PTI SECURITY SYSTEMS

VP Keypad Access Device
Installation and Operation Manual

SECURITY ACCESS CONTROL VIDEO

www.ptisecurity.com *800.523.9504*

114A3868 revision.E- July 2017

ETL LISTED US Intertek

Thank you for purchasing the VP Keypad 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 A 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 A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

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, therefore shielded twisted pair cable with ground wire is required for optimal operation. Additionally, larger gauge wire must be used the farther the device is from the controller,

Incorrect installation of electrical components can result in damage to electronics as well as personal injury.

Cross-wiring the AC power with the DC power will damage the electronics.

Cross-Wiring the Power wires with the Data wires will damage the electronics

Cross-wiring the positive and negative on the DC part of the system will damage the electronics.

Do NOT run low voltage system wires in the same conduit as high voltage wiring

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.

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

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.

Contents

Technical Specifications 1

Installation 2
- Introduction 2
- Mounting Access Devices 3
- Installing VP Series Keypads 9
- Installation Instructions 11

Connecting Additional Features (not on all models) 16
- Intercom 16
- Gate Operators 18
- Pinhole camera 19
- Testing the Keypad 20

Operation 22
- VP Keypad Setup Function 22
- Setup Parameters/Functions 23
- Optional Setup Functions 24
- Standard Display Messages 28
- Access Response Messages 31

System Maintenance 33

Troubleshooting 35
- Test Power and Communication 36
- Test Individual Devices, Card and Code Input 40
- Test multiple devices or entire site 41
- Warranty & Disclaimer 43

Technical Specifications

Power Supply:

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

Relay Specifications:

Maximum Switching Voltage*:	30 VAC / 24VDC
Maximum Switching Current*: * Resistive Load	1A (NO / NC)

Environmental:

Ambient Temperature:	-40°C to +85°C (-40°F to 185°F)
Ambient Humidity:	0 to 85% non-condensing

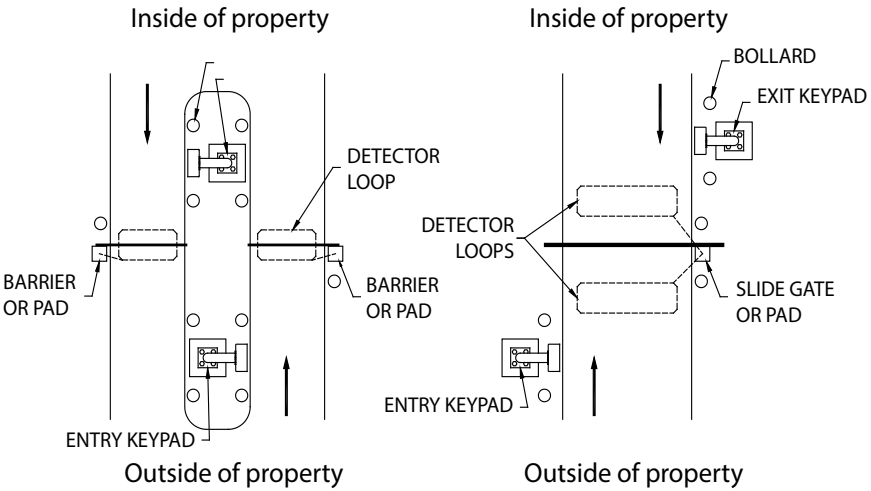
Installation

Introduction

The VP Access Device (VP) controls entry to or exit from a secured area. It works in conjunction with a controller and control software. The VP can be used to control gate access, building access, room access, elevator access, etc. and 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 VP determine where and how the device will be installed, since the mounting location is determined by how the device will be used. For drive up access, install the device where it can be reached from a vehicle's driver door. If the VP is used for walk up access, install it where it can be accessed by a person on foot.

Drawing 1: *Drive up accessability*



Drive Up Accessibility

When the VP 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 of these locations use gooseneck stands on an island between the entry and exit gates (or to the left side of the gate if a single gate is used). "Drawing 1: Drive up accessability" on page 2 shows different entry layouts.

Local building codes may set a minimum and maximum height for devices that are accessible by vehicle. shows suitable mounting locations when used for vehicle access.

Walk Up Accessibility

When the VP is used for walk up access, it can be mounted on a stand or attached to a wall. It can also be surface mounted so that it protrudes from the wall.

Mounting Access Devices

The proper mounting height for the VP varies with the application and it can be installed at an entrance on a gooseneck/bollard or attached to a wall.

Once the keypad location is determined, note , the location and purpose of the device on a site security wiring plan. Keep the plan in a safe location for future maintenance and service purposes.

Surface Mount

- Surface mounted keypads are often used in conjunction with door strikes and elevators.
- Mounting height is usually 48" – 58" from the floor to the center of the '5' button on the touchpad. However, the final location of the keypad may be affected by local building codes.
- The choice of fasteners depends on the construction material of the wall.

If the VP is installed on an exterior wall, seal the contact point between the housing and the wall with a silicone sealant rated for outdoor use. This prevents moisture and insects from getting into the housing.

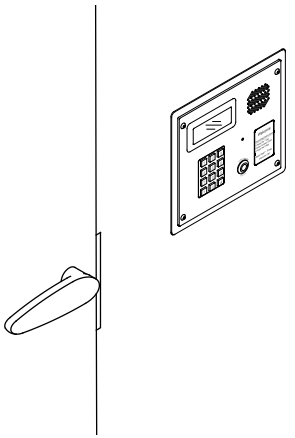
Flush Mount

A flush mount box allows the keypad to be set into hollow walls and is 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.

A gasket is needed for the face plate if the flush mount kit is used outdoors. Refer to "Drawing 8: Wiring for VP keypad" on page 10 for the mounting details of the flush mount adapter.

The actual placement of the VP device and its wiring methods may be affected by local building codes.



Drawing 2: Flush mount keypad

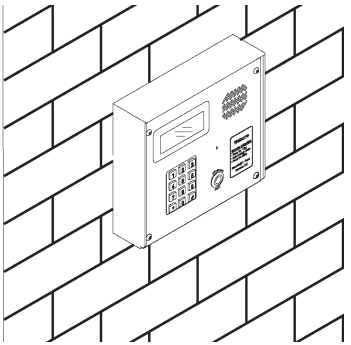
An elevator flush mount is available made of brushed stainless steel for mounting inside elevator cars; this model does not include an intercom.

Box Mount

A box mount with no shaded overhang is available for locations that require the keypad to be mounted lower than standard height, such as for handicap access. This box mount must be ordered separately.

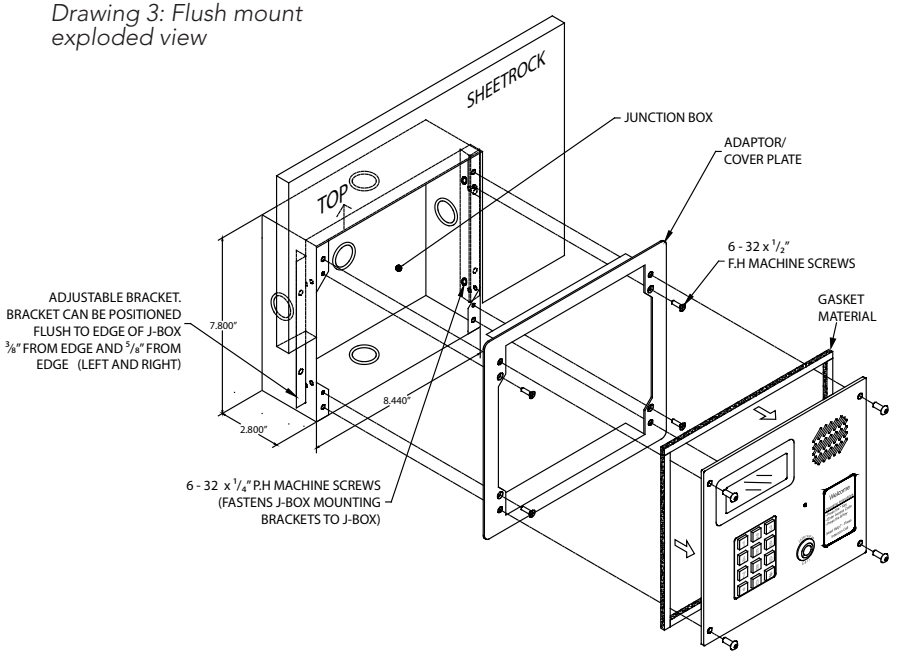
With a normal VP mount, a standing person may not be able to see the display. Mounting height varies from 42" – 58" from the finished floor to the center of the '5' button on the touchpad.

Most standard keypad installations 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.



Drawing 4: Box mount for keypad

Drawing 3: Flush mount exploded view



Gooseneck Stand Mount

A gooseneck is commonly used for driveways for vehicle access. The gooseneck 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 of a gooseneck has a hole that accepts conduit (¾" maximum) for electrical wiring. Ensure the conduit is placed properly and the wiring runs through the conduit before mounting the gooseneck stand to the concrete base. The final location of the gooseneck and the mounting techniques may be affected by local building codes.

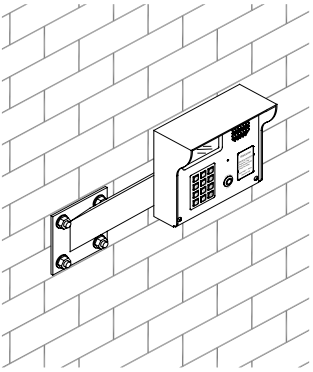
- As a precaution, the gooseneck should be protected with concrete bollards to prevent vehicles from damaging the electronics.

- There are several different styles of gooseneck stands available. See for the dimensions of two common styles in "Drawing 6: Gooseneck stand mount" on page 7.

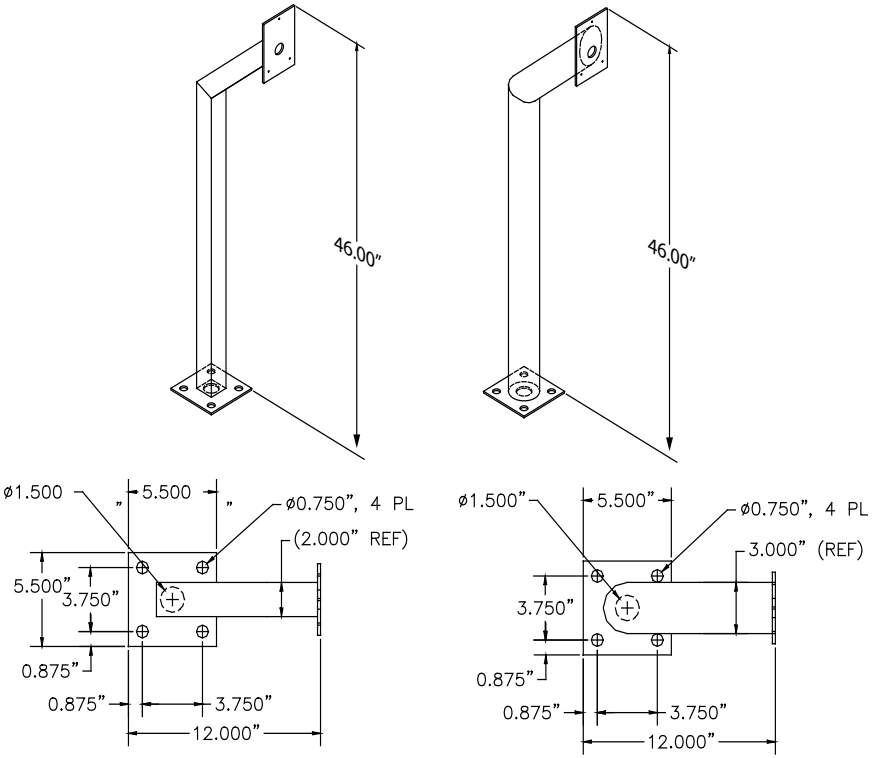
Both single and double bollards are mounted on a Schedule 40 10 3/4" diameter pipe with a .365" wall. This pipe is footed in concrete and filled 3/4 of the way with concrete to create a solid barrier. The entire pipe and bollard are then painted to match the facility. Contact PTI Security Systems for 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 ajacent to a building wall, as shown in "Drawing 9: Silicone seal for gooseneck" on page 11.



Drawing 5: Wall mount Gooseneck



Drawing 6: *Gooseneck stand mount*

The wallmount gooseneck also gives wheelchair users 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.

If the VP is installed on an exterior wall, seal the contact point between the housing and the wall with a silicone sealant rated for outdoor use. This prevents moisture and insects from getting into the housing.

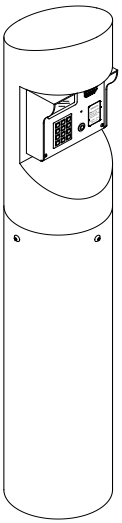
Keypad Adapter Plate

- A keypad adapter plate is an aluminum plate used to mount keypads to stands, bollards, and goosenecks manufactured by other companies.

- The installer measures, marks, and drills holes in the adapter plate to match the stand configuration. To prevent tampering, ensure the holes are countersunk on the same side as the installed screws so that the keypad covers the mounting screws.

- The screws and screwholes provided on the aluminum plate match up with the VP keyhole mounting pattern.

Single Bollard



A bollard is an attractive and functional stand for keypads. It helps protect the keypad from vehicle damage. It can be used in driveways for vehicle access or near doors as a keypad stand. Height is determined by the length of the pipe on which it is mounted.

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

Drawing 7: single bollard

Installing VP Series Keypads

Power and data communication wiring are the most important wiring component for VP devices. A VP requires power and communication lines connected to the controller.

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

PTI recommends that power and data communication be run through a **single 18 AWG, 4-conductor shielded cable.** Some installations will require larger gauge wire. See "Drawing 8: Wiring for VP keypad" on page 10 for details on connecting the wiring to the VP device.

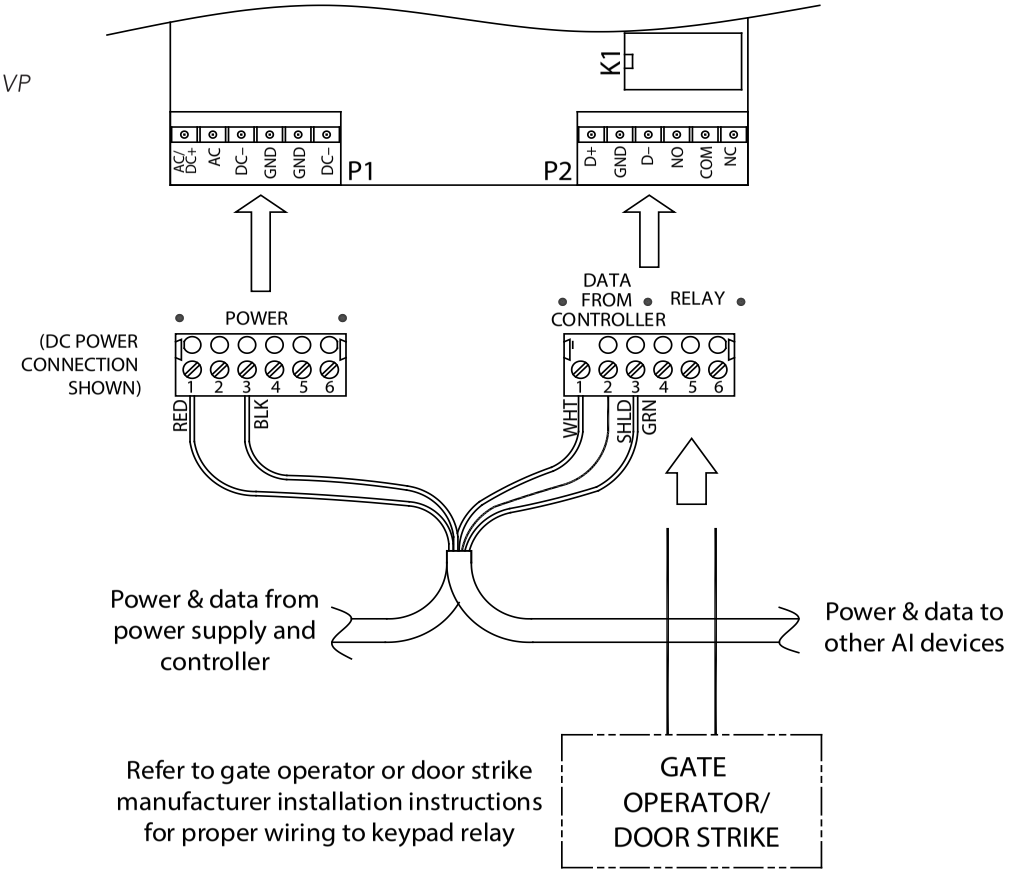
With the RS485 communication scheme, a keypad can be located as far as 4000 feet from the controller, therefore shielded twisted pair cable with ground wire is required for optimal operation. Additionally, larger gauge wire must be used the farther the device is from the controller.

Additional cables may be needed for the intercom, gate operator, door strike, presence detector, or other device.

- Use approved electrical conduit to supply the wiring to the VP.
- Local building codes determine the actual installation techniques and wiring methods.
- Only licensed contractors should install VP devices.
- Correct installation methods are critical for a trouble-free keypad. Most of the problems that emerge during use can be traced back to poor installation techniques or improper wiring.

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

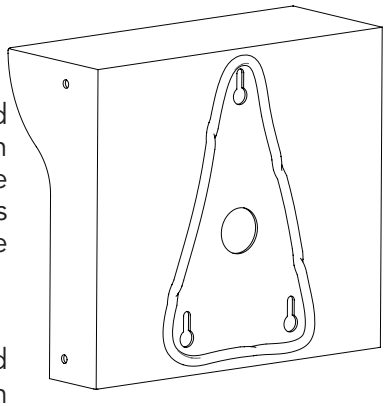
Drawing 8: Wiring for VP keypad



Installation Instructions

1 Open the device by removing the four stainless steel button head machine screws on the side 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. Seal around the back of each screw hole and around the back of the wire hole with an outdoor silicone sealant as shown in



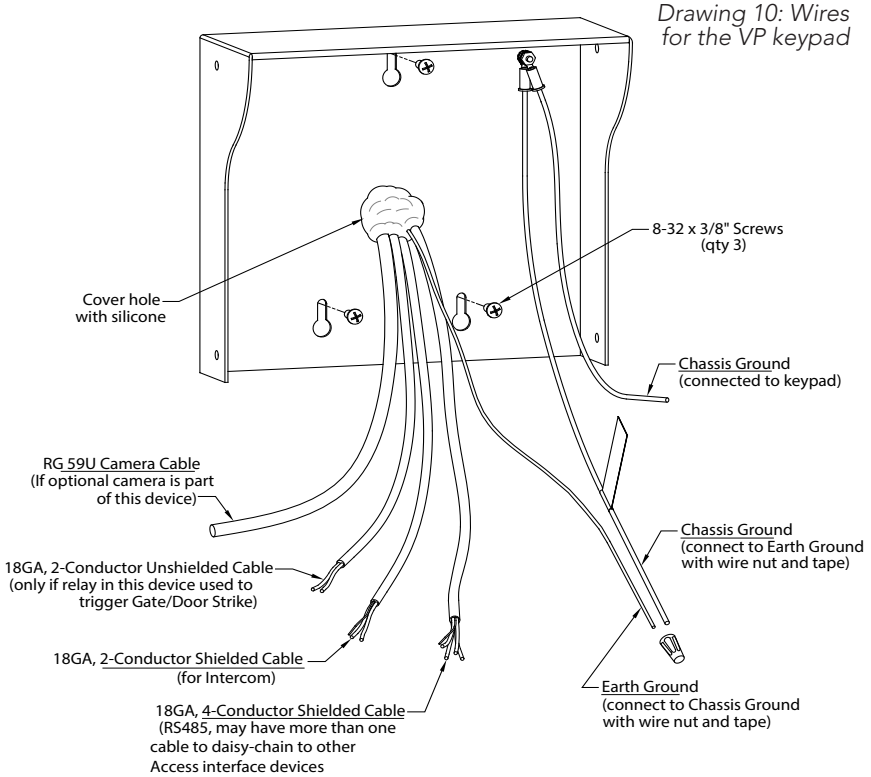
Drawing 9: Silicone seal for gooseneck

3 If the keypad is being mounted on a gooseneck or bollard, run a bead of silicone in a triangle around the three screw holes as shown in Drawing 9 on page 11:

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.

4 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 positioned inside the keypad housing for future maintenance and service. Each keypad should have the following wires as shown in “Drawing 10: Wires for the VP keypad” on page 12:

Drawing 10: Wires for the VP keypad



- One of 18 AWG, 4-conductor, shielded cable coming in from the controller or from the previous AI device in line.
- One of 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 of earth ground wire
- One or two 2 of 18 AWG, 2-conductor cable(s) coming from the gate operator or door strike.*

---

* A cable for the door strike or gate operator will only be present if the relay inside the specific keypad is used to trigger the door or gate. The controller can be configured to trigger a gate or door using relays on the circuit board, a separate relay board, or almost any other AI device.

For security reasons, the relay in the keypad used to gain access to the secured area should not be used to allow access to the area. Relays which allow access to secured areas should be in the secured area

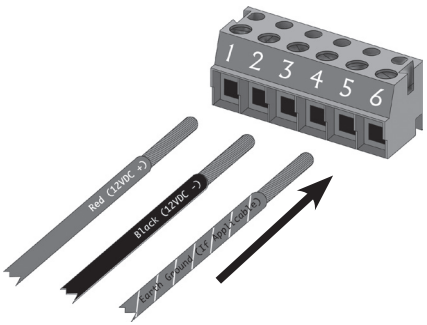
- One of 18 AWG, 2-conductor, shielded cable coming from the intercom base station if intercoms are being used.
- One of RG59U video cable if a pinhole camera is being used.
- One of 18 AWG, 2-conductor cable for the presence sensor if it is being used.

5 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.

6 Remove the terminal blocks from the keypad circuit board by sliding them up and off.

7 For **Terminal Block P1** "Drawing 11: Terminal block P1 wiring" on page 1311: Insert both **red wires** (coming in from the power supply and going out to the next AI device) into **terminal slot 1** on the first terminal block (P1).

Drawing 11: Terminal block P1 wiring



Terminal Block P1 (Left)

1. Red DC + *
2. (see footnote)
3. Black DC -
4.
5. Earth Ground if applicable
6.

* If using AC power, place the AC wires in slots 1 and 2. We recommend 12-18 VDC, but 12-18 VAC can be used.

8 Ensure that both wires are seated all the way inside the slot. Use a flathead precision screwdriver to tighten down the terminal screw.

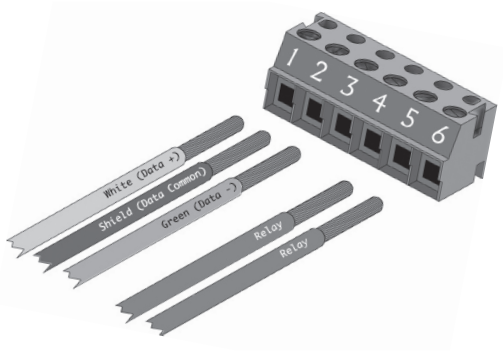
9 Verify that the terminal slot has tightened down on the copper wire and not on the rubber insulation. There should be no copper wire showing outside of the terminal slot. Gently tug the wires to verify that they are tightly held inside the terminal slot.

10 Insert both black wires into **terminal slot 3** on **P1**. Ensure that both wires are seated all the way inside the slot.

Repeat this process with each of the remaining wire connections, placing them as shown in "Drawing 11: Terminal block P1 wiring" on page 13.

11 For **Terminal block P2** "Drawing 12: Terminal block P2 wiring" on page 14. If a gate operator or door strike is being triggered directly from this keypad,use **pins 4, 5, and 6** for the relay and the wires will connect to two of these three pins.

Drawing 12: Terminal block P2 wiring



Terminal Block P2 (Right)

1. White Data +
2. Shield *
3. Green Data -
4. Relay Normally Open Wire
5. Relay Common Wire

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

12 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 normally closed and common.

An earth ground must be supplied either:

- Through the mounting of the keypad to a conductive surface with an earth ground.
- Using the earth ground wire and a proper earth ground connection.

13 The **earth ground wire** is connected in locations where the keypad is mounted on a wall that is wood, stone, or other nonconductive material. It is not always necessary when it is mounted on a grounded bollard or gooseneck.

Loose un-insulated wires (Typically used for earth ground) cannot be located inside the unit's case. Make connections for un-insulated ground wire outside the case.

14 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. In this case, **Jumper J1** should be set to **'Normal'**.

15 This installation must meet applicable code as the type of wire, depth of burial, and size of the rod may vary by municipality

16 **Connect any additional features such as an intercom, gate operator, or pinhole camera. Details are on page 16 to page 19.**

17 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.

Connecting Additional Features (not on all models)

The VP keypad may have additional features and functions. They need to be connected after steps 1 - 14.

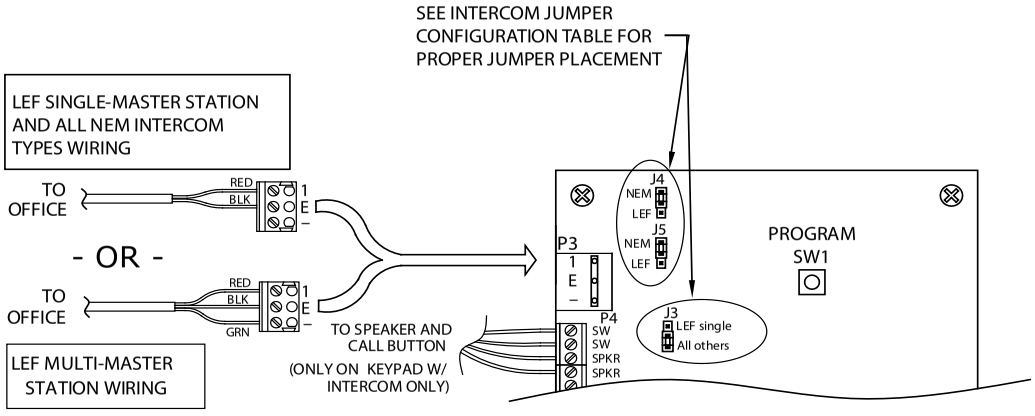
Intercom

- Connect the wires to **terminal block P3** in the upper left corner of the board as shown in "Drawing 13: Intercom wiring and jumper configuration" on page 17. 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.

The **VP with Intercom** can be connected to an **Aiphone LEF or Aiphone NEM intercom.**

- The intercom wiring must be separate from all other wiring to either keypad. Use 18 AWG, 2 or 3-conductor shielded cables for the intercom depending on the type of intercom being used. Refer to the Aiphone specifications for more detail.

- The intercom type jumpers on either keypad circuit board must be set to match the type of intercom that you are using, so reference the configuration table in Drawing 13 on page 17.



Drawing 13: Intercom wiring and jumper configuration

INTERCOM JUMPER CONFIGURATION TABLE			
INTERCOM TYPE	VP JUMPER CONFIGURATION		
NEM (ALL)	J4 NEM LEF	J5 NEM LEF	J3 LEF Single All Others
LEF (ALL BUT SINGLE MASTER STATION)	J4 NEM LEF	J5 NEM LEF	J3 LEF Single All Others
LEF (SINGLE MASTER STATION)	J4 NEM LEF	J5 NEM LEF	J3 LEF Single All Others

Gate Operators

- Most electric gate operators require a **'normally open'** contact **(pins 4 & 5)**. Some electric door strikes require a **'normally closed'** contact **(pins 5 & 6)**.
- If door strikes are used it is recommended that they be 12V DC.
- Install a shunting diode across the solenoid to prevent ground spikes from disrupting the keypad communication.

Do not place a diode across AC strikes as it will short out the power supply for the strike.

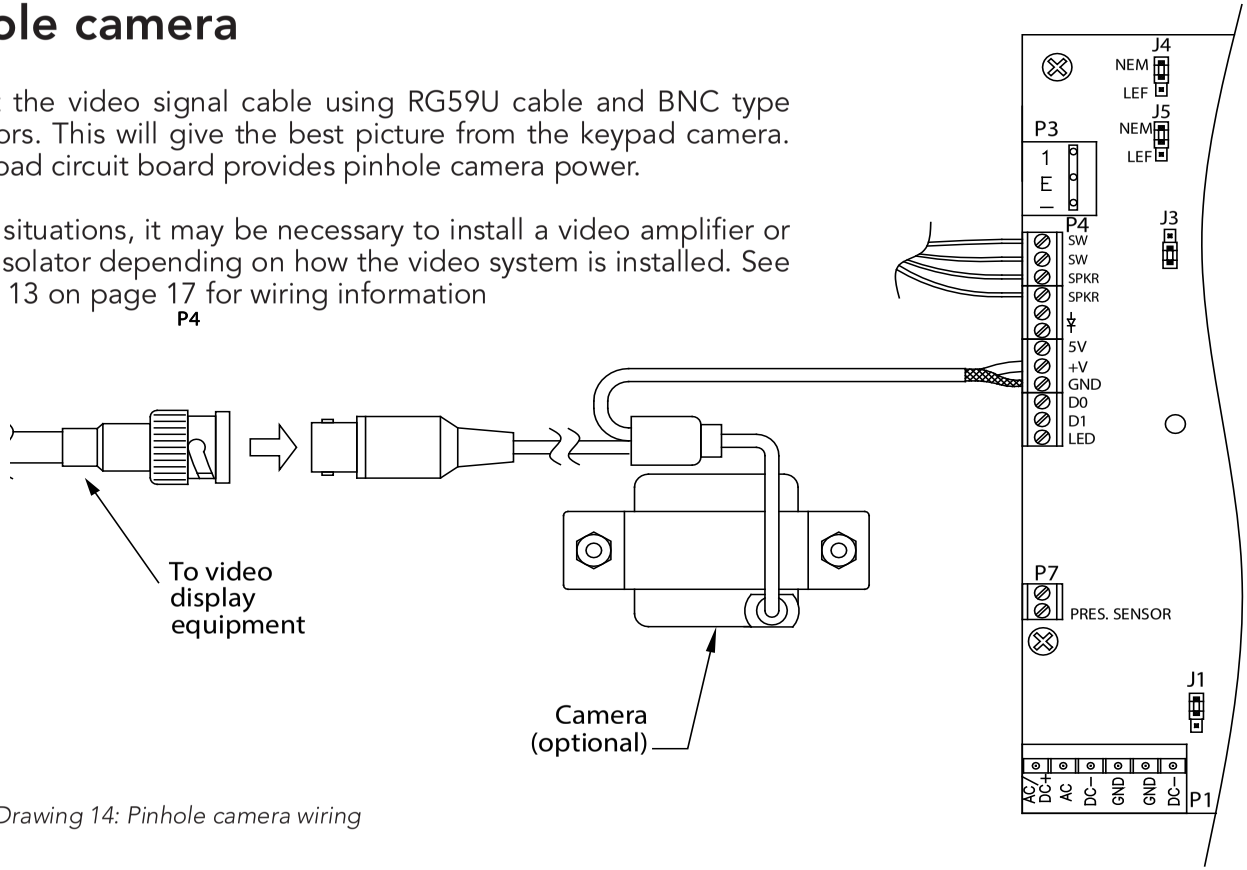
- The VP has a presence sensor function that allows the keypad to be connected to a loop detector, or pressure mat requiring a 'presence' in order to use the keypad. This function prevent users from walking to, and using, the keypad in a driveway area where they may be in danger from vehicles or the gate.
- This function is often used in connection with a gate operator and loop detector. Loop detector output wires are connected to **terminal block P7** in the keypad. The keypad is then programmed with the `Presence Required 'ON'`. see 'Setup Functions' on page 26 for information on setting up this feature.
- Do not connect a gate operator or door strike to a keypad located directly outside the area it secures. This improves security by preventing someone from vandalizing the keypad to gain access to your site.

Check the voltage level!
Relay voltage must not exceed 30 volts.
Wiring the relay to the operating device introduces the operating device control voltage into the keypad housing.
The VP is not designed for the presence of high voltage inside the keypad case.

Pinhole camera

Connect the video signal cable using RG59U cable and BNC type connectors. This will give the best picture from the keypad camera. The keypad circuit board provides pinhole camera power.

In some situations, it may be necessary to install a video amplifier or a video isolator depending on how the video system is installed. See Drawing 13 on page 17 for wiring information



Drawing 14: Pinhole camera wiring

Testing the Keypad

1 Test the display by supplying power to the keypad.

- The default date and time should appear on the display. If the controller is configured correctly, it will update the date and time on the keypad display automatically. The controller updates the date and time once-a-minute.

2 To verify that the backlight is working:

- Press the * key. The backlight should light up and the display will read `Please Enter Access Code.`
- If no keys are pressed within 10 seconds, the display will return to the `Date/Time` and the backlight will shut off.

3 To test touch pad operation:

- Press the * key. When the display shows `Please Enter Access Code`, press `0, 1, 2, 3, 4, 5, 6, 7, 8, 9`. Each digit should appear on the display as it is pressed (if Secure Entry is enabled an `X` for each digit appears)
- Press 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.

4 Test for communications with the controller

- Power up 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.

5 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 the keypad display `Please Wait` then returns to `12:00` (the power-up default time), recheck the wiring, baud rate settings, and address settings. Also ensure that the controller is set to the correct number of remotes.

Operation

VP Keypad Setup Function

To enter setup mode:

> To enter setup mode:
> 1. Press the *, 0 and # simultaneously
> 2. Enter the factory password 8898
> 3. Press the # key

In the event the password is changed and then forgotten, you can disconnect power from the keypad 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 also be prompted to Restore Factory Defaults. Select yes to restore all default factory settings including the password.

> Press the # key to advance through each setup parameter.
>
> A parameter is automatically saved when you press # and move to the next parameter.
>
> A time-out is built into the system that will exit Setup mode if there is no input on the keypad for an extended period of time
>
> If a time-out occurs, 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 two (2) ways to exit Setup mode:
> - Press the 7, 8, and 9 keys simultaneously
> - Go through all of the setup functions

Setup Parameters/Functions

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

```
Restore Defaults
*=Yes #=No
```

This prompt only occurs if the program button is held while powering the 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.

```
Setup Menus
*=chng #=next
```

Identifies how to use the keys: the * key is used to change a parameter and the # key is the enter key to move to the next menu.

```
Current Add: 001
New (1-127):
```

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. Factory default is 1.

```
* to Change Baud:
9600
```

The controller communications baud rate. Scroll through the list of available rates by pressing the * key. Factory default is 9600.

Optional Setup Functions

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.

```
Setup Password
* =Change #=No
```

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 changes, if both entries match, the password will be changed. Otherwise, a message will indicate that the passwords do not match.

```
Tamper Switch:
   Disabled
```

Controls the use of the tamper sensor. 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 Entry
   Disabled
```

Controls the characters displayed during code entry. When set to Enabled, the display will show only an X for each key pressed. When set to Disabled, the numbers pressed will be echoed to the display. Factory default is Disabled.

```
Beep with Key
   Enabled
```

Controls the internal buzzer used to provide audio feedback for any key press. When set to Enabled, the buzzer will produce a short beep when a key is depressed. When set to Disabled, the buzzer will not sound with key presses. Factory default is Enabled.

Beep with Access Enabled

Causes the internal buzzer to sound when an access is granted. 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 Enabled.

Beep with Alarm Disabled

Controls the internal buzzer used to provide audible feedback when a system alarm occurs. When set to Enabled, the internal buzzer will sound whenever an alarm occurs and remain on until the alarm resets from the controller. When set to Disabled, the internal alarm buzzer will not sound with an alarm event. Factory default is Disabled.

Language XX.XX English

Language display for user messages. There are eight options — English, French, Spanish, Italian, German, Danish, Dutch, and Norwegian. This affects the user messages and the setup functions. The XX.XX denotes the revision of the language firmware. Factory default is English.

Date Format US

Controls the date display on screen. Options are US and European. US format displays MM/DD/YY. European displays DD/MM/YY. Factory default is US.

```
Time Format
12 Hour
```

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 11:59:59 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. Factory default of 12-hour.

```
Max. #Attempts:00
(0-10,0=off):
```

Sets the maximum number of attempts within a one minute period before the keypad prevents further code entry — e.g. if the number is set to 3, 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 continues to press keys the lockout time will continue to be reset.. The maximum number of attempts is 10. Use 000 to disable the lockout feature. The factory default is 000.

```
Presence In Req.
Disabled
```

Used where a vehicle sensor is installed in a drive or other traffic area. When this feature is Enabled, a presence must be detected before a code or card can be used (usually by a loop in the ground under the driveway). This feature can also be used with an alternate alarm system. Factory default is Disabled

```
Card Format
26 Bit
```

Set the format of the cards being used for access — options are 26, 30, 31, and 34 Bits. See the card manufacturer specifications to determine the Bits of the card. Factory default is 26 Bit.

```
Trip Relay NoCom
    Disabled
```

After any code has been entered the display will read `Access Granted` and the relay will be tripped to allow access. When `Enabled`, the keypad will allow the relay to be triggered when the communications are offline. **Enabling this setting compromises site security.** Factory default is Disabled.

```
Com Off Time:005
  (1-25 sec):
```

Sets the amount of time the keypad should wait before deciding it has lost communication with the controller. Any value from 1 to 25 seconds can be entered. Factory default is 5 seconds.

```
Setup Complete
  Press # key
```

Message displayed when exiting 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 standard display message for the VP keypad when no keys have been pressed is the date and time as shown.

```
Fri,  08 / 01 / 08
      12 : 13  PM
```

Depending on how the system is configured, the user will have an access code to enter, or a magnetic stripe card to swipe. When the user approaches the keypad, the standard display message will be shown on the display.

The display and keypad are backlit at a low level to conserve power when the device is not in use. This low level of light is sufficient to read the display at night. As soon as a customer presses the * key, the display returns to full brightness.

Access Codes and Cards

To enter an access code, the user presses *. The following message will be displayed.

```
* PLEASE ENTER *
  ACCESS CODE
```

The user enters their access code using the touch pad and presses the # key. The keypad sends the code to the controller and waits for a response while the keypad goes through the security checks described in "Security Checks" on page 29 . The message on the display changes to the following while waiting for a response.

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

To use magnetic stripe cards, the user swipes their card through the slot in the card reader. The magnetic stripe on the card must be aligned to pass through the slot facing the left side of the reader.

If the unit is not able to read the card correctly through the slot, or if there is an error on the card, the following message will be displayed:

```
Sorry -
Try Card Again
```

When the card is read, the keypad will go through the security checks described in "Security Checks" on page 29. If all security checks pass, the keypad sends the card data to the controller and waits for a response. The message on the display will change to the following while waiting for a response.

```
* PLEASE WAIT *
```

When the keypad receives a response from the controller it will display the response message. The messages received from the controller vary depending on the type of response. The various response messages are shown in the Access Response Messages section.

Security Checks

The VP performs a series of security checks 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.

Communications Check — the first item checked is communications between the units on site and the controller. When the keypad is not communicating with the controller and the `Trip Relay NoComm` is disabled, the unit will display the following message and revert back to the date and time.

```
* PLEASE WAIT *
```

Tamper Check — the VP performs a tamper check to see if the tamper switch has been enabled. If it is enabled, the VP checks that the switch is secure.

If either condition is true or the tamper is disabled, the VP will proceed to the next security check. If the VP detects tampering, it will display the following message and no further access attempts will be allowed.

```
Sorry -
Tamper Lockout
```

Presence Required Check — After checking the tamper, the VP will check to see if the `Presence is Req` option has been selected. If it has been selected, the VP 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 keypad will continue with the next security check. If the VP does not detect a required presence, it will display the following message and no further access attempts will be allowed.

```
Sorry -
No Presence Det
```

Maximum Attempts Check — The maximum attempts check is designed to discourage a user from entering random numbers to enter the site. If the `Max #Attempts` feature is set to a value between 1-10, the VP will check to see if the user has tried a code more than the permitted number of times. If not, the VP will allow the user to enter an access code.

If a user exceeds the maximum number of unsuccessful attempts, the VP displays the following message and disables any further access. The VP will not allow any further attempts for 60 seconds since the last keystroke. If a key is pressed while this message is displayed, the 60 second timer resets and begins again.

```
Sorry….
* See Manager *
```

Trip Relay Offline Check — After the customer has entered their code, the VP checks to see if the `Trip Relay NoCom` option has been enabled. If it has been enabled and the keypad is not in communication with the controller, then the VP will display the following message and further access attempts will be allowed.

```
Access Granted
```

Access Response Messages

There are several standard messages built in to the VP. The types of messages the VP receives 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 *
Entry Is Granted
```

For a valid Exit:

```
* Thank You *
Exit is Granted
```

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

```
Sorry -
Area Closed
```

When the customer is not authorized to enter an area:

```
Sorry -
Area Denied
```

When the customer's code has expired:

```
Sorry -
Code Expired
```

When the customer's card has expired:

```
Sorry -
Card Expired
```

When the customer has been suspended:

```
Sorry -
Access Suspended
```

When the code the customer entered is not valid:

```
Sorry -
Access Denied
```

When the card the customer used is not valid or not read properly:

```
Sorry -
Try Card Again
```

System Maintenance

The VP keypad requires a minimal amount of maintenance. However, as with any electronic or mechanical device that is used regularly, a small amount of maintenance done periodically will extend the life of the product.

Periodic Visual Inspection

The VP 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 keypad mounts to the gooseneck stand or wall

Periodic Cleaning

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

Cleaning the Housing and Touch pad

Inspect and clean the housing and touch pad at least twice per year.

✓ To clean the housing, spray the unit with a mild household cleaner then wipe it with a soft cloth.

✗ Do not use harsh chemicals, abrasives, or petroleum-based products as they can damage the finish on the device.

✗ 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 touch pad.

Remove the VP from the housing to inspect and clean the inside of the unit. When inspecting the inside of the housing and the VP, 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.

✓ A small can of compressed air can be used to remove insects and dust from the circuit board.

✗ **Do not use cleaners of any kind**, including water, to clean inside the housing or on the circuit board.

Cleaning the Magnetic Stripe Reader

The VP is shipped with a cleaning card for the magnetic stripe reader (if installed). The cleaning card is a small, credit-card sized plastic card with a special cleaning surface on one side that is saturated with a cleaning solution.

To clean the reader, swipe the cleaning card several times through the slot in the reader and dispose of the card after use. Additional cards can be ordered from PTI Security Systems. Always keep a supply of cards on hand.

Troubleshooting

For a new installation, typical problems 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 installation (previously working), 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.

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

1 Does the VP Access Device have Power?

Check the display of the VP. 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 & 3, (or P1 pins 1 & 2 if using AC power)

Yes – Proceed to step 2

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

2 Is the voltage at the VP, connector P1 pins 1 & 3 (1 & 2 for AC), greater than 12 Volts? (Use a volt meter to measure the voltage).

Yes – Proceed to step 3

No – Check Power Supply and Wiring and retest

3 **Is the voltage at the VP, connector P1 pins 1 & 3 (1 & 2 for AC), greater than 18 Volts? (Use a volt meter to measure the voltage).**

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.

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

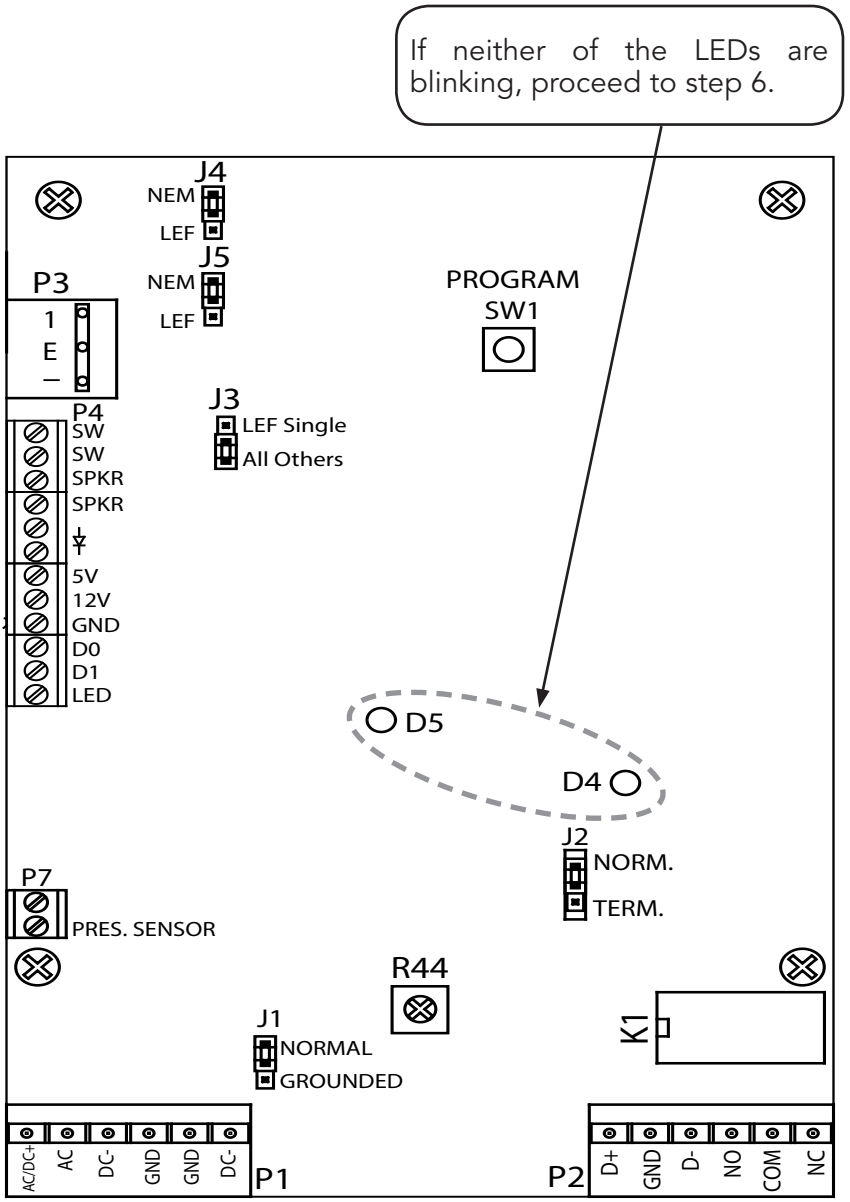
No – Proceed to step 4

4 **Is the VP communicating with the controller and software?**

Check the LEDs on the VP board or run the `Health Check report` in StorLogix.
When the VP is communicating with the controller, LEDs D4 and D5 will be blinking. See "Drawing 15: VP board diagram" on page 38 for the location of the LEDs.

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

No – Check wiring and proceed to step 5



Drawing 15: VP board diagram

5 Are any other devices set to the same address as the VP?

In Falcon 2000 - look at `Remote Online Status report`

In Storlogic ver.4.1 - look at `AI device current status`.

In Storlogic ver.5.0 - look at `Health Check`

Check the addresses on all of the devices, or disconnect the VP and run the report for your software version listed above. If the system setup report shows the remote number (address) assigned to the VP as being ON LINE with the VP disconnected, then another device is sharing the same address.

Yes – Change one of the devices and retest

No – Proceed to the step 6

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

In Falcon 2000 - look at `Falcon Setup`

In Storlogic ver.4.1 - look at `Falcon XT Setup`.

In Storlogic ver.5.0 - look at `Falcon XT Setup`

If the value is lower than the address of the VP, the controller will not try to communicate with it.

Yes – Change the maximum number of remotes and retest

No – Contact Technical Support if the VP is still not working.

Test Individual Devices, Card and Code Input

Use the following steps for troubleshooting individual devices or keypads. 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.

Try a code or card at the keypad controlling the gate. Ensure the code or card is one that works at that location and time. Try several codes to verify operation. Note which code(s) were used and the response at each device, as well as the response on the software event log.

↓

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.

↓

If only one device is not working, determine if the problem is in the device or the location. Make sure to allow for customer access, then remove the faulty device. Switch the faulty device with a similar device that works and remember to switch addresses too. If the problem remains in the same location, it is probably a wiring issue. Contact a service company to check the wiring.

↓

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 multiple devices or entire site

Generally, multiple problems are a sign of wiring issues, 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:

Allow for customer access and open all device housings.

↓

Unplug the power and data terminal blocks on every AI device on the site.

↓

Once every device on the site is unplugged, add one device at a time back into the system.

↓

Allow the device to function for an hour and then add in the next device in line.

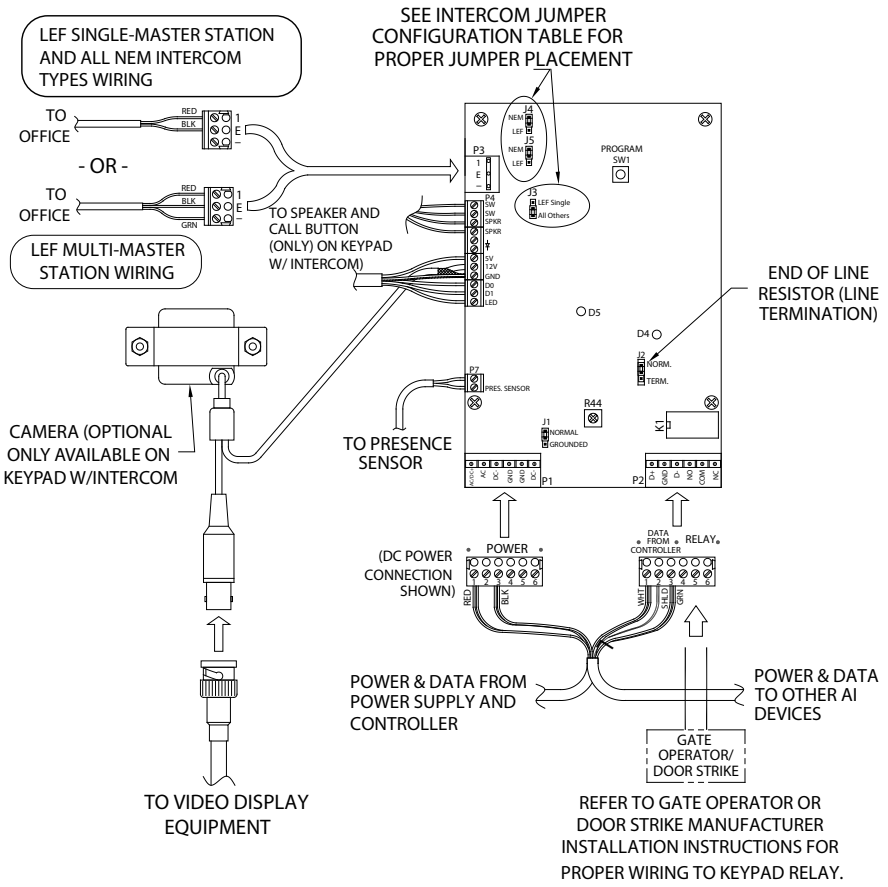
↓

Eventually, a device will be added that triggers the problem. Switch this device with one that has been previously added to verify if the problem exists in the location or in the device.

↓

If the problem stays in the same location, it is probably a wiring issue. Contact a service company to check the wiring.

Drawing 16: : Wiring Diagram of VP Keypad System



WIEGAND READER WIRING TABLE	
FROM (WIEGAND)	TO (P4 ON KEYPAD)
+DC (RED)	5V
DATA0 (GRN)	D0
DATA1 (WHT)	D1
LED (ORN)	LED
GROUND (BLK)	GND
SHIELD GND (SHIELD)	

INTERCOM JUMPER CONFIGURATION TABLE			
INTERCOM TYPE	JUMPER CONFIGURATION		
NEM (ALL)	**J4** NEM / LEF	**J5** NEM / LEF	**J3** LEF Single / All Others
LEF (ALL BUT SINGLE MASTER STATION)	**J4** NEM / LEF	**J5** NEM / LEF	**J3** LEF Single / All Others
LEF (SINGLE MASTER STATION)	**J4** NEM / LEF	**J5** NEM / LEF	**J3** LEF Single / 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 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 breach 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. This warranty does not cover the replacement of batteries that are used to power PTI Security Systems 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 ensure 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

PTI SECURITY SYSTEMS


SECURITY


ACCESS


CONTROL


VIDEO

For Technical Support, Please Visit:

tickets.ptisecurity.com

114A3868 revision.E- July 2017