

# API KEYPAD

## STORLOGIX CLOUD MANUAL



# 2024

**PTI** SECURITY SYSTEMS  
**ASSA ABLOY**



## STORLOGIX CLOUD MANUAL

Sales: +1.800.523.9504  
Support: +1.866.240.7602  
Web: [ptisecurity.com](http://ptisecurity.com)

Rev A - May 2024

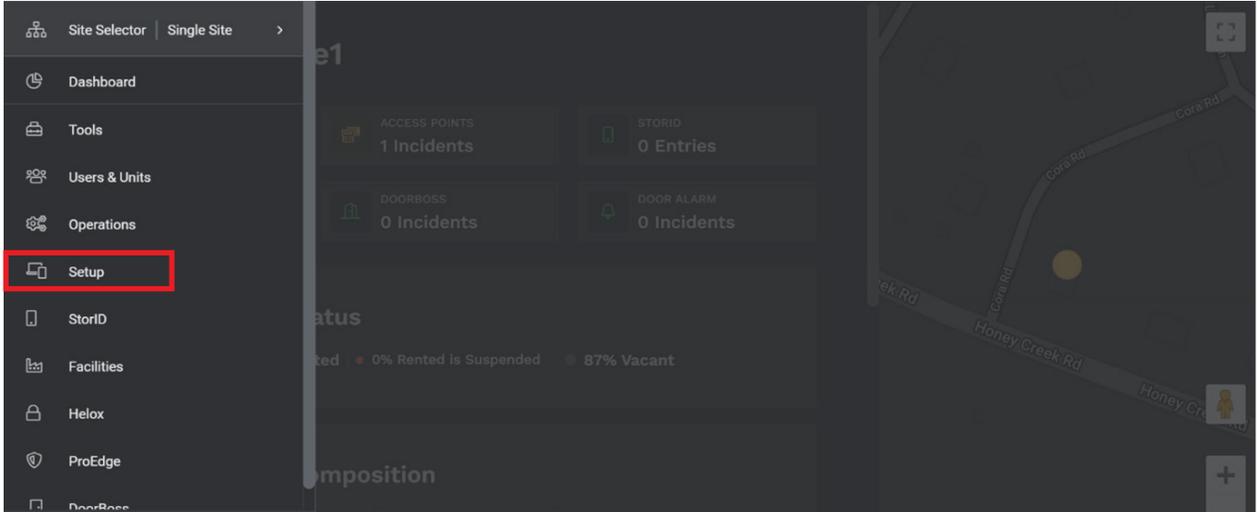
### INTRODUCTION

This document is intended to provide a high level overview of setting up the AP1 keypad in the StorLogix Cloud system.

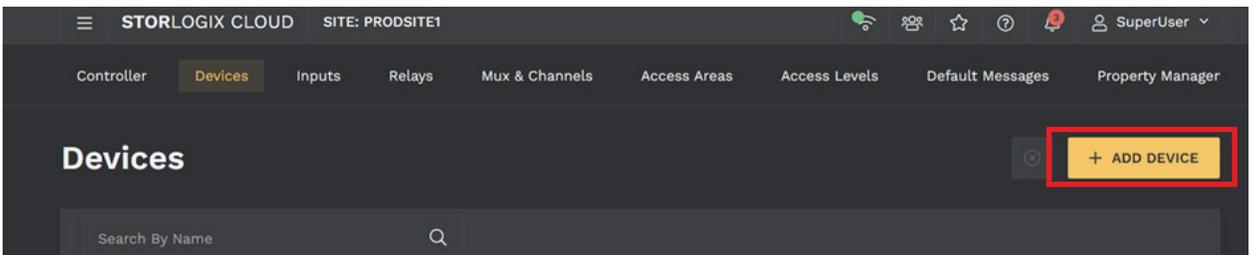


# INSTALLATION OF AP1 IN STORLOGIX CLOUD

- 1 Navigate to the homepage of StorLogix Cloud and click on the *Setup* tab.

