API KEYPAD
USER MANUAL

2024

PTI SECURITY SYSTEMS

ASSA ABLOY

VER 08012025

API KEYPAD

User Manual

TABLE OF CONTENTS

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 when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

AP1 KEYPAD

User Manual

Sales: +1.800.523.9504
Support: +1.866.240.7602
Web: ptisecurity.com

Rev J – October 2025

INTRODUCTION

The AP1 (Access Point 1) is a PTI RS485 peripheral used for access control at a gate or door. This document is intended to provide a high level overview of how to operate the the unit. For additional information, please contact PTI Support.

It includes:

- OLED graphic display with customization capability
- 12 key tamper resistant touchpad with RGB backlit keys and an optional integrated heater
- Bluetooth Low Energy integration to the Easy Code Mobile application
- Two supervised inputs for door and gate monitoring or request to exit controls.
- Two relays for door and gate control.
- An RS485 Interface with 2500 Volts of isolation and state of the art surge protection.
- State of the art power input surge protection with isolated power.
- Integrated voltmeter for monitoring input power.
- Wide DC input voltage range that allows for 24V battery backed supplies. This results in lower IR cable loss resulting in much longer power supply to device cable lengths.
- One piece enclosure with hinge for easy servicing.
- Two screws secure enclosure. Screws are captive and cannot be lost.
- High quality, elevator style terminal blocks ensure reliable connections.
- Dual mode tamper detection for security and reliability.
- Remote firmware update capability
- Remote configuration capability (pending system implementation)

Electrical Specifications*:

Input Voltage:	12 to 18VDC supplied by a Class 2 current limited source
Power Consumption:	300mA maximum (does not include keypad heater)
Communication:	2-wire RS485 at 9600 baud
Inputs:	2 with optional supervision using 1K resistors in series, parallel or both.
Outputs:	2 relays rated at 2 A @ 30 Vdc resistive
Operating Temperature:	-40 to +85 C (-40 to 185F)
Humidity:	95% relative humidty
Ingress Protection	IP55 – requires proper mounting
Heater (optional)	Requires a 12 - 14 volt, 1.5 Amp supply

Regulatory:

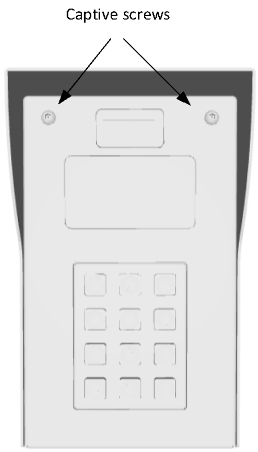
Bluetooth SIG	Declaration ID: D067838
FCC ID	2BFJY-1000239 2BFJY-1000260
UL294	ETL US and Canada: Report # 2002292, conforms to UL STD 294; and certified to CAN/ULC 60839-11-1
IC ID	Non-heated AP1: 32223-1000239 Heated AP1: 32223-1000260
CE	EN 55032 (2015 and A11 2020), AS/NZS CISPR 32, CISPR 32, EN 55035 (2017 +A11 2020), ETSI EG 203 367 V1.1.1, ETSI EN 300 328 V2.2.2), EN 61000-3-2, EN 50130-4 (2011/A1:2014), ETSI EN 301 489-17 V3.2.4 (2020-09)

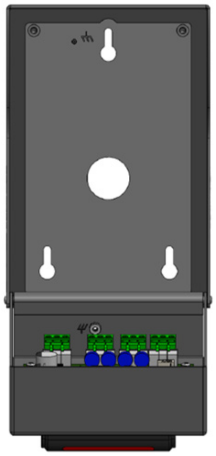
**Specifications subject to change without notice*

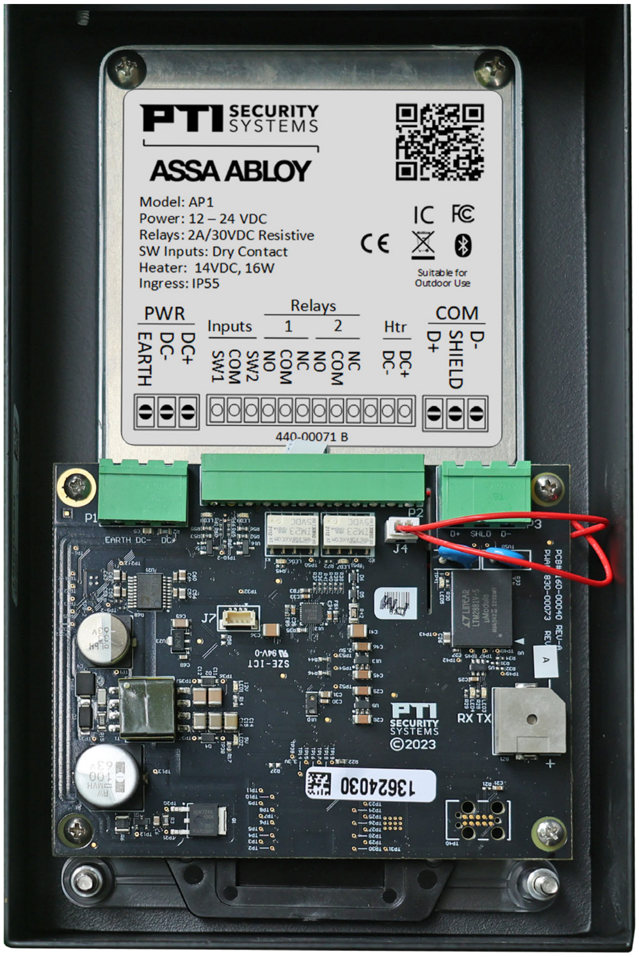
How to Open and Close the AP1

The AP1 is held closed with two captive screws at the top and a hinge at the bottom. Use a TORX T15 bit to loosen the two captive screws and the top front of the AP1. When loosening or tightening the screws it will be necessary to alternate between the two to prevent binding.

NOTE: If the sides of the back housing get compressed, as can happen with handling or mounting, the two halves will interfere when opening or closing. Bending out the sides just below the visor will remedy.



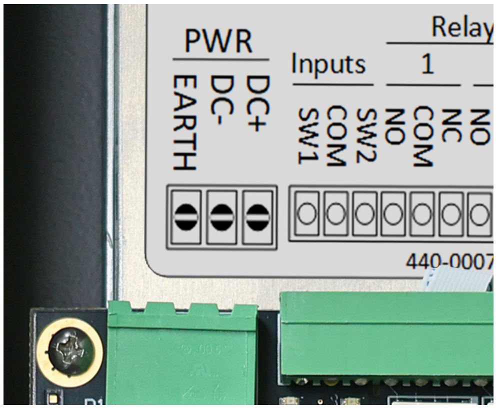




Board Connections and LEDs

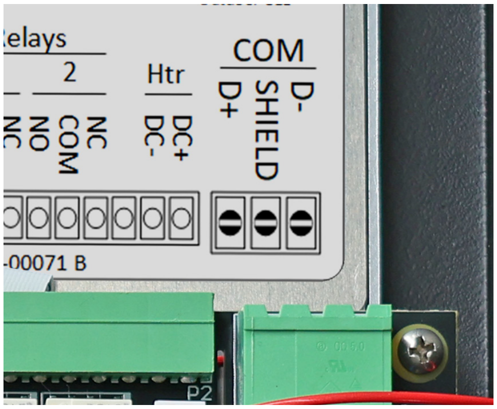
Connectors

Earth Ground
DC-
DC+
Connect to a DC power source of 12 to 48 volts. AC input is NOT supported. A Class 2 current limit supply must be used.



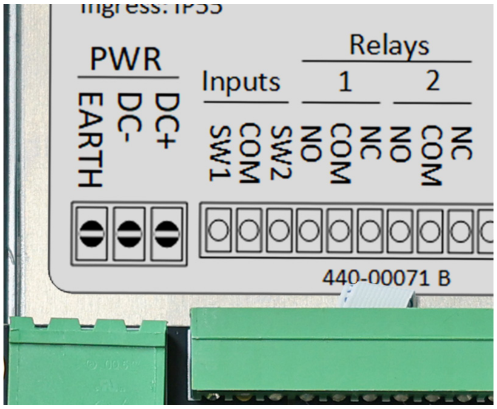
D+ / 'A'
GND / Shield Connection
D- / 'B'

Connect to system controller RS485 connection. Communications are electrically isolated therefore, the GND / Shield connection should only be connected to the GND / Shield connection of other peripherals or the system controller. Optionally, it can be connected to a suitable earth ground.

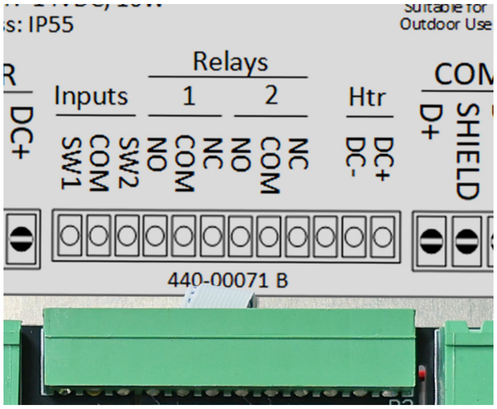


SW1
Common
SW2

Can be used for built in door controls or simply report their state to the controller. A dry contact switch connects between SW1 and COM or SW2 and COM. Supervised switches can be used to detect tampering (wire to switch is cut or shorted).



The LEDs just below the SW1 and SW2 input contacts indicate the switch state:
Off – Open
On – Closed
Flashing – Tampered



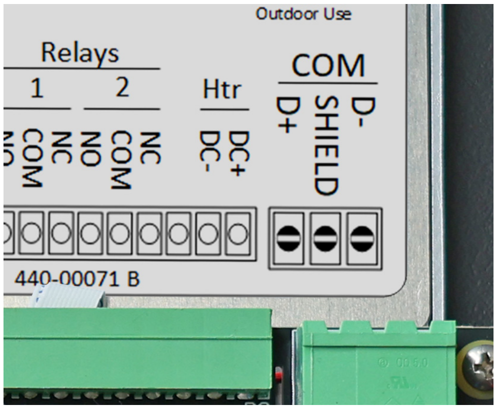
Relay 1 / Relay 2

NO – Normally Open
COM – Common
NC – Normally Closed

Relay 1 controls the door strike, mag lock or gate trigger. Connection between the NO and COM contacts is made when active. It is activated whenever the AP1 grants access.

Relay 2's function is determined by the AP1's configuration setting. It can be set to function as an alarm output, slave to relay 1, slave to relay on with different on time, a heater controller (active when freezing temperatures occur) or activated only by the system controller.

The LEDs below the relays will light when the relay is active



Heater (if purchased)
Heater Power Connections

JMP – Connect this terminal to Relay 2 COM using insulated 18 AWG wire.
DC- - Heater negative power supply connection
DC+ - Heater positive power supply connection

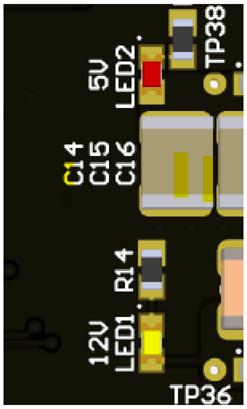
The connections are only used if an optional heater is installed in the AP1. Heater power connections are separate from the AP1 power connections. Relay 2 is used to control the heater. Connector J4 connects to the optional heater incorporated into the 12 key touch-pad. A 2AMP power supply is recommended when the optional heater is used with the keypad.

See APPENDIX to compute if an additional power supply is needed to support the optional heater.

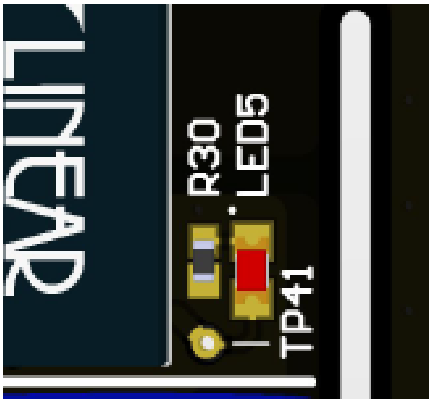
LEDs

Power Supplies

The red and green LEDs indicate the status of the internal 5V and 12V power supplies. Failure of these LEDs to light when power is supplied to the AP1 would indicate a fault or failure condition.

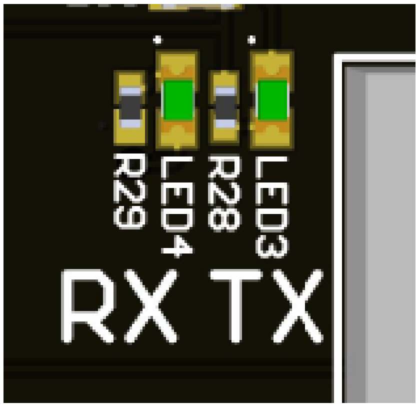


Red LED5 indicates the status or the isolated RS485 power supply. Failure of this LED to light when power is supplied to the AP1 would indicate a fault or failure condition.



RS485 Communication

The LEDs above the RX and TX silkscreen indicate the status of the RS485 network. The RX led will light when the network is being driven by the system controller. The TX light will light when the AP1 is driving the network.



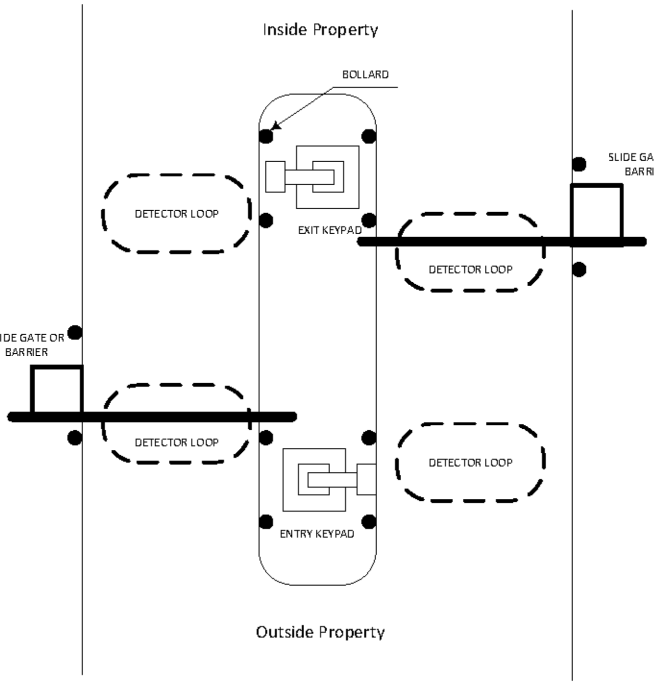
The RX light will be flashing when the AP1 is powered and properly connected to the system controller.

The TX light will flash when the AP1 is responding to a message successfully received from the system controller. A flashing TX light will typically indicate communication between the system controller and AP1 has been established.

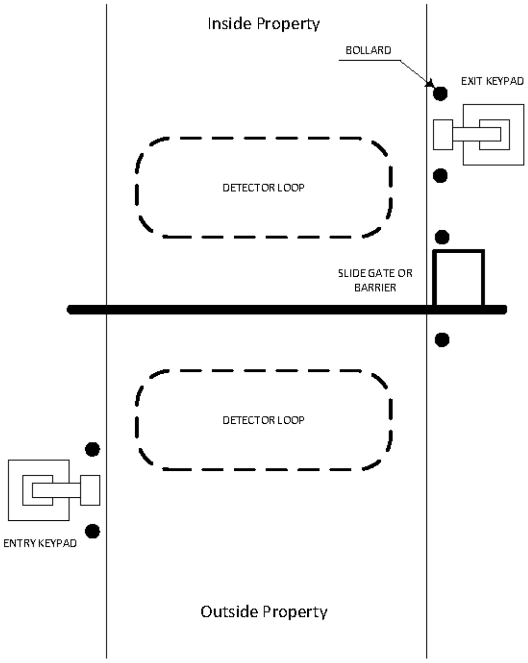
Typical Applications

Before installing the keypad, 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 the vehicle's driver door. If the keypad is being used for walk up access, install it where it can be accessed by a person on foot.

Island Scenario



Single Lane Scenario



When positioning the keypad for drive up accessibility, it must be mounted with easy reach of the driver of an automobile or light truck when considering the touchpad being used for access. Most of these locations use gooseneck stands or keypad bollards with cap 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 and shows suitable mounting locations when used for vehicle access.

Walk Up Accessibility

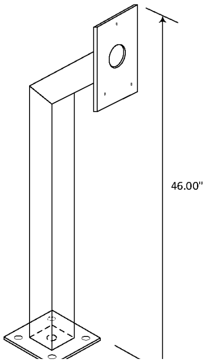
When positioning the keypad for walk up accessibility, it can be mounted on a stand or attached to a wall. It can also be surface mounted so that it protrudes from the wall.
Mounting Keypad

Mounting height varies with the application and it can be installed on a gooseneck stand, keypad bollard, or to a wall.

Gooseneck Stand Mount

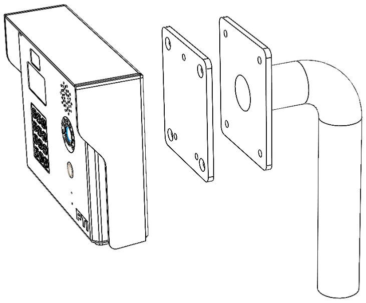
Gooseneck stands are commonly used for vehicle drive aisles but can also be used near doors for wheelchair access or when sidewalks and landscaping require.

- The base plate of the gooseneck has a hole that accepts the conduit (3/4” maximum) for 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 filled bollards to prevent vehicles from damaging the keypad.
- There are several different styles of gooseneck stands available.



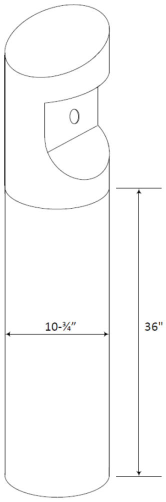
For a standard gooseneck, some holes might differ from the standard hole pattern used by PTI. Therefore, an adapter plate can be used. The adapter plate can be obtained by calling PTI sales. To install the adapter plate, add the plate between the gooseneck and keypad.

➡ **NOTE: Drilling into the back of the keypad will void warranty.**



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 are usually filled with concrete and used as the barrier to protect the keypads.
- 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 an dfilled ¾ of the way with concrete to create a solid barrier.



PTI recommends that power and data communication be run through a single 18AWG, 4-conductor shielded cable. Some installations will require larger gauge wire.

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

Additional Cables may be needed for the gate operator, door strike or other devices.

- Use approved electrical conduit to supply the wiring to the keypad.
- Local building codes determine the actual installation techniques and wiring methods.
- Only licensed contrators should install these 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.

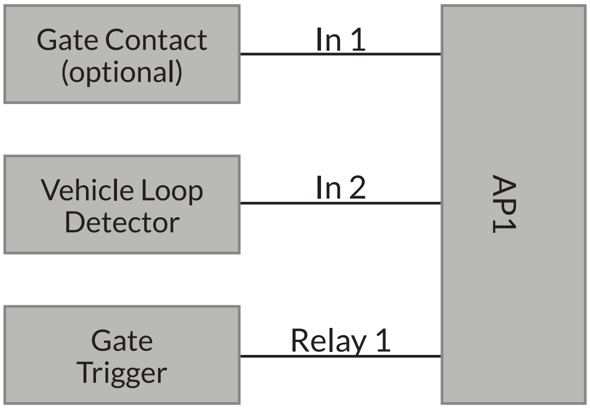
All installations must conform to local building and electrical codes. When discrepancies exist between local codes and this manual, local code takes precedence.

Single Keypad Gate Access

In this application a single keypad is used to control ingress into the facility. A loop detector is used for egress connected to Input 2. Relay 1 is used to trigger the gate.

Optionally, input 1 can be used to monitor the gate.

In this application Inputs 1 and 2 should be set for monitoring door or gate and RTE respectively.



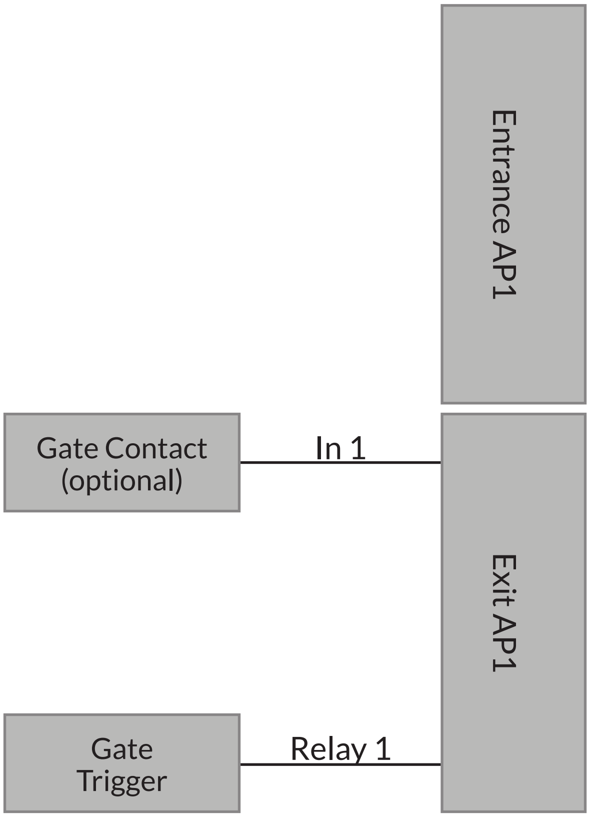
Dual Keypad / Maximum Security Gate Access

This application is for gate access with maximum security. The gate is only triggered from Relay 1 of the Exit keypad. Opening the entrance keypad will not allow access to the gate control.

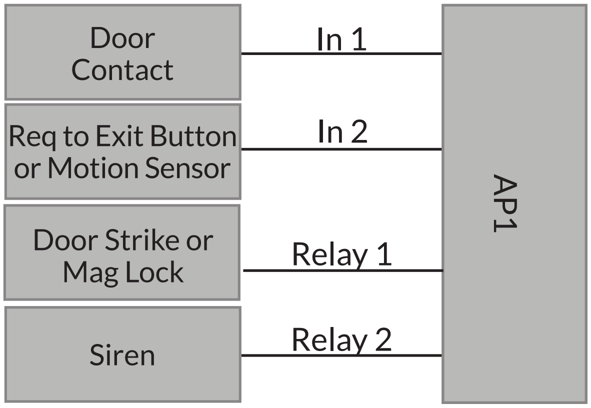
The controller must activate the relay on the exit AP1 for ingress into the facility.

Optionally, input 1 can be used to monitor the gate.

In this application Input 1 of the Exit AP1 should be set for monitoring door or gate.



Door Control and Monitoring

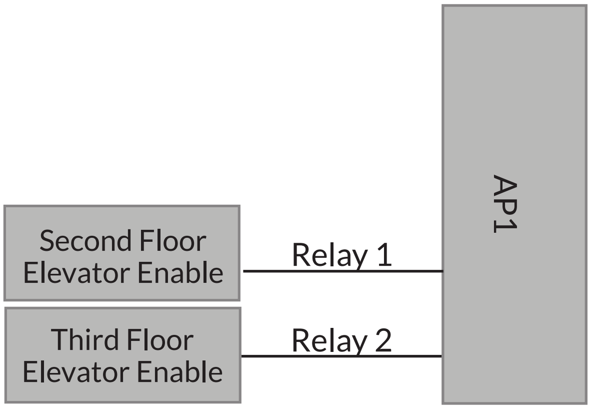


This application is used to control and monitor a door. Events, which can trigger alarms, will be created when the door is forced open or held open past the specified limit.

Relay 2 can be left unused or can be used to drive a siren.

In this application Inputs 1 and 2 should be set for monitoring door or gate and RTE respectively.

Two Floor Elevator Control

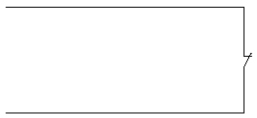
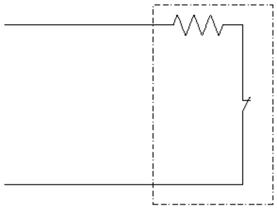
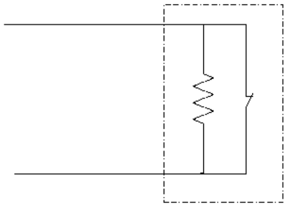
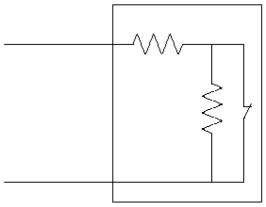


In this application the AP1 is used to control access to two floors by using the relays to enable the floor button. The keypad can be mounted inside the elevator cab.

Elevator access functionality must be implemented in the system controller.

Input Switch Supervision

The AP1 has the capability to monitor the two inputs for tampering. This is accomplished by using supervised switches. Supervised switches incorporate 1K ohm resistors securely located inside the switch housing.

Supervision Type	Diagram	Description
Unsupervised		An unsupervised configuration is shown to the left. There is no supervision resistor. In this configuration the controller detects no difference in a cut wire or open switch or a shorted wire or closed switch. A switch configured as unsupervised will not produce a tamper event for its input as it has no means of knowing that tampering has occurred.
Series Supervised		A Series Supervised configuration includes a 1K ohm resistor in series with the switch. In this configuration, a short in the wires can be detected and tamper event produced. A cut or open will not be seen any differently that an open switch contact, therefore this configuration only provides protection for normally open switches.
Parallel Supervised		A Parallel Supervise configuration includes a resistor in parallel with the switch. In this configuration, an open can be detected and produce a tamper event. A short will not be seen by the controller any differently than a closed switch contact, therefore this configuration only provides protection for normally closed switches.
Dual Supervised		A Series / Parallel supervised configuration includes a 1K resistor in parallel and a 1K resistor in series with the switch. This configuration can detect both opens and shorts in the wires which connect to the switch and will produce tamper events as a result. This configuration provides protection for both normally open and normally closed switches.

Configuration

The configuration menu is accessible by pressing the '*', '0' and '#' keys simultaneously. A '>' prompt will appear. Enter the password to enter configuration mode. The default password is "8898". After entering the correct password an "ok >" prompt will appear. If an incorrect password or command is entered a "? >" prompt will appear.

Note: As with any default password, in order to provide a secure installation, it must be changed. This can be accomplished in the configuration menu.

In configuration mode, commands consist of one, typically two digits followed by the '#" key.

Commands are grouped by most significant digit as shown below. Any command ending in a '0' will display a command help screen.

	Description
0	Displays a list of help screens for command groups 10 – 50
00	Displays a list of help screens for command groups 60 – 90
10	Displays the help screen for command group 10 Communications
11	Sets the RS485 address - 127
12	Sets the Baud Rate
13	Sets time since the last poll at which the AP1 considers itself off-line. Used in conjunction with command 42 where any code grants access and trips Relay 1
14	Toggles RS485 Termination. Note: (1) Only one device, besides the controller, should have RS485 termination enabled. (2) Using termination on multiple RS485 devices will cause communication errors
20	Displays the help screen for command group 20 Security
21	Toggles the tamper enable
22	Cycles between SW1 EOL supervision options
23	Cycles between SW2 EOL supervision options
24	Toggles secure code entry. When enabled key entry for credential is replaces with an '*' character
25	Used to change the password to enter configuration mode. Note: Record the new password or you will not be able to enter configuration mode.
30	Displays the help screen for command group 10 Beeper and Display

31	Toggles beep with key press
32	Toggles beep with access
33	Toggles beep with alarm
34	Toggle between US and European Date format
40	Displays the help screen for command group 10 Relay 1 and Inputs
41	Sets relay 1 on time. This is the time the relay is one if access is granted by the controller or the request to exit button becomes active. Note that the controller can send commands to override this setting
42	Cycles between the 'any code opens gate' options. These include off, on until communication with controller is established and on anytime communication is lost. Works in conjunction with command 13
43	Cycles between the Input configuration options. Options include: • Both inputs are general purpose and simply report to controller • Input 1 is for a door / gate contact, Input 2 is for an active RTE input (button). An active RTE event triggers Relay 1
44	Sets the allowed door open time. If the door is held open longer than this time a door help open event will occur
45	Toggles the on until closed setting. Relay 1 remains on until the door is closed. Used for magnetic locks to prevent pinching
50	Displays the help screen for command group 50 Relay 2 / Alarm menu
51	Cycles through the Relay 2 functions: • Alarm Out • General Purpose (only activated by controller) • Different Hold time. Activated when Relay 1 is activated but for a different length of time. Used for controlling door holders • Slave to Relay 1. Is on whenever Relay 1 is on • Heater. IS active when temperature approach or are below freezing
52	Relay 2 on time when the function different hold time is selected
53	Alarm Time. The time that the buzzer will sound or Relay 1 will be active then sound buzzer with alarm or Relay 2 functions as an alarm output. Triggered an alarm state event in the AP1 occurs: Tamper, Door forced open, Door held open

AP1 Properties and Status

During normal operation, press the '*' key followed by the '#' key. The AP1 will display a status screen which will show the following:

- Part Number
- Serial Number
- Mfg Date / Internal Temperature (not ambient)
- Firmware Revision and State of Firmware Update Process
- States of Inputs and Relays. O - Input is Open, C -Input is Cut, X - Input is Tampered, 0 - Relay is inactive, 1 - Relay is Active.
- Address, Communication State and Baud Rate
- Voltage at Power Input (PWR DC+ and DC-) and Surge Faults that have occurred

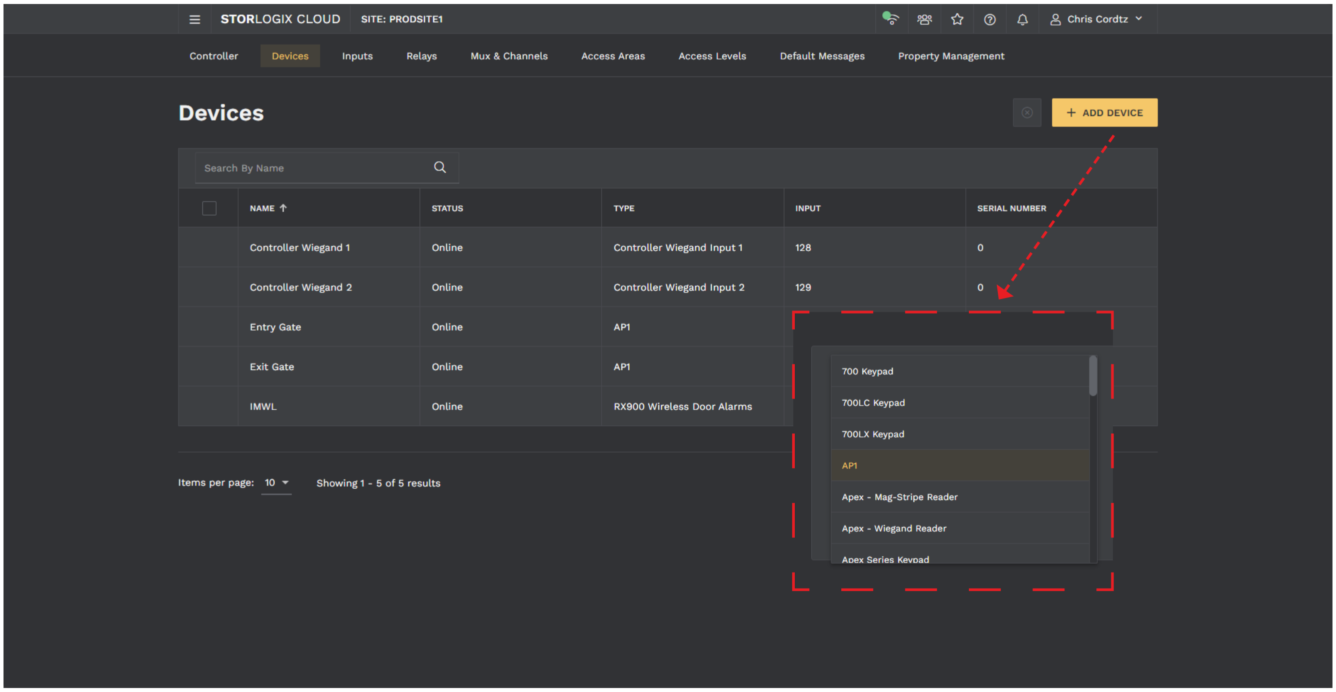
Not that this screen is static. While it is displayed pressing '#' will update it.

USER MANUAL | ADDING A NEW KEYPAD TO A FACILITY

Adding a new keypad to a facility's access control system requires the keypad to be setup within the access control system. Based on the access control platform, identification of the new AP1 keypad within the platform will change.

➡ When installing the AP1 on a StorLogix Cloud site, select 'AP1' as the device type.

➡ For installations on a StorLogix Desktop (local) site, select 'Apex' as the device type.



Devices

☐	NAME ↑	STATUS	TYPE	INPUT	SERIAL NUMBER
	Controller Wiegand 1	Online	Controller Wiegand Input 1	128	0
	Controller Wiegand 2	Online	Controller Wiegand Input 2	129	0
	Entry Gate	Online	AP1		
	Exit Gate	Online	AP1		
	IMWL	Online	RX900 Wireless Door Alarms		

Items per page: 10 Showing 1 - 5 of 5 results

Revision History:
1 – Initial release
2 – Added the operation and graphic display section
3 - Mounting options added; regulatory certificates
4 - Specifications updated
5 - Electrical specifications updated
6 - Appendix added displaying device voltage usage
7 - Interior label updated to reflect latest label
8 - Power supply and keypad amperage updates

1. Power for the heater is provided separately to (1) maintain compatibility with legacy touchpad heaters and (2) to allow the keypad to run from a higher voltage power supply not limiting it to the heater requirements.
2. A single power supply can be used to power both the heater and the AP1 provided the following requirements are met:
   - The supply does not exceed the maximum allowable heater voltage of 12 V nominal, 14V maximum. This range allows use of a battery backed 12 V supply.
   - When the heater is on and the keypad is under operation (display lit brightly, relays turned on) the voltage at the AP1 power terminals must not drop below 11 volts, otherwise the AP1 may reset. In this situation the AP1 internal voltmeter can be useful for measuring the input voltage. To test, follow these steps:
   - Wire the heater power in parallel to the AP1 power.
   - Set Relay2 function to Alarm Output (Cmd 51)
   - Set Alarm Time to maximum (300 seconds Cmd 53)
   - Enable Tamper Detection (Cmd 21)
   - Open the keypad to cause a tamper alarm. This will trip relay 2 turning the heater on.
   - Operate the keypad and monitor the voltage to ensure it is at or above 11 volts at all times.
   - When testing is complete, set Relay 2 function back to Heater and Alarm and Tamper to their desired settings.

Power Supply Limits

Power Supply Limits	Actual Amerage (mA)	Maximum Limit (75% Load)
1 Amp	1.2 A	900 mA
2 Amp (recommended for AP1 w Heater)	3 A	2250 mA
4 Amp	5 A	3750 mA
6 Amp	7 A	5250 mA

Device Amperage Usage

Remote Unit Type	Current Draw
Legacy Keypad or Keypad With Intercom	300 mA
AP1 Keypad without Heater	300 mA
AP1 Keypad with Heater	1300 mA
Apex Access Device	300 mA
Hardwired Multiplexer (16 - 96Ch)	300 mA
Weigand	300 mA
8 - Ch Relay Board	500 mA
Wireless Multiplexer	500 mA

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.

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 call our live support team at +1.866.240.7602 Monday-Friday; 10:00am-7:00pm EST.