match the facility. Contact PTI Security Systems for full measured installation plans and instructions.

Wall Mount Gooseneck

A wall mount gooseneck allows the keypad to be mounted on a wall. It may be used for door strikes or for gates in driveways that run next to a building wall. A gooseneck can also be used to assist with wheelchair access to a device. Mounting height is generally 48” – 58” from finished floor to the ‘5’ button on the touchpad for walk up access and 45 inches from driveway level to the ‘5’ button on the touchpad for vehicular access.

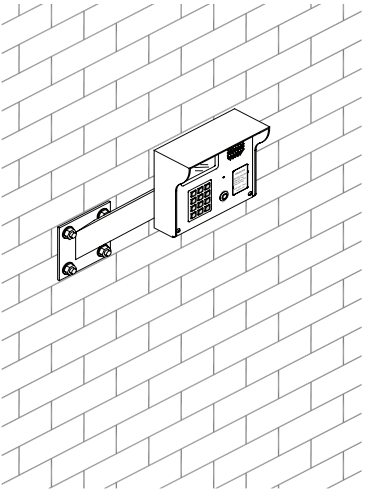


Figure 11

Keypad Adapter Plate

A keypad adapter plate is an aluminum plate used to mount keypads to stands, bollards, and goosenecks manufactured by other companies. The installer will measure, mark, and drill holes in the adapter plate to match the stand they are using. The holes should be countersunk on the same side as the installed screws so that the keypad will cover the mounting screws to prevent tampering. The screws and screwholes that are provided on the aluminum plate match up with the APEX keyhole mounting pattern.

Single Bollard

A bollard is used as an attractive and functional stand for keypads. It helps protect the keypad from being struck by vehicles. It can be used in driveways for vehicle access or near doors as a decorative keypad stand. It can be painted any color to compliment the site. Mounting height is determined by the height of the pipe on which it is mounted.

Double Bollard

Similar in design to the single bollard, the double bollard is taller and has a second mounting point above the first to allow both cars and RVs to enter through the same gate without requiring drivers to get out of the vehicle to use the keypad. This design can also be used to mount a Knox Box for fire safety.

Bollards can also be filled with concrete and used as barriers to protect keypads, walls, or gates.

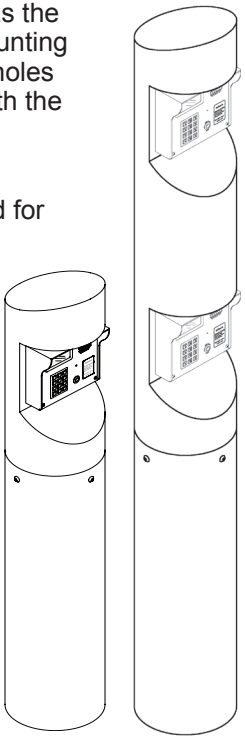


Figure 12a and 12b

Installing APEX Access Devices

Power and data communication wiring is the most important wiring component for APEX devices. The APEX requires power and communication lines to be supplied from the controller. We recommend that power and data communication be run through a single 18 AWG 4-conductor shielded cable as this cable works well in most cases. Some installations require larger gauge wire. See Figure 13 for details on connecting the wiring from the controller to the APEX.

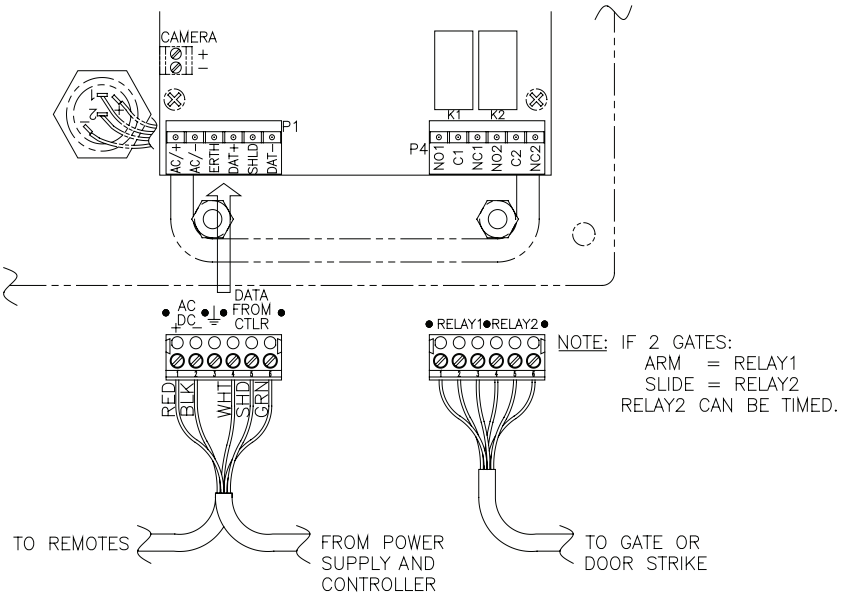


Figure 13

In addition to the power and communication cable, cables may also be needed for the intercom, gate operator, door strike, presence detector, or other device. Never install any other devices in the same run of wire as the APEX. Use a different cable for each device. Most communities require the wiring to be supplied to the APEX through approved electrical conduit. Local building codes determine the actual installation techniques and wiring methods. Only licensed contractors should install APEX devices.

The installation methods used are critical to trouble-free operation of the keypad. Most of the problems that surface over time can be traced back to poor installation techniques or improper wiring.

NOTE: All installations must conform to local building and electrical codes. When discrepancies exist between local codes and this manual, local code takes precedence.

Following are instructions on installing an APEX series keypad and connecting the wiring run from the system controller:

1. Open the device by removing the four stainless steel button head machine screws on the front of the keypad case using the security hex key provided with the unit. The front and back half will separate.
2. Mount the back plate to the desired keypad location using the three-keyed holes. Be sure to seal around the back of each screw hole and around the back of the wire hole with an outdoor silicone sealant. If the keypad is being mounted on a gooseneck or bollard, run a bead of silicone in a triangle around the three screwholes. If the keypad is being mounted on a wall, before mounting, run a bead of silicone in a square around the back of the keypad about ½ inch from the edge.

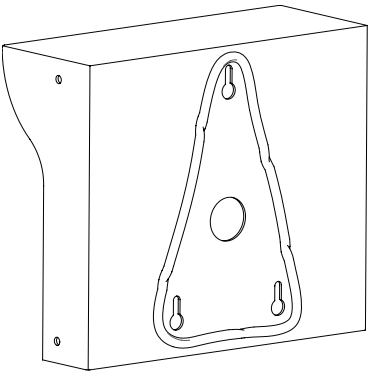


Figure 14

3. Pull the necessary wires through the wire hole on the back of the housing. Allow an extra 1 foot of wire to remain inside the housing. After the wire connections are complete, excess wire can be pushed back into the gooseneck or wall or it can be carefully set inside the keypad housing for future maintenance and service. Each keypad should have the following wires:
   - One 18 AWG, 4-conductor, shielded cable coming in from the controller or from the previous AI device in line.
   - One 18 AWG, 4-conductor, shielded cable going out to the next AI device in line (if there is another AI device down the line).
   - One earth ground wire

- One or two 18 AWG, 2-conductor cable(s) coming from the gate operator or door strike. *
- One 18 AWG, 2-conductor, shielded cable coming from the intercom base station if intercoms are being used.
- One RG59U video cable if a pinhole camera option is being used.
- One 18 AWG, 2-conductor cable for the presence sensor if it is being used.

* The cable to the door strike or gate operator will only be present if the relay inside the particular keypad is being used to trigger the door or gate. The controller can be configured to use relays on the circuit board, on a separate relay board, or on almost any other AI device to trigger a gate or door. For security reasons, the relay in the keypad nearest a door or gate should not be the one used to directly trigger the gate or door.

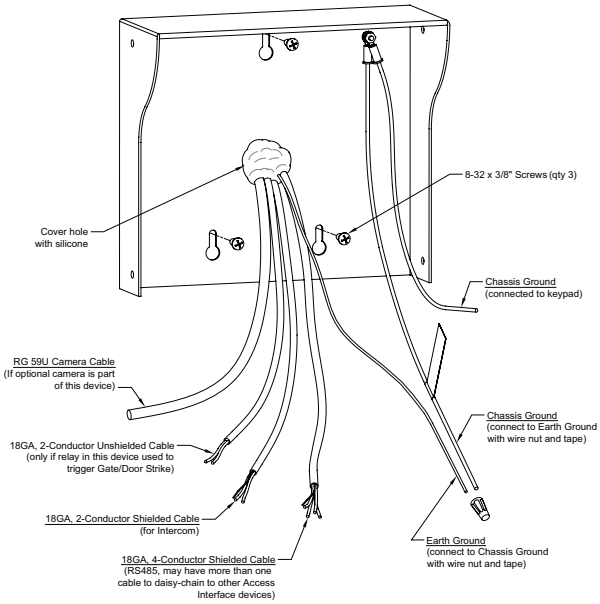
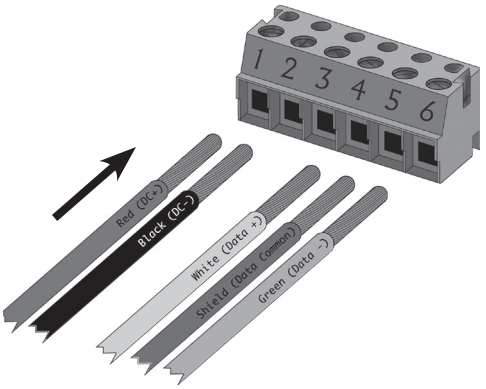


Figure 15

4. Strip back the outer insulation and shield foil from both of the 18 AWG, 4-conductor, shielded cables (coming from the controller or previous AI device in line and going out to the next AI device in line), being careful not to cut the bare shield wire. Strip ¼ inch of insulation off the end of each of the individual colored conductor wires.
5. Remove the terminal blocks from the keypad circuit board by sliding them up and off. The terminal blocks may be somewhat difficult to remove as a tight electrical connection is necessary. If they are tight, rock them slightly back and forth while lifting away from the board.

6. Insert both red wires (coming in from controller and going out to next AI device) into terminal slot 1 on the first terminal block (P1). Ensure that they are both seated all the way inside the slot. Use a flathead precision screwdriver to tighten down the terminal screw. Verify that the terminal slot has tightened down on the copper wire and not on the rubber insulation. There should be no copper wire showing outside of the terminal slot. Gently tug the wires to verify that they are tightly held inside the terminal slot. Repeat this process with each of the remaining wire connections as shown in Figure 16.



Terminal Block P1 (left)

1. Red DC+ *
2. Black DC - *
3/ Earth Ground if applicable
4. White Data +
5. Shield **
6. Green Data -

* If using AC power, place the AC wires in slots 1 and 2. We recommend 12 – 18 VDC.

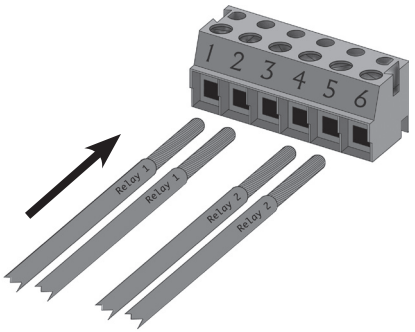
** Shield wire should be insulated with heat shrink or electrical tape.

Figure 16

7. The right (relay) terminal block is used for the relay connections. Pins 1, 2, and 3 are for the first relay and Pins 4, 5, and 6 are for the second. If a gate operator or door strike is being triggered directly from this keypad, the wires will connect to two of these three pins on Relay 1. Refer to the gate or door strike manufacturer's instructions to determine whether it needs to be connected to the normally open and common or to the common and normally closed. Relay 2 can be programmed to serve any of a number of functions using both the internal APEX programming and/or the software.
8. The earth ground wire should be connected in situations where the keypad is mounted on (or in) a wall that is wood, stone, or other nonconductive material. When installing an elevator APEX or the flush mount APEX, earth ground must always be connected. An earth ground connection is not always necessary when the keypad is mounted on a bollard or gooseneck.

   To connect the ground wire, run a copper wire from a grounded water pipe or from a copper rod in the ground to the keypad and connect it to the green earth ground wire using a wire nut. This installation must meet applicable code as the type of wire, depth of burial, and size of the rod may vary by municipality.

9. Connect any additional features, such as intercom, camera, gate operator, or door strike, that are installed on the APEX.
   - **Intercom.** Connect the wires to terminal block P2 in the upper left corner of the board as shown in Figure 18a. The connection and jumper settings will vary depending on whether the intercom is LEF Single Master Station, LEF Multiple Master Station, or NEM type intercom. Refer to the manufacturer's instructions. It is also important to set the jumper settings as shown in Figure 18b. These will vary depending on the type of intercom setup used.



Terminal Block P4 (Right)

1. Relay 1 Normally Open Wire
2. Relay 1 Common Wire
3. Relay 1 Normally Closed Wire

4. Relay 2 Normally Open Wire
5. Relay 2 Common Wire
6. Relay 2 Normally Closed Wire

Figure 17: Relays

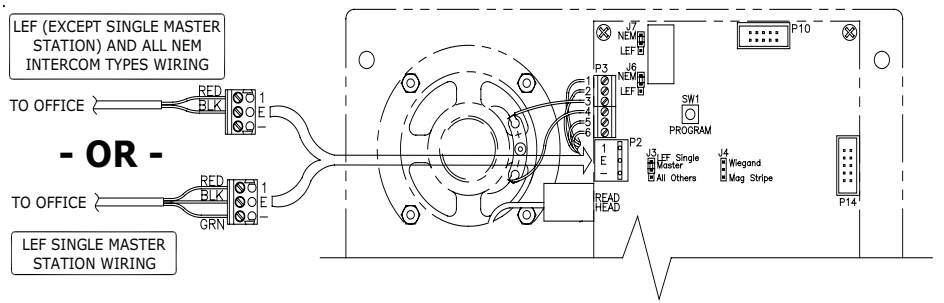


Figure 18a: Intercom

INTERCOM JUMPER CONFIGURATION TABLE			
INTERCOM TYPE	**APEX JUMPER CONFIGURATION**		
NEM (ALL)	**J7** NEM / LEF	**J6** NEM / LEF	**J3** LEF Single Master / All Others
LEF (ALL BUT SINGLE MASTER STATION)	**J7** NEM / LEF	**J6** NEM / LEF	**J3** LEF Single Master / All Others
LEF (SINGLE MASTER STATION)	**J7** NEM / LEF	**J6** NEM / LEF	**J3** LEF Single Master / All Others

Figure 18b: Intercom

The standard APEX device can be connected to an Aiphone LEF or Aiphone NEM intercom. The intercom wiring must be separate from all other wiring to the APEX. Shielded 18 AWG, 2- or 3-conductor cable should be used for the intercom depending on the type of intercom being used. Refer to the intercom manufacturer's specifications for more detail. The intercom type jumpers on the APEX circuit board must be set to match the type of intercom being used.

- **Pinhole Camera.** Connect the video signal wire using RG59U video wire and BNC type connectors. The pinhole camera power is supplied by the APEX. It may be necessary to install a video amplifier or a video isolator depending on how the video system is installed. See Figure 19 for information on connecting the camera.

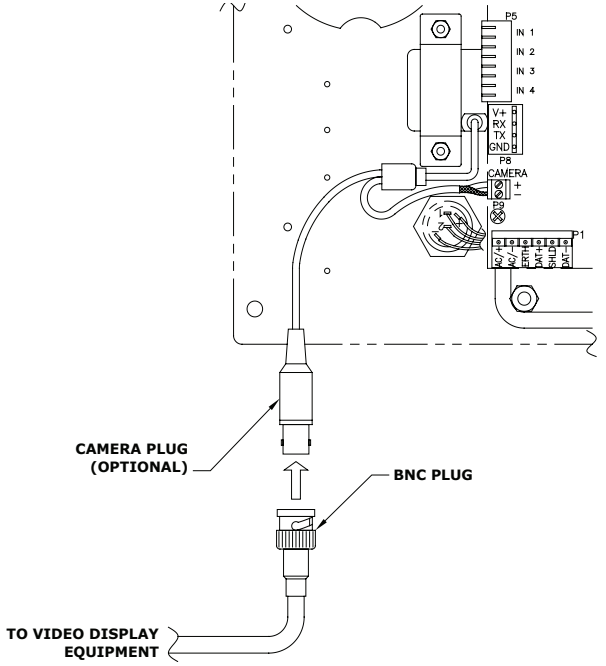


Figure 19

- **Gate Operator.** Most gate operators use a single dry contact to trigger the gate to open. See Figure 20 for details on connecting a gate operator to the APEX.

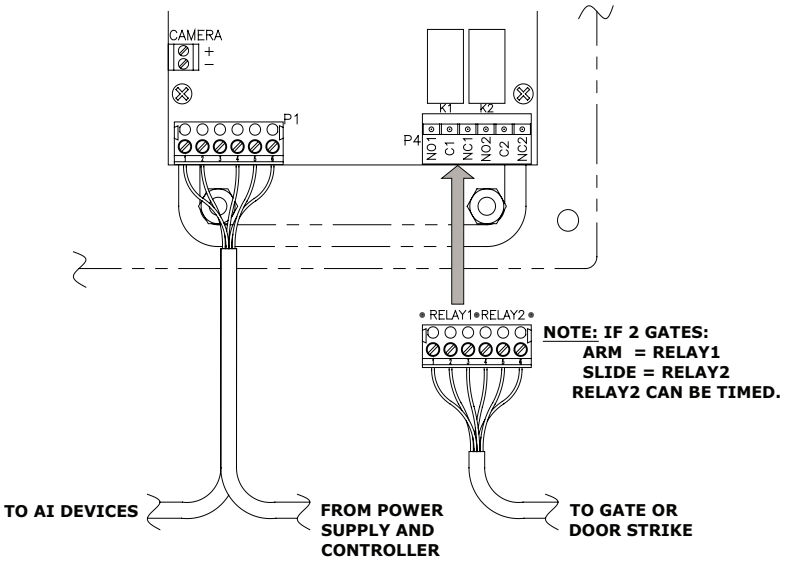


Figure 20

The APEX is equipped with two form C relays for use with gate operators. Both relays are connected to the removable terminal block at the lower right corner of the board (P4). Make sure the signal from the operator meets the electrical specifications for the relays. DO NOT USE ANY HIGH VOLTAGE SIGNALS. Refer to the gate operator manual for the gauge of wire required. The pin connections for the connector are as follows:

Pin 1 – Relay 1 Normally Open
Pin 2 – Relay 1 Common
Pin 3 – Relay 1 Normally Closed
Pin 4 – Relay 2 Normally Open
Pin 5 – Relay 2 Common
Pin 6 – Relay 2 Normally Closed

A gate operator can be connected to either relay depending on how the APEX is setup. If desired, more than one operator can be connected to a single APEX device. If two or more APEX devices trigger one gate, that gate only needs to be connected to one of the devices. For security reasons, the gate operator should not be connected to the APEX being used for entry to prevent anyone from accessing the facility by vandalizing the entry APEX.

- **Door Strike.** The door strike connection is similar to a gate operator connection, except that the door strike requires power supplied by an external power supply. The power supply required will depend on the type of door strike. Do NOT use the same power supply that provides power to the APEX device. Refer to Figure 21 for details of connecting the door strike.

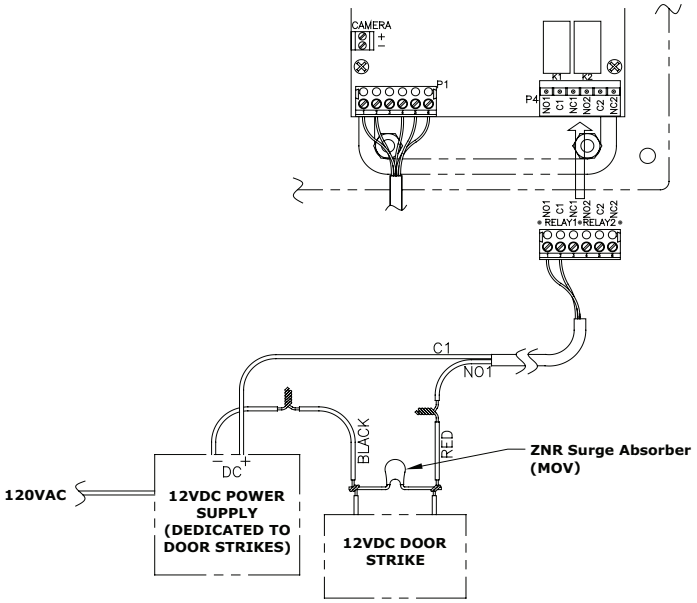


Figure 21

In Figure 21, the two wires that connect to the relay are labeled C1 and NO1. These should be connected to the Common and Normally Open contacts of one of the relays. The door strike can be connected to either relay if the Extended Door controls are not being used.

If Extended Door controls are being used, the door strike must be connected to relay 1. In addition, the door contact must be connected to input 1 and the request to exit device (if used) must be connected to input 2. Inputs 1 and 2 cannot be used for any other function while Extended Door Controls are enabled.

10. After all wiring is complete, gently push the excess wire back through the hole in the wall or gooseneck, leaving just enough slack to allow the keypad to be opened for service or maintenance. Seal the back wire hole with outdoor rated silicone sealant and then screw the housing back together.

Testing the Keypad

1. Test the display by applying power to the keypad. The default date and time should appear on the display after power is applied. The controller updates the date and time to the keypad once a minute. The date and time on the display should update if the keypad is configured correctly. To verify that the backlight is working, press the * key. The backlight should come on and the display will read Please Enter Access Code. If no keys are pressed for 10 seconds the display will return to the Date/Time and the backlight will shut off.
2. To test touchpad operation, press the * key. When the display shows Please Enter Access Code, press 0, 1, 2, 3, 4, 5, 6, 7, 8, 9. You should see each digit appear on the display as it is pressed (you will see an X for each digit if Secure Entry is enabled). After pressing the # key to transmit the code to the controller, the display will show Please Wait until a response is returned from the controller. If the keypad is communicating with the controller, the display will show either Entry Granted or another corresponding message.
3. Test for communications with the controller by applying power to the controller. The date and time at the controller will automatically update on the keypad and appear in the display. This verifies communications from the controller to the keypad. Test communications from the keypad to the controller by entering an access code into the keypad and pressing the # key.
4. If the keypad display responds with anything other than Please Wait before returning to the date and time, the keypad has successfully communicated with the controller. If only the message Please Wait appears before the keypad defaults back to the power-up default time of 12:00, recheck the wiring, Baud rate settings, and dipswitch settings. Also ensure that the controller is set to the correct number of remotes.

OPERATION

Input/Output Descriptions

Relay Outputs

The APEX Access Device is equipped with two Form C relays. Relay 1 is used to trigger an access point (door strike, gate operator, etc.). Relay 2 can be used for several different functions depending on the options set. Relay 2 can be set for SLAVE TO RELAY 1, DIFFERENT HOLD TIME, AUX. OUTPUT, HOLD OPEN BY TIME, and ALARM OUTPUT. See the APEX Access Device Setup Function section for instructions on changing the settings.

Slave to Relay 1. When set for SLAVE TO RELAY 1, Relay 2 will operate simultaneously with Relay 1. Some installation may use a secondary slide gate along with a barrier gate. In these applications, Relay 2 can be used to trigger the secondary gate at the same time as the primary gate, thus eliminating the need for an isolation relay.

Different Hold Time. Selecting DIFFERENT HOLD TIME causes Relay 2 to trigger at the same time as Relay 1 but stay active for a different length of time. Using the previous example, the two gates may require different trigger times. For example, the barrier gate may require a hold time of 1 second and the slide gate a hold time of 5 seconds. In this case, use the DIFFERENT HOLD TIME option. This function can also be used to activate a door holder. See Using Extended Door Controls for more information.

AUX Output. When set for AUX. OUTPUT (the default setting), Relay 2 can be used for any external device or secondary access point. It responds just like a relay on the relay board. This is useful for lighting zones, elevators, or additional gates or door strikes. This feature is set up in the control software.

Hold Open By Time. When two gates are used, it is sometimes desirable to hold the secondary gate open during certain hours. The HOLD OPEN BY TIME option allows the second relay to activate for a certain period of time each day. For example, a site may want the slide gate across the main entrance to stay open during regular business hours and use the barrier gate for access. After hours, both gates must activate to allow entry and exit.

For this configuration, select the HOLD OPEN BY TIME option, then set the hours for Relay 2 to Active. Every day of the week can have different open and close hours. In addition, holiday hours can be set and the next holiday date entered. When that date occurs, the holiday hours will be used instead of the regular hours. (The next holiday date must be reprogrammed after each holiday.) If the “Slave After Hours” option is enabled, Relay 2 will act as a slave to Relay 1 outside the programmed hours.

Alarm Output. When the ALARM OUTPUT setting is selected, Relay 2 will be used to turn on an alarm device, such as a siren or strobe, when an alarm occurs. Any system alarm will trigger this relay.

The hold time for Relay 1 is determined by the controller and not by the APEX except when extended door controls are used.

Dry Contact Inputs

The four optional inputs are designed for use with a dry contact input device such as a unit door or office door switch or relay. The contact must be a dry contact type device that does not source any voltage. Each input has multiple functions depending on the options set. If no options are set, the four inputs will operate and report to the controller as standard door contacts. The multiplexer number will be the unit address of the APEX device and the channel will be the input number (1-4). When other options are selected, the door reporting functions of the inputs used for the options are disabled and the alternative functions are enabled.

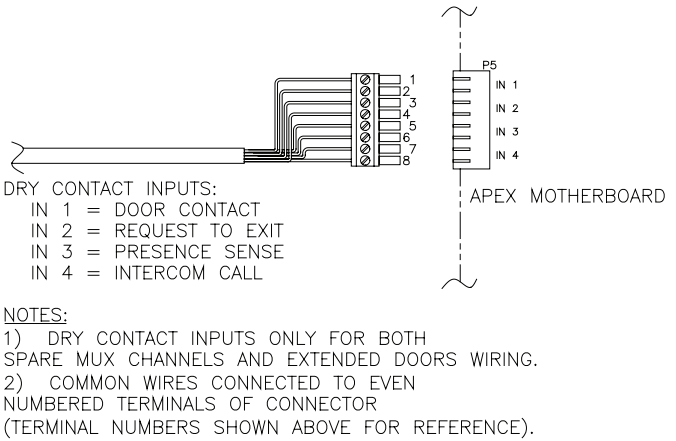


Figure 22

Inputs 1 and 2 – Extended door controls. When extended doors are set, Input 1 is used for the door contact and Input 2 is used for a request to exit device contact. See Using Extended Door Controls for more information.

Input 3 – Presence Sense. Input 3 is used for the presence sensor when this option is enabled. When enabled, an input is required from a vehicle loop detector or a pressure mat before the keypad will accept any input from the user. This prevents people from walking up to a drive-through gate and entering a code.

Input 4 – Intercom Call. Input 4 is used with the Intercom Call Report function. When the intercom call report option is selected, any contact on Input 4 will report as an intercom call to the controller. A special call button switch is necessary for this option.

Using Extended Door Controls

The extended door controls function allows comprehensive access management. Door controls are designed for use with a door to a building but can be used for a gate or other access device. There are four connections used by the extended door controls. Input 1 is used for the door alarm contact, Input 2 is used for the request to exit device, Relay 1 is used to trigger the door strike, and Relay 2 is used to activate a door holder. When the extended door control function is enabled, the other uses of these inputs and relays are disabled.

Operation of this function depends on having a door equipped with both a door strike and a door alarm contact. The door strike will be connected to Relay 1 and the door alarm switch will be connected to Input 1. The APEX activates Relay 1 for the Door Strike Time entered during setup programming. This allows the APEX device to activate the door from a request to exit device. Relay 1 will activate the door strike when a valid access command is sent from the controller. This is the only case in which the hold time for Relay 1 is not determined by the controller. Instead it is set by the Door Strike Time parameter Setup Function. Once the door strike is activated, the door can be opened.

To prevent the door from being held or propped open, the Max. Door Open Time parameter can be set in the Setup function. If the door is held open for longer than the time specified by the Max. Door Open Time, the controller will respond with an alarm and the Door Held Open message. When the door is closed, the controller will report Door Closed.

A request to exit (RTE) device is typically a push button or motion detector designed to open a door from the inside. If an RTE device is added to Input 2, the door strike will be activated by the controller or by the signal from the RTE device. If the door is opened without Relay 1 being active, the controller will respond with an alarm and the Door Held Open alarm message.

If an optional door holder is used, Relay 2 will control that device. When the door is opened by the controller or by the RTE device, Relay 2 will activate to turn on the door holder and hold the door open. To use a door holder, Relay 2 must be set for DIFFERENT HOLD TIME in the APEX Device Setup Function. The amount of time the door is held is specified by the Relay #2 Hold Time parameter. This time must be set to a value less than the Max. Door Open Time to avoid false alarms.

APEX Access Device Setup Function

To enter Setup mode:

1. Press the *, 0, and # keys simultaneously
2. Enter the factory default password: 8898
3. Press the # key

NOTE: In the event the password is changed and then forgotten, you can disconnect power from the APEX and then hold the program button while reconnecting power. This will bypass the password prompt and enter the Setup mode directly. When using this method, you will be prompted to Restore Factory Defaults. Select Yes to restore all default factory settings including the site name and password.

Press the # key to advance through each setup parameter. A parameter is automatically saved when you press # and move to the next parameter. If the timeout is allowed to occur, the current parameter will NOT be saved.

Numeric values are entered directly into the unit using the number keys. When an option is presented, use the * key to scroll through the available settings.

There are three (3) ways to exit Setup mode:

1. Press the 7, 8, and 9 keys simultaneously
2. Go through all of the setup functions
3. Press the program button on the circuit board

A timeout is built into the system that will exit Setup mode if there is no input on the keypad for an extended period of time.

Setup Parameters / Functions

Setup parameters in the order displayed by the APEX access device are:

RESTORE FACTORY DEFAULTS? Press * for YES Press # for NO	**This prompt only appears if the program button is held while power is applied to the APEX device.** Pressing the * key to select YES will restore all of the factory defaults. **WARNING:** This will overwrite all setup parameters including the setup password and the site name.
Restoring Defaults	Shown only while the APEX device is restoring the factory defaults.
Defaults Restored! Press # to Continue	Shown after the factory defaults are restored.
Current Address: 001 Enter New Address: PRESS # WHEN DONE	Polling address used by the controller. Any number from 1 to 127 can be entered. The numbers 0 and 22 cannot be used. Each device connected to the controller must have a unique address. The factory default is 1.
Communications Rate:9600 Press * to Change PRESS # WHEN DONE	The communications baud rate used by the controller. Scroll through the list of available rates by pressing the * key. The factory default is 9600.

At this point, the basic parameters required for operation have been entered. If no other options are active or required, you can exit the setup mode. Following are optional parameters to customize the feel of the site.

NOTE: Several options allow the setting of time in seconds. When minutes are desired, multiply the number of minutes by 60 to get the number of seconds. For example: 3 minutes X 60 seconds per minute = 180 seconds.

Change the Setup Password? Press * for YES Press # for NO	Allows you to change the setup password from the factory default of 8898. When YES is selected, the unit will prompt for the new password. The new password must be entered twice for verification before it will be changed. If both passwords entered match, the password will be changed. Otherwise, a message will indicate that the passwords do not match.
Tamper Sensor is: ENABLED Press * to Change PRESS # WHEN DONE	Controls the use of the tamper sensor. Options are ENABLED and DISABLED. If enabled, the keypad will not function and an alarm will occur from the controller if the unit is tampered with. Factory default is ENABLED.
Secure Code Entry? NO Press * to Change PRESS # WHEN DONE	Controls the characters displayed during code entry. When set to YES, the display will show only * for each key pressed. When set to NO, the numbers pressed will be echoed to the display. Factory default is NO.
Beep with Key Press? YES Press * to Change PRESS # WHEN DONE	Controls the internal buzzer used to provide audio feedback for any key press. When set to YES, the buzzer will produce a short beep when a key is pressed. When set to NO, the buzzer will not sound with key presses. Factory default is YES.
Beep with Access? YES Press * to Change PRESS # WHEN DONE	Causes the internal buzzer to sound when an access is attempted. A valid access will cause the buzzer to sound one long beep. All other attempts will cause the buzzer to sound four short beeps. Factory default is YES (on).
Sound Buzzer w/Alarm: NO Press * to Change PRESS # WHEN DONE	Controls the internal buzzer used to provide audible feedback when a system alarm occurs. When set to YES, the internal buzzer will sound whenever an alarm occurs and will remain on until the alarm resets from the controller. When set to NO, the internal buzzer will not sound when an alarm occurs. Factory default is NO.
Current Language: ENGLISH Press * to Change PRESS # WHEN DONE	Allows user messages to be displayed in one of nine languages. The other languages are French, Spanish, Danish, Norwegian, Deutsch (German), Dutch, Portuguese, and Italian. Only user messages are changed, the setup functions remain in English. Factory default is English.

Date Format: US Press * to Change PRESS # WHEN DONE	Controls how the date is displayed on the screen. Options are US and EUROPEAN. US format displays MM/DD/YY. European format displays DD/MM/YY. The factory default is US.
Time Format: 12 Hr. Press * to Change PRESS # WHEN DONE	Controls how the time is displayed. Options are 12 Hour and 24 Hour. The 12 Hour displays the time as HH:MM:SS followed by am or pm. The hour will be displayed as 12:00:00 am to 12:00:00 pm. The 24 Hour format displays the time as HH:MM:SS without the am or pm indicator. The hour will be displayed as 00:00:00 to 23:59:59. The factory default of 12 Hour.
Relay #2 Function: AUX. OUTPUT Press * to Change PRESS # WHEN DONE	Controls the function of Relay 2. Options are ALARM OUTPUT, HOLD OPEN BY TIME, SLAVE TO RELAY 1, DIFFERENT HOLD TIME, and AUX. OUTPUT. Each option is described in detail. The factory default is AUX. OUTPUT.
When Relay #2 is set for: SLAVE TO RELAY #1	Causes Relay 2 to operate at the same time as Relay 1. This allows it to be used for a secondary device without having to put in a separate isolation relay.
When Relay #2 is set for: DIFFERENT HOLD TIME	Relay 2 operates at the same time as Relay 1 but is activated for a different length of time. This is useful when dual gate operators or door holders are used that require different activation times. When this option is selected, the following prompt will appear.
Relay #2 Hold Time In seconds: 001 PRESS # WHEN DONE	Sets the hold time for Relay 2 when it is used with a DIFFERENT HOLD TIME from Relay 1. The maximum time is 255 seconds.
When Relay #2 is set for: AUX. OUTPUT	Causes Relay 2 to operate as a separate relay that can be used for door or gate access, lighting zones, elevators, etc. Its function is independent of Relay #1 and is controlled by the controller. This feature allows the APEX to be used as a 2-channel relay as well as an access device.
When Relay #2 is set for: ALARM OUTPUT	Activates Relay 2 when a system alarm occurs, allowing the relay to be used to control an external siren horn or other alarm device.
When Relay #2 is set for: HOLD OPEN BY TIME	Allows Relay 2 to be used for a secondary slide gate or other overlock device that will be held open at a fixed time of day. You can set the open and close times for each weekday and for holidays. The next holiday date is also programmed.

Enter MONDAY OPEN Time PRESS # WHEN DONE	Sets the time of day on Monday that Relay 2 will activate.
Enter MONDAY CLOSE Time PRESS # WHEN DONE	Sets the time of day on Monday that Relay 2 will deactivate.
Enter TUESDAY OPEN Time PRESS # WHEN DONE	Sets the time of day on Tuesday that Relay 2 will activate.
Enter TUESDAY CLOSE Time PRESS # WHEN DONE	Sets the time of day on Tuesday that Relay 2 will deactivate.
Enter WEDNESDAY OPEN Time PRESS # WHEN DONE	Sets the time of day on Wednesday that Relay 2 will activate.
Enter WEDNESDAY CLOSE Time PRESS # WHEN DONE	Sets the time of day on Wednesday that Relay 2 will deactivate.
Enter THURSDAY OPEN Time PRESS # WHEN DONE	Sets the time of day on Thursday that Relay 2 will activate.
Enter THURSDAY CLOSE Time PRESS # WHEN DONE	Sets the time of day on Thursday that Relay 2 will deactivate.
Enter FRIDAY OPEN Time PRESS # WHEN DONE	Sets the time of day on Friday that Relay 2 will activate.
Enter FRIDAY CLOSE Time PRESS # WHEN DONE	Sets the time of day on Friday that Relay 2 will deactivate.
Enter SATURDAY OPEN Time PRESS # WHEN DONE	Sets the time of day on Saturday that Relay 2 will activate.
Enter SATURDAY CLOSE Time PRESS # WHEN DONE	Sets the time of day on Saturday that Relay 2 will deactivate.
Enter SUNDAY OPEN Time PRESS # WHEN DONE	Sets the time of day on Sunday that Relay 2 will activate.
Enter SUNDAY CLOSE Time PRESS # WHEN DONE	Sets the time of day on Sunday that Relay 2 will deactivate.
Enter HOLIDAY OPEN Time PRESS # WHEN DONE	Sets the time of day on the next Holiday that Relay 2 will activate.
Enter HOLIDAY CLOSE Time PRESS # WHEN DONE	Sets the time of day on the next Holiday that Relay 2 will deactivate.
Enter the Next Holiday Date: PRESS # WHEN DONE	Sets the next date that will use the holiday hours.

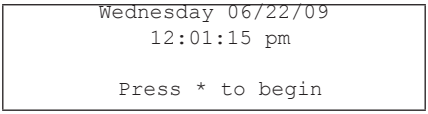
Slave After Hours ENABLED Press * to Change PRESS # WHEN DONE	Allows Relay 2 to activate when Relay 1 is tripped outside of hold open hours. Useful when using a secondary gate. Factory default is Enabled.
Max. # of Attempts Before Lock Out: 000 PRESS # WHEN DONE	Sets the maximum number of attempts within a one minute period before the APEX will prevent further code entry. If the number is set to three, then after three successive attempts with invalid codes, the user will be locked out. The lockout will remain active for 60 seconds after the last key press. If the user keeps pressing keys the lockout time will continue to be reset. The maximum value is 10. Factory default is 000, which disables the lockout feature.
Use Custom Message? NO Press * to Change PRESS # WHEN DONE	Displays a third message on the display before any key is pressed. The APEX will scroll through three messages instead of two and allows communication with customers. It cannot be changed from the controller. Factory default is NO.
Trip Relay Offline? NO Press * to Change PRESS # WHEN DONE	Causes Relay 1 to trip if the APEX is not communicating with the controller. **WARNING:** Improper use of this option leave your site vulnerable. **Do not** set this option on an entry keypad. Factory default is NO.
Current Comm. Off Time (seconds) 005 PRESS # WHEN DONE	Sets the amount of time the APEX should wait before considering it has lost communication with the controller. Any value from 1 to 255 seconds can be entered. Factory default is 5 seconds.
Extended Door Ctls: DISABLED Press * to Change PRESS # WHEN DONE	Sets the extended door controls. It requires the optional inputs. When ENABLED, the device allows control of a door with request to exit inputs and hold open alarm notification. Input 1 is used for the door alarm contact and Input 2 is used for the request to exit device contact. Relay 1 is used to activate the door strike so that it will open and Relay 2 is used to activate a hold open device for the door. Factory default is DISABLED.
Door Relay Time In seconds: 000 PRESS # WHEN DONE	The length of time (in seconds) for which the door relay will activate. The user must open the door during this period of time or the door will not open. The maximum value is 255 seconds. Factory default is 2 seconds.
Max Door Open Time In seconds: 00000 PRESS # WHEN DONE	The number of seconds the door can be held open before an alarm is sent to the controller. If someone props a door open for longer than this time, the alarm will sound. The maximum value is 65535 seconds. The maximum value translates to 1092.25 minutes (65535 seconds / 60 seconds per minute) or 18.2 hours (65535 seconds / 3600 seconds per hour). This feature is available when using extended door controls. Factory default is 30 seconds.

Presence Input Req. NO Press * to Change PRESS # WHEN DONE	Requires use of the optional inputs. Input #3 must be active before a code can be entered. This can be used where a vehicle sensor is required in a drive or other traffic area. When set to YES, Input #3 is dedicated to this function and cannot be used as an alarm input. Factory default is NO.
Intercom Call Report: NO Press * to Change PRESS # WHEN DONE	Requires the optional inputs. Allows the controller to report an intercom call. When set to YES, Input 4 is used for the intercom call. The exact configuration of the connections depends on the intercom type. This option requires the use of an intercom call button. Factory default is NO.
Change the Displayed Site Name? Press * for YES Press # for NO	Allows the displayed site name to be changed. If YES is selected, setup will proceed to the following step. Select NO to jump to the last parameter.
Site Name 1st Line: Your Storage *=Left #=Right	The first line of the site name that is displayed on the screen. Use the * and # keys to move left and right through the line. When the cursor is on a character, it can be changed by repeatedly pressing the corresponding number key until the desired character appears—similar to the method used for cell phones. Each key has both number and letter functions. ***A space is the last character on every key***. The following is a list of the keys and the characters each has in the order they appear. 1: 1QZqz., 2: 2ABCabc 3: 3DEFdef 4: 4GHIghi 5: 5JKLjkl 6: 6MNOmno 7: 7PRSprs 8: 8TUVtuv 9: 9WXYwxy 0: 0-#*$@’
Site Name 2nd Line: Facility 1=1QZqz., 0=0-#*$@’ *=Left #=Right	The second line of the displayed site name. It is changed in the same way as the first line.
Setup Complete PRESS # WHEN DONE	Message displayed when exiting from setup mode. Pressing the # key will return the device to normal operation. If no key is pressed, the device will return to normal operation after a few seconds and all information will be automatically saved.

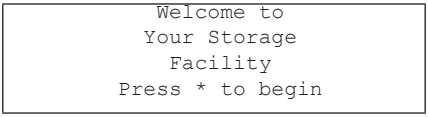
Standard Display Messages

The APEX has two standard messages and one optional message that are displayed when the power is on and no other functions have been selected. The display will switch between the messages approximately once every 5 seconds. The two standard messages are the date and time message and the Welcome to… message. The third message is an optional custom message.

Date and Time Message. The default time and date message. It is the first of two standard messages that the APEX displays when no keys have been pressed and no cards used. When the APEX is configured for reading magnetic stripe or proximity cards, the bottom line of the display will show Use Card or Press *.



Welcome to… Message. The second standard message displayed by the APEX when no keys have been pressed and no cards used. The two middle lines can be changed in the setup function to reflect the company name, giving a more friendly welcome each time a customer, employee, or resident enters or exits. Each line is limited to 20 characters. When the APEX is configured for reading magnetic stripe or proximity cards, the bottom line of the display will show Use Card or Press *.



Access Codes and Cards

Depending on how the system is configured, the user will have an access code that can be entered or a magnetic stripe card that can be swiped. When the user approaches the device, one of the standard display messages will be shown on the display. The system prompts the user with the message Use Card or Press *.

The display and keypad are backlit at a low level to conserve power when no one is using the device. This low level is sufficient to read the display at night. As soon as a customer enters a code or presents a card, the display comes to full brightness.

Access Codes. To enter a code, the user presses *. The following message will be displayed.

```
* PLEASE ENTER *
YOUR ACCESS CODE
PRESS # WHEN DONE
```

The user enters their access code using the touchpad and presses the # key. The APEX will send the code to the controller and wait for a response while the APEX goes through the security checks described in the Security Checks section. The message on the display will change to the following while waiting for a response.

```
* PLEASE WAIT *
VERIFYING ACCESS
```

Magnetic Stripe Cards. When the APEX is set to use magnetic stripe cards, the user swipes his or her card through the slot in the card reader on the APEX. The orientation of the card is important. The magnetic stripe on the card must be aligned to pass through the slot facing the wide side of the reader. If the APEX is not able to read the card correctly or if there is an error on the card, the following message will be displayed:

```
* WE'RE SORRY *
PLEASE TRY YOUR CARD
AGAIN
```

Once the card is read, the APEX will go through the security checks described in the Security Checks section. The Verifying Access message will be displayed while waiting for a response.

Proximity Cards. When the APEX is set to use proximity cards, the user simply places his or her card against the card reader on the APEX. The orientation of the card is not important. If the APEX is not able to read the card correctly or if there is an error on the card, the following message will be displayed:

```
* WE'RE SORRY *
PLEASE TRY YOUR CARD
AGAIN
```

Once the card is read, the APEX will go through the security checks described in the Security Checks section. The Verifying Access message will be displayed while waiting for a response.

Security Checks

A series of security checks are performed by the APEX before allowing entrance. These checks are used to prevent unauthorized access attempts. When a customer uses an access code, the checks are performed as soon as the code is entered. If the customer uses a card, the checks are performed as soon as the card has been swiped in the magnetic stripe reader or presented to the proximity reader.

Tamper Check. The APEX performs a tamper check to see if the tamper switch has been enabled. If it is enabled, it ensures that the switch is secure. If both conditions are true or the tamper is disabled, the APEX will proceed to the next security check. If the APEX detects tampering, it will display the following message and no further access attempts will be allowed.

```
* WE'RE SORRY *

THIS UNIT HAS BEEN
  TAMPERED WITH
```

Presence Required Check. After checking the tamper, the APEX will check to see if the Presence Required option has been selected. If it has been selected, the APEX will check the input to see if a presence has been detected. If this option has been turned off or if a presence has been detected, the APEX will continue with the next security check. If the APEX does not detect a required presence, it will display the following message and no further access attempts will be allowed.

```
* WE'RE SORRY *

NO PRESENCE HAS BEEN
    DETECTED
```

Maximum Attempts Check. The maximum attempts security check is designed to discourage someone from attempting numbers at random to enter the site. If the Max. Attempts before Lockout feature is set to a value other than zero, the APEX will check to see if the user has tried a code more than the allowed times. If not, the APEX will proceed to the next security check. If the maximum number of unsuccessful attempts has been exceeded, the APEX will display the following message and disable any further access attempts. The APEX will not allow any further attempts until it has had 60 seconds without any key being pressed. If a key is pressed while this message is displayed, the 60 second timer starts over.

```
* WE'RE SORRY *

PLEASE SEE THE
   MANAGER
```

Trip Relay Offline Check. The final security check for the APEX is to check the Trip Relay Offline option. If it has been enabled, the APEX will allow the access process to continue. If it has been disabled and the APEX is not in communication with the controller, then the APEX will display the following message and no further access attempts will be allowed.

```
We're Sorry, this
device is out of
service. Please see
the manager
```

Once the controller has gone through its security checks, it will verify the code and send a response to the APEX. The response message will be displayed. The messages that can be received from the controller vary depending on the type of response.

Access Response Messages

There are several standard messages built in to the APEX. The types of messages the APEX receives from the controller in response to an access request vary depending on the conditions. The following briefly describes the conditions and the displayed message.

For a valid Entry:

```
Welcome to
Your Storage
Facility
ENTRY IS GRANTED
```

For a valid Exit:

```
THANK YOU FOR USING
Your Storage
Facility
EXIT IS GRANTED
```

When the area is closed (outside of allowed access hours):

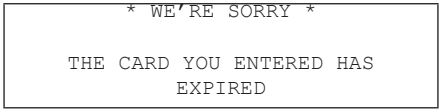
```
* WE'RE SORRY *

THIS AREA IS
CURRENTLY CLOSED
```

When the customer is not authorized to enter an area:

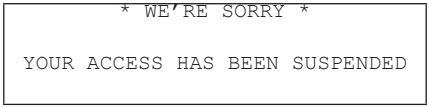
```
* WE'RE SORRY *

YOU ARE NOT ALLOWED
INTO THIS AREA
```

When the customer's code has expired:

When the customer's card has expired:



When the customer has been suspended:



When the code the customer entered is not valid:

When the card the customer used is not valid:

SYSTEM MAINTENANCE

The APEX Access Device requires minimal maintenance. However, as with any electronic or mechanical device that is used regularly, a small amount of maintenance done on a regular basis will extend the life of the product.

Periodic Visual Inspection

The APEX device should be inspected monthly. When performing the visual inspection, look for the following items:

- Damage caused by contact with vehicles, vandalism, etc.
- Damage caused by water, rain, salt spray, etc.
- Breaks or cracks in the sealant where the APEX mounts to the gooseneck stand or wall

Periodic Cleaning

The APEX should be cleaned at least twice a year. More frequent cleaning may be required in harsh environments.

Cleaning the Housing and Touchpad

Inspect and clean the housing and touchpad at least once a year. To clean the housing, spray the unit with a mild household cleaner and wipe with a soft cloth. Do not use harsh chemicals, abrasives, or petroleum-based products as they can damage the finish on the housing. Do not immerse the device in water or use a pressure washer. A small, soft brush (a toothbrush works well) can be used to clean between the keys on the touchpad.

Remove the APEX from the housing to inspect and clean the inside of the unit. When inspecting the inside of the housing and the APEX, look for the following items:

- Dirt or dust that has collected on the inside of the housing and the circuit board
- Signs of water damage or corrosion caused by prolonged contact to water
- Insects or insect droppings

Wipe out the inside of the housing with a soft cloth to remove any debris that has collected. Do not use cleaners of any kind, including water, to clean inside the housing or on the circuit boards. A small can of compressed air can be used to remove insects and dust from the circuit board.

Cleaning the Magnetic Stripe Reader

The APEX is shipped with a cleaning card for the magnetic stripe reader (if installed). The cleaning card is a small plastic card with a special cleaning surface on one side that has been saturated with a cleaning solution. To clean the reader, swipe the cleaning card several times through the slot in the reader. Once the card has been used, it should be disposed of. Additional cards can be ordered from PTI Security Systems. It is advisable to keep a supply of cards on hand.

TROUBLESHOOTING

For a *New Installation,* the typical problems encountered are related to the installation or configuration process. Start at step 1 in the Troubleshooting Steps section and proceed until the problem is found and resolved.

For an *Existing (previously working) Installation,* the first step is to determine whether anything has been changed at the site. For instance, Has there been any new construction? This includes any changes to the site, adding units, reconfiguring units, changing or adding video surveillance components, changing any electrical wiring, roofing changes, painting, etc. Even with a small change, wiring can be disturbed or disconnected or something new can interfere with equipment operation.

- If there has been new construction, start at step 1 in the Troubleshooting Steps section and proceed until the problem is found and resolved.
- If the APEX is not working, start at step 1 and proceed until the problem is found and corrected.
- If the APEX is receiving power, start at step 4 and proceed until the problem is found and corrected.

Keep thorough notes during troubleshooting to compare against and to help find problems, prevent confusion, and save time if site service by a technician is required.

Test power and communication

Step 1

Does the APEX Access Device have Power?

Yes – Proceed to step 2

No – Check Power Supply and Wiring and retest or see Multiple Device Problems

This can be tested quickly by checking the display of the APEX. If the display is on or if any of the LEDs on the board are on, the board has power. If there is no indication of power from the display or LEDs, use a volt meter to check for the presence of voltage on connector P1 pins 1 & 2.

Step 2

Is the voltage at the APEX, connector P1 pins 1 & 2, greater than 10.5 Volts? (Use a volt meter to measure the voltage).

Yes – Proceed to step 3

No – Check Power Supply and Wiring and retest

Step 3

Is the voltage at the APEX, connector P1 pins 1 & 2, greater than 18 Volts? (Use a volt meter to meas3ure the voltage).

Yes – Voltage is too high, check power supply and retest

No – Proceed to step 4

NOTE: Create a voltage map of the site by sketching out the locations of every AI device on the site. Use a multimeter to take DC power readings at each device. Note these readings on the sketch. Any device that is receiving less than 12V is underpowered and can cause the entire system to lock up.

Step 4

Is the display on the APEX blank?

Yes – Replace the APEX and retest

No – Proceed to step 5

Step 5

Is the APEX communicating with the controller and software?

Yes – Contact Technical Support if the APEX is still not working.

No – Check wiring and proceed to step 6

This can be determined by checking the LEDs on the APEX board or by running the system setup report on the controller. When the APEX is communicating with the controller, LEDs D1 – D6 will be blinking. If only D1 and D4 are blinking, proceed to step 7. Refer to Figure 23 for the location and function of the LEDs.

Step 6

Are any other devices set to the same address as the APEX?

Yes – Change one of the devices and retest

No – Proceed to the step 7

This can be determined by checking the addresses on all of the devices or by disconnecting the APEX and running the system setup report on the controller. If the system setup report shows the remote number (address) assigned to the APEX as being ON LINE with the APEX disconnected, then another device is sharing the same address.

Step 7

Is the maximum number of remotes in the controller set to a number greater than the address of the APEX?

Yes – Contact Technical Support if the APEX is still not working.

No – Change the maximum number of remotes and retest

This can be determined by running the system setup report from the controller or by checking the value under function 14. If the value is lower than the address of the APEX, the controller will not try to communicate with it.

Test card and code input

Use the following steps for troubleshooting keypads, Wiegand devices, and single door modules. Keep thorough notes during troubleshooting to compare against and to help find problems, prevent confusion, and save time if site service by a technician is required.

1. Try a code or card at the keypad controlling the gate. Be sure the code or card is one that is known to be working at that location and time. Try several codes to verify operation. Note which code(s) were tried and the response at each device as well as the response on the software event log.
2. Try the same code(s) or card(s) at other access devices on the property. Compare the result with the previous step. Try to narrow down whether multiple devices are affected or just one.
3. If the problem is narrowed down to one device, it must be determined if the problem is in the device or the location. Make sure to allow for access and egress of customers and then remove the device in question. Switch the device with another similar device that has been proven to be working. For example, if the entrance keypad isn't working, but the exit one is, then switch the two. Be sure to switch the addresses also. If the problem stays in the same location, it is probably a wiring issue. Contact a service company to check the wiring.

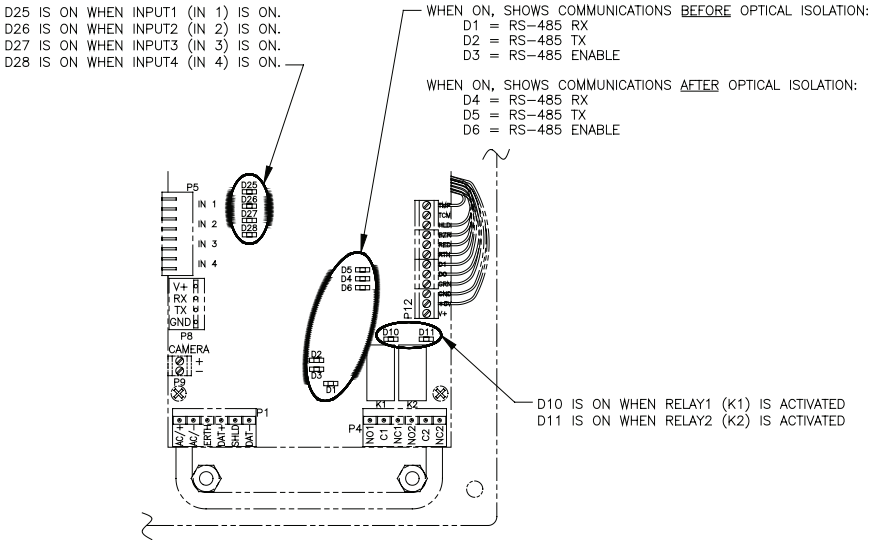


Figure 23

4. If there are multiple problems or ongoing issues, the process in the previous step can be performed for an entire site. Generally, multiple problems are a sign of problems in the wiring, either from bad splices, pinched or nicked wires, radio frequency interference, water in the conduit, or incorrect wire type. To check an entire site, allow for access and egress of customers and open the housings and unplug the power and data terminal blocks on every AI device on the site. When every device on the site is unplugged, add one device back into the system at a time. Allow that device to function for an hour and then add in the next device in line. Eventually, a device will be added that causes the problem to manifest. Switch this device with one that has been previously added to verify if the problem exists in the location or in the device.
5. Verify that all devices are receiving enough power. Create a voltage map of the site by sketching out the locations of every AI device on the site. Use a multimeter to take DC power readings at each device. Note these readings on the sketch. Any device that is receiving less than 12V is underpowered and can cause the entire system to lock up.

Test individual devices

To test individual devices, use the following procedure:

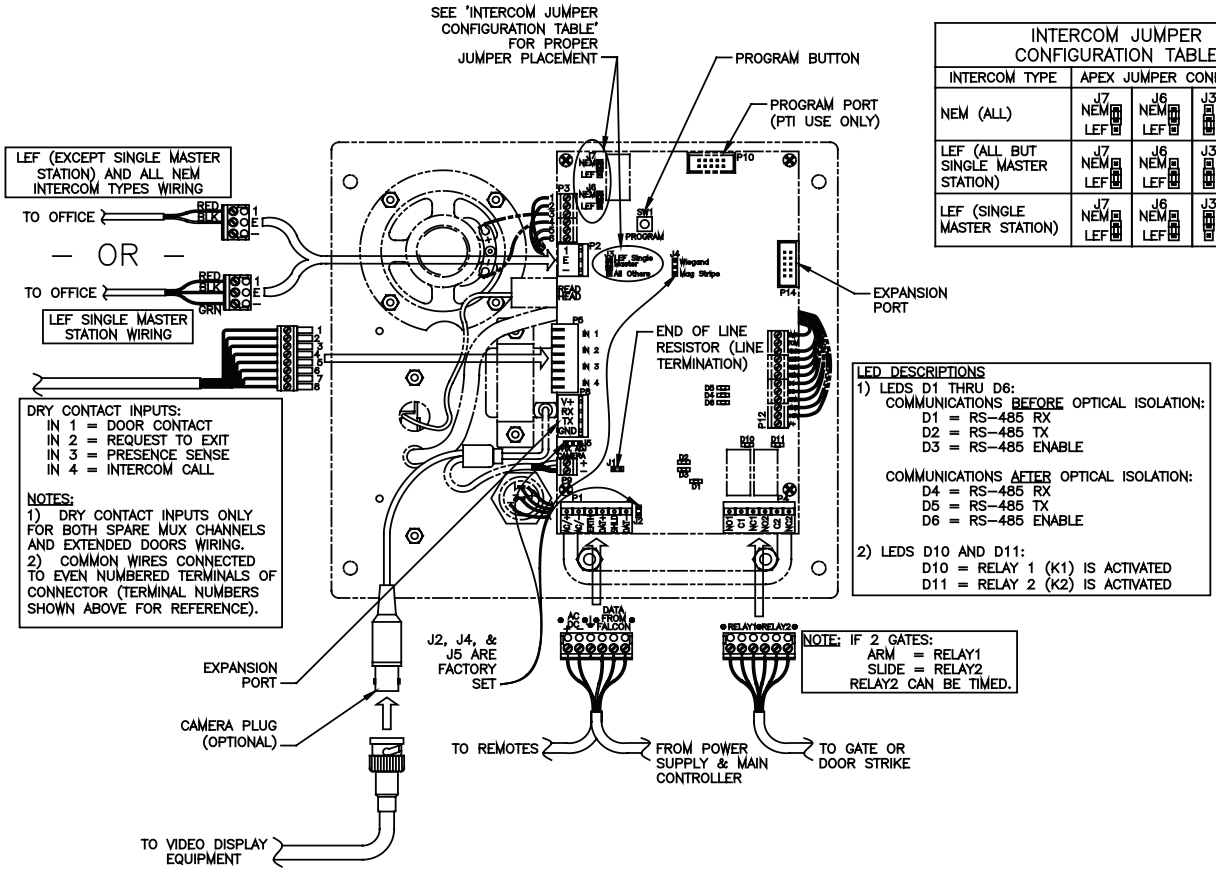
1. Try a code or card at the AI device controlling the gate. Be sure the code or card is one that is known to be working at that location and time. Try several codes to verify operation. Note which code(s) were tried and the response at each device as well as the response that appears on the event log.
2. Try the same code(s) or card(s) at other access devices on the property. Compare the result with the previous step. Try to narrow down which devices are affected.
3. To determine whether the problem is in the device or the location, make sure to allow for access and egress of customers and then remove the device in question. Switch the device with another similar device that has been proven to be working. For example, if the entrance keypad isn't working, but the exit one is, then switch the two. Be sure to switch the addresses also. If the problem stays in the same location, it is probably a wiring issue. Contact a service company to check the wiring.

Test multiple devices or entire site

Generally, multiple problems are a sign of problems in the wiring, either from bad splices, pinched or nicked wires, radio frequency interference, water in the conduit, or incorrect wire type. To check the entire site for problems, use the following procedure:

1. Allow for access and egress of customers and open all device housings.
2. Unplug the power and data terminal blocks on every AI device on the site.
3. Once every device on the site is unplugged, add one device at a time back into the system.
4. Allow the device to function for an hour and then add in the next device in line.

   Eventually, a device will be added that causes the problem to manifest. Switch this device with one that has been previously added to verify if the problem exists in the location or in the device.
5. If the problem stays in the same location, it is probably a wiring issue. Contact a service company to check the wiring.



INTERCOM JUMPER CONFIGURATION TABLE

INTERCOM TYPE	APEX JUMPER CONFIGURATION		
NEM (ALL)	J7 NEM / LEF	J6 NEM / LEF	J3 LEF Single Master / All Others
LEF (ALL BUT SINGLE MASTER STATION)	J7 NEM / LEF	J6 NEM / LEF	J3 LEF Single Master / All Others
LEF (SINGLE MASTER STATION)	J7 NEM / LEF	J6 NEM / LEF	J3 LEF Single Master / All Others

WARRANTY & DISCLAIMER

PTI Security Systems warrants its products and equipment to conform to its own specifications and to be free from defects in materials and workmanship, under normal use and service, for a period of one year from the date of shipment. Within the warranty period, PTI Security Systems will repair or replace, at its option, all or any part of the warranted product which fails due to materials and/or workmanship. PTI Security Systems will not be responsible for the dismantling and/or re-installation charges. To utilize this warranty, the customer must be given a Return Materials Authorization (RMA) number by PTI Security Systems The customer must pay all shipping costs for returning the product.

This warranty does not apply in cases of improper installation, misuse, failure to follow the installation and operating instructions, alteration, abuse, accident, tampering, natural events (lightning, flooding, storms, etc.), and repair by anyone other than PTI Security Systems. This warranty does not warrant the replacement of batteries that are used to power our products.

This warranty is exclusive and in lieu of all other warranties, expressed or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. PTI Security Systems will not be liable to anyone for any consequential or incidental damages for breech of this warranty or any other warranties.

This warranty will not be modified or varied. PTI Security Systems does not authorize any person to act on its behalf to modify or vary this warranty. This warranty applies to PTI Security Systems products only. All other products, accessories, or attachments used in conjunction with our equipment, including batteries, will be covered solely by their own warranty, if any. PTI Security Systems will not be liable for any direct, incidental, or consequential damage or loss whatsoever, caused by the malfunction of product due to products, accessories, or attachments of other manufacturers, including batteries, used in conjunction with our products.

The customer recognizes that a properly installed and maintained security system may only reduce the risk of events such as burglary, robbery, personal injury, and fire. It does not insure or guarantee that there will be no death, personal damage, and/or damage to property as a result. PTI Security Systems does not claim that the Product may not be compromised and/or circumvented, or that the Product will prevent any death, personal and/or bodily injury and/or damage to property resulting from burglary, robbery, fire, or otherwise, or that the Product will in all cases provide adequate warning or protection.

PTI Security Systems products should only be installed by qualified installers. The customer is responsible for verifying the qualifications of the selected installer.

PTI Security Systems shall have no liability for any death, injury, or damage, however incurred, based on a claim that PTI Security Systems Products failed to function. However, if PTI Security Systems is held liable, directly or indirectly, for any loss or damage arising under this limited warranty or otherwise, PTI Security Systems's maximum liability will not in any case exceed the purchase price of the Product, which will be fixed as liquidated damages and not as a penalty, and will be the complete and exclusive remedy against PTI Security Systems

Warning: The User should follow all installation, operation, and maintenance instructions. The User is strongly advised to conduct Product and systems test at least once each week. Changes in environmental conditions, electric or electronic disruptions, and tampering may cause the Product to not perform as expected.

Warning: PTI Security Systems warrants its Product to the User. The User is responsible for exercising all due prudence and taking necessary precautions for the safety and protection of lives and property wherever PTI Security Systems Products are installed. PTI Security Systems does not authorize the use of its Products in applications affecting life safety.

Notice. Some PTI Security Systems products use 900Mhz wireless technology. Other devices at the site such as cordless telephones or alarm components may cause interference that will disrupt the operation of the system or may be interfered with by the system. PTI Security Systems assumes no liability for any problems caused by interference. It is the sole responsibility of the user to identify and correct such problems.

For Technical Support, Please Visit:
support.ptisecurity.com

www.ptisecurity.com