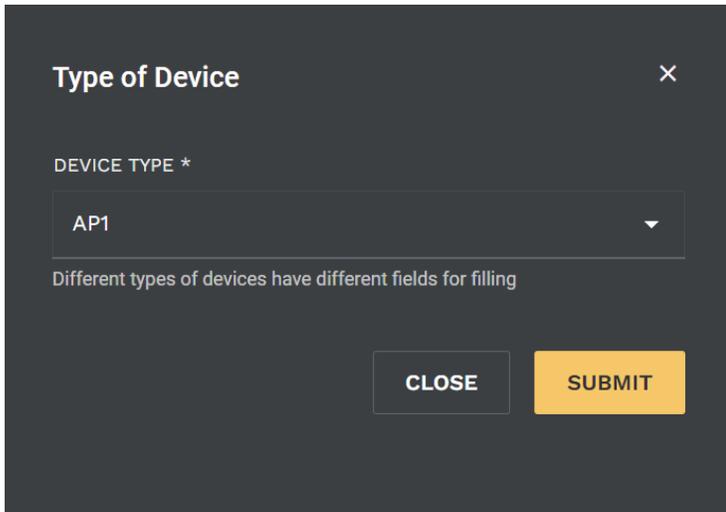


- 2 Click on *Add Device*.



3

Select AP1 from the *Device Type* drop down menu and click **Submit**.



Type of Device

DEVICE TYPE \*

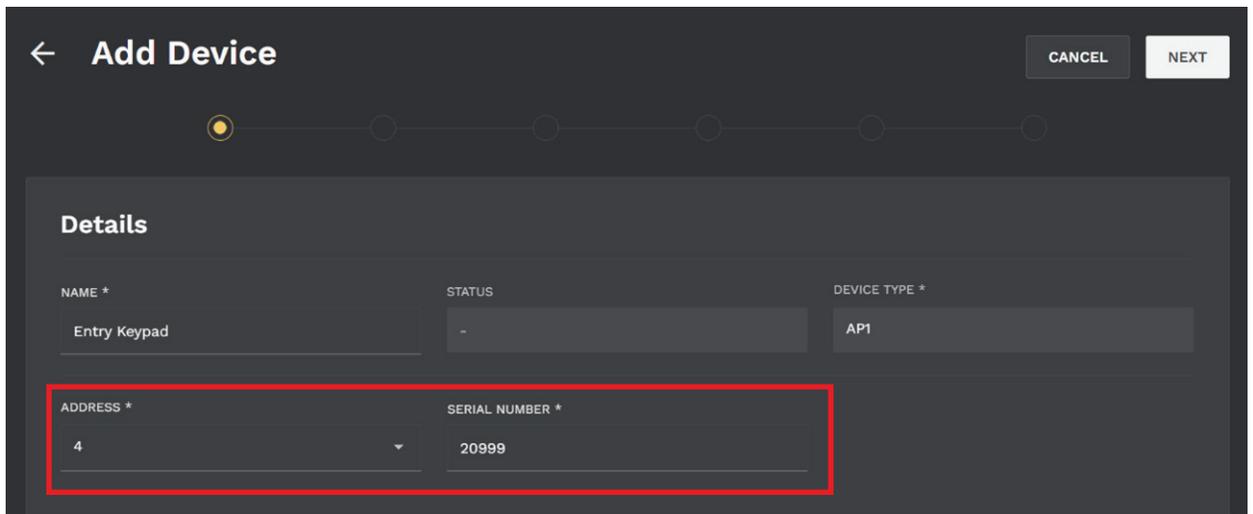
AP1

Different types of devices have different fields for filling

CLOSE SUBMIT

4

Choose a name for the AP1 keypad. Then select a RS485 network address by setting the address in the AP1 keypad menu. The default address is 1. Add the same address into StorLogix Cloud. Then type the 5 digit serial number by pressing “0” “#” and “\*”



← Add Device

CANCEL NEXT

Details

NAME \* STATUS DEVICE TYPE \*

Entry Keypad - AP1

ADDRESS \* SERIAL NUMBER \*

4 20999

5

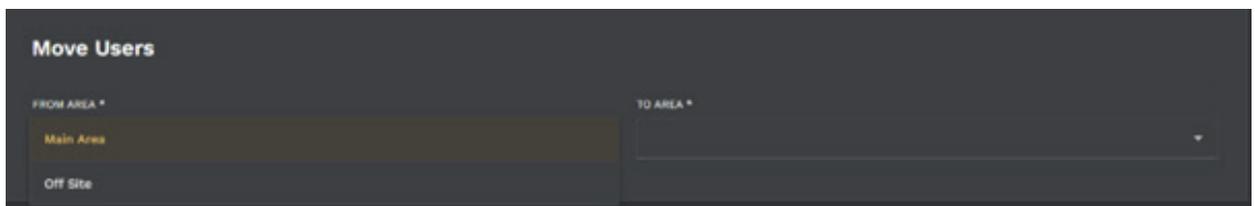
Select an **Access Area** - the area that requires controlled entry.

**Main Area:** The facility

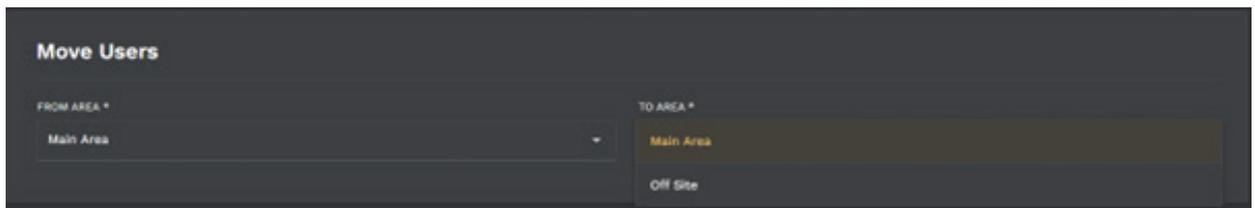
**Off Side:** Area outside the facility

Moving users from Off Site to Main Area would make an entry keypad. Moving users from main Area to Off Site would make an exit keypad.

If another keypad needs to be created, navigate to the Access Areas tab and add buildings and floors as needed.



The screenshot shows a dark-themed interface titled "Move Users". It features two dropdown menus. The "FROM AREA" dropdown is open, showing "Main Area" (highlighted in yellow) and "Off Site". The "TO AREA" dropdown is currently empty.



The screenshot shows the same "Move Users" interface. The "FROM AREA" dropdown is now closed and shows "Main Area". The "TO AREA" dropdown is open, showing "Main Area" (highlighted in yellow) and "Off Site".

6

Select a **Function Mode** - how you want your keypad to act - from the drop down menu.

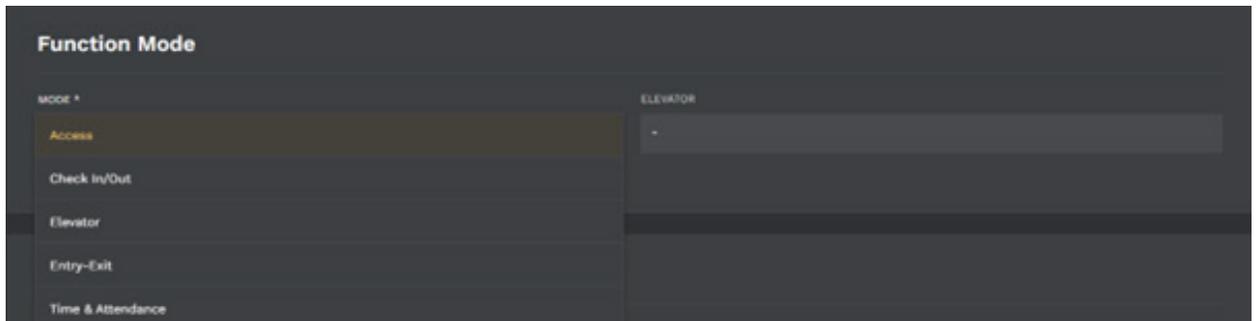
**Access:** If your keypad is just for facility access.

**Check In/Out:** If a single keypad acts as an entry and exit keypad.

**Elevator:** If your keypad is to access an elevator.

**Entry/Exit:** If your keypad is either entry or exit, not both.

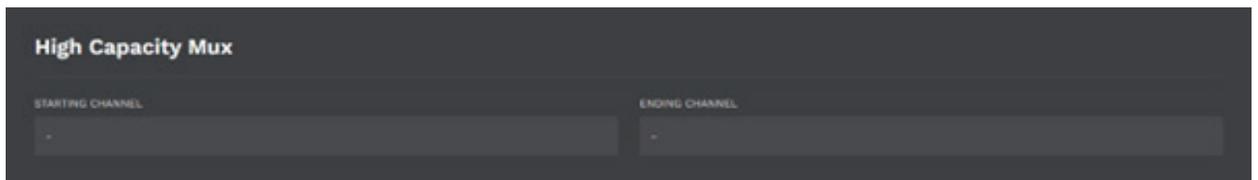
**Time & Attendance:** If your keypad \_\_\_\_\_



The screenshot shows a dark-themed interface titled "Function Mode". On the left, there is a vertical list of options under the heading "MODE \*": "Access", "Check In/Out", "Elevator", "Entry-Exit", and "Time & Attendance". The "Access" option is highlighted with a yellow background. To the right of this list is a section labeled "ELEVATOR" with a single input field containing a hyphen (-).

7

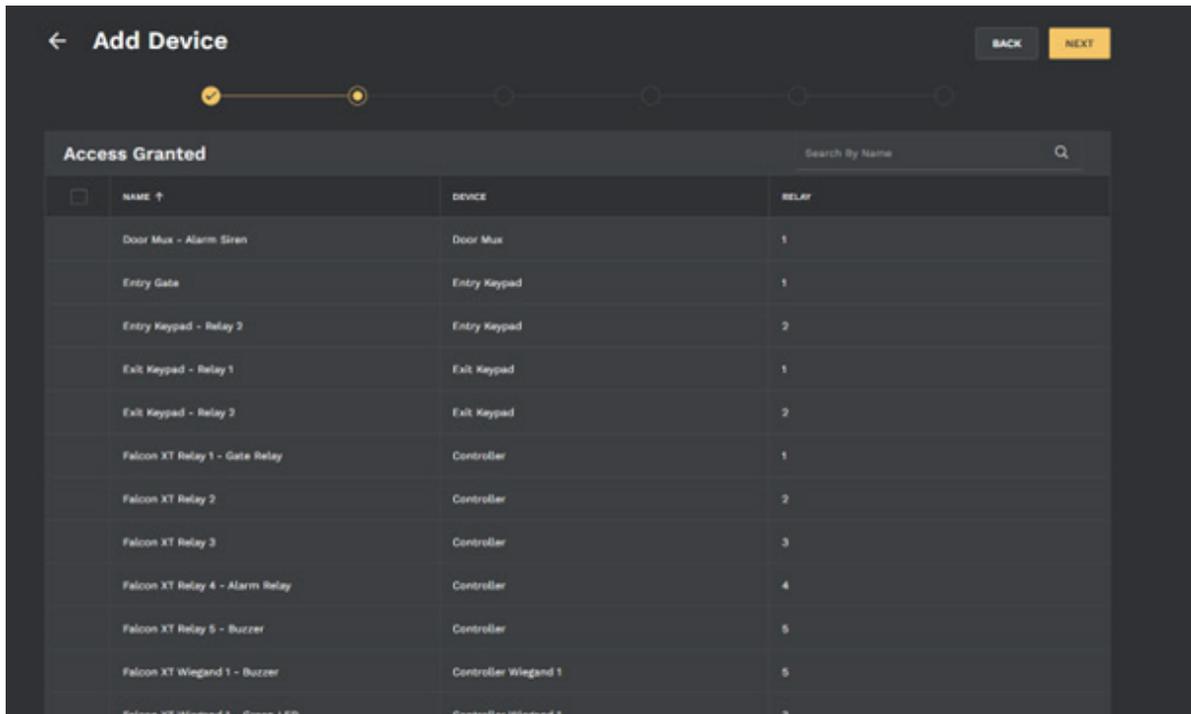
The High Capacity Mux will already have an assigned value for the Starting and Ending Channels.



The screenshot shows a dark-themed interface titled "High Capacity Mux". It features two input fields: "STARTING CHANNEL" on the left and "ENDING CHANNEL" on the right. Both fields contain a hyphen (-).

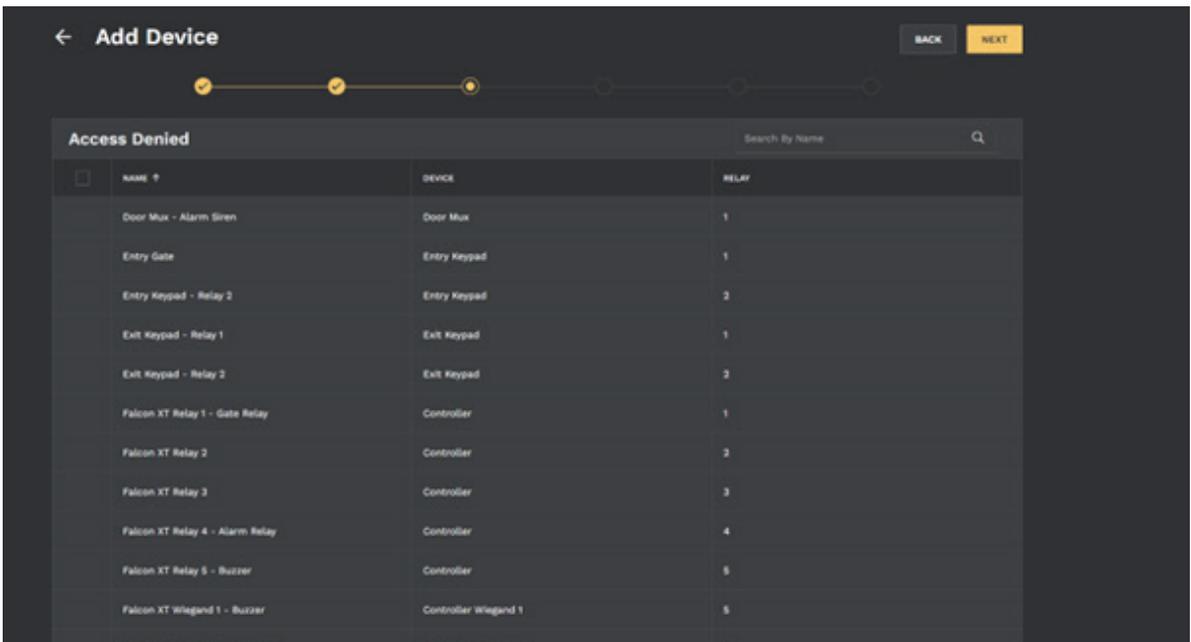
8

Select the relay to trigger the gate or door when access is granted. Then click *Next*.



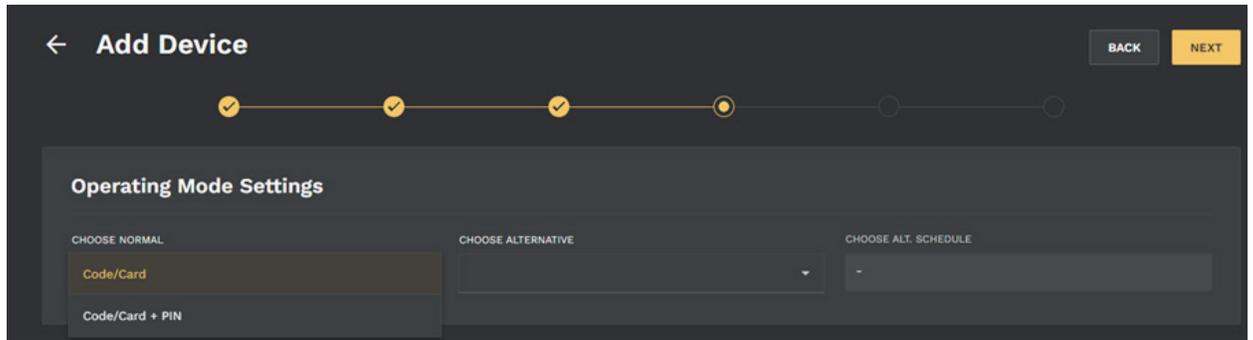
9

Select an option under *Access Denied* section to temporarily deny access for the keypad. Then click *Next*.



10

Choose an **Operating Mode** - the mode of entry to use this keypad - from the drop down menus. Thank click **Next**.

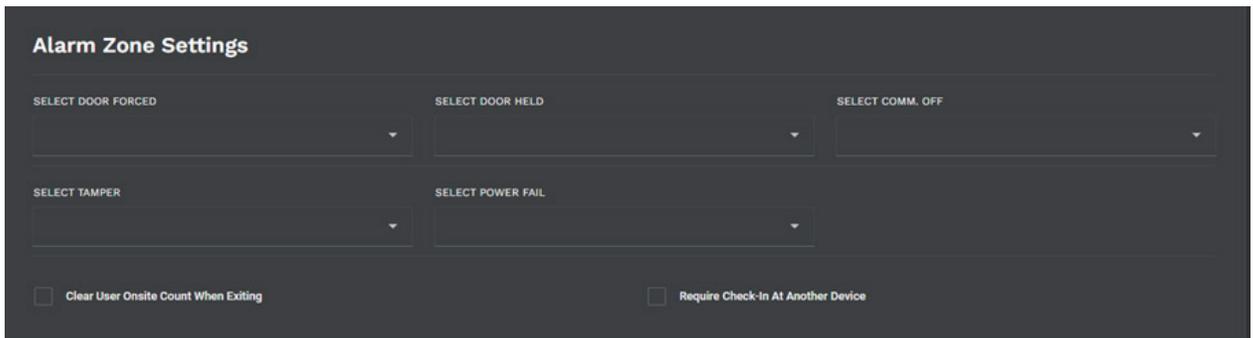


The screenshot shows the 'Add Device' configuration screen. At the top, there is a progress indicator with five steps, the fourth of which is highlighted. Below this, the 'Operating Mode Settings' section contains three columns: 'CHOOSE NORMAL', 'CHOOSE ALTERNATIVE', and 'CHOOSE ALT. SCHEDULE'. Under 'CHOOSE NORMAL', there are two dropdown menus: the first is set to 'Code/Card' and the second is set to 'Code/Card + PIN'. The 'CHOOSE ALTERNATIVE' and 'CHOOSE ALT. SCHEDULE' sections also have dropdown menus, though they are currently empty. At the top right of the screen, there are 'BACK' and 'NEXT' buttons.

11

Choose an **Alarm Zone** setting of when a selected door is forced, held, or tampered with from the drop down menus.

Triggering an alarm when the keypad loses communication or power fails is also an option here.

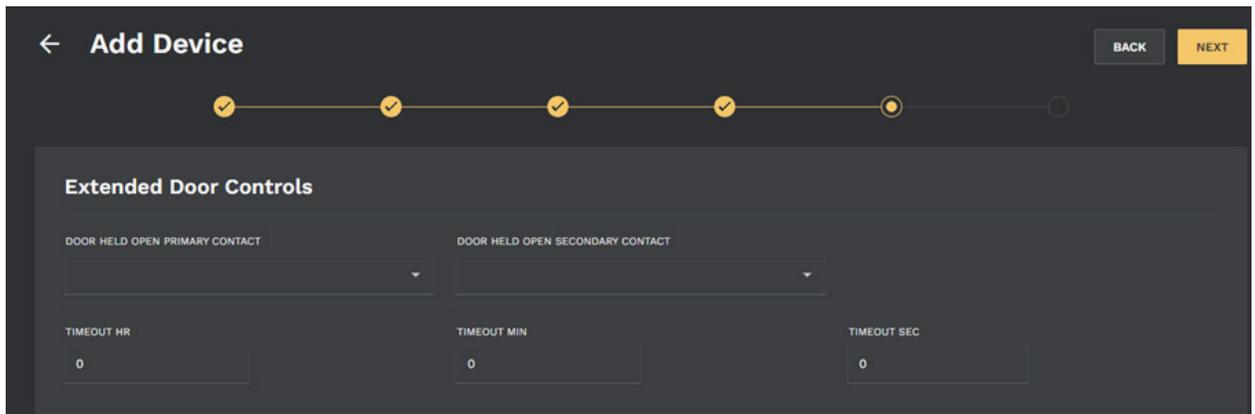


The screenshot shows the 'Alarm Zone Settings' screen. It features five dropdown menus arranged in two rows. The first row contains 'SELECT DOOR FORCED', 'SELECT DOOR HELD', and 'SELECT COMM. OFF'. The second row contains 'SELECT TAMPER' and 'SELECT POWER FAIL'. At the bottom of the screen, there are two checkboxes: 'Clear User Onsite Count When Exiting' and 'Require Check-In At Another Device', both of which are currently unchecked.

12

Choose an **Extended Door Control**. By using an input in a controller, a door release can be added.

Select a **Timeout** which allows for customization of the hours, minutes and seconds the relay will be held open from the drop down menu. Then click **Next**.



The screenshot shows the 'Add Device' configuration screen. At the top, there is a progress indicator with five steps, the fifth of which is highlighted. Below this, the 'Extended Door Controls' section contains three dropdown menus: 'DOOR HELD OPEN PRIMARY CONTACT', 'DOOR HELD OPEN SECONDARY CONTACT', and 'TIMEOUT SEC'. Below the 'TIMEOUT SEC' dropdown are three input fields for 'TIMEOUT HR', 'TIMEOUT MIN', and 'TIMEOUT SEC', each with the value '0' entered. At the top right of the screen are 'BACK' and 'NEXT' buttons.

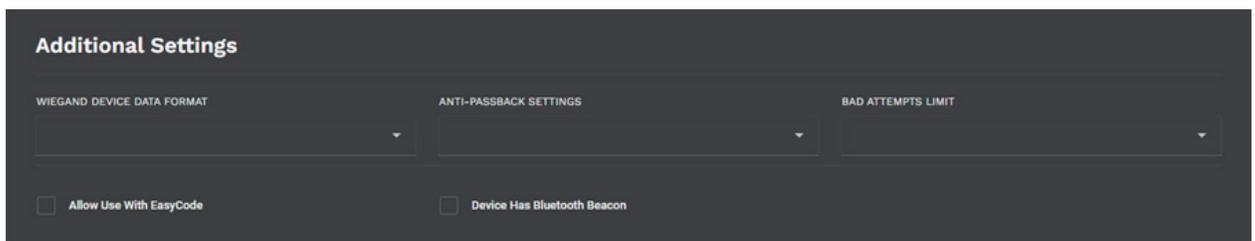
13

Choose additional settings from the drop down menus if needed.

Adding a **Wiegand Device Data Format** allows a card reader to be used.

Adding **Anti-Passback Settings** allows restriction of access codes or pins.

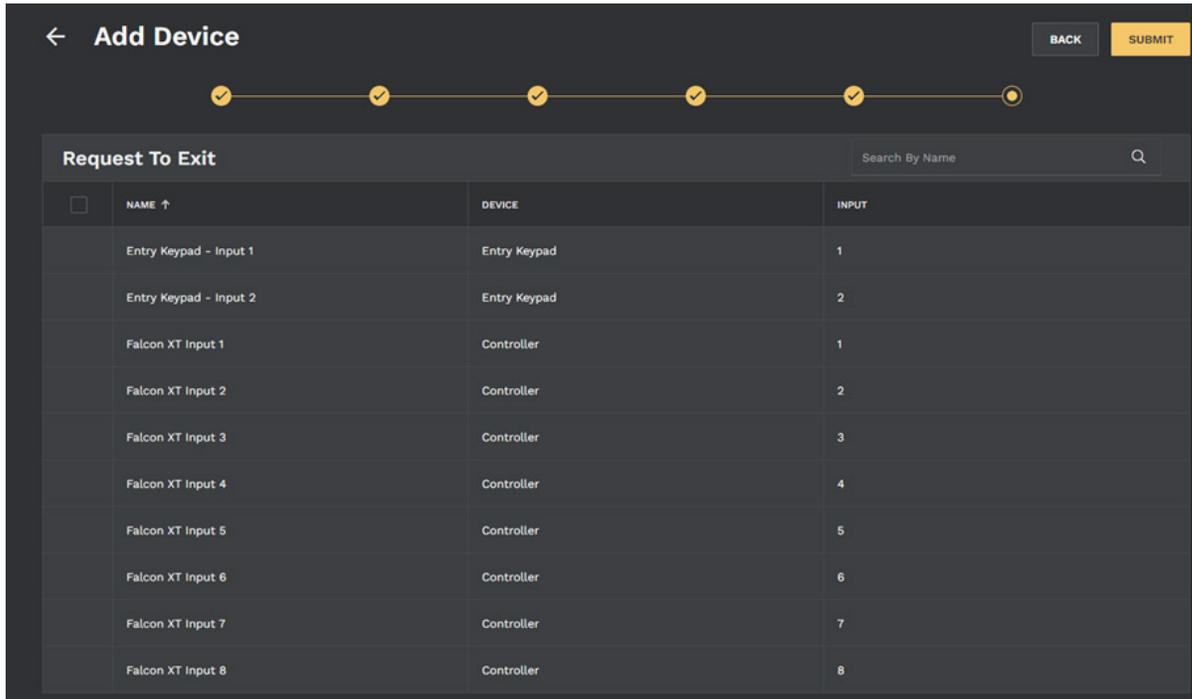
Setting a **Bad Attempts Limit** limits the restriction of access codes.



The screenshot shows the 'Additional Settings' section. It features three dropdown menus: 'WIEGAND DEVICE DATA FORMAT', 'ANTI-PASSBACK SETTINGS', and 'BAD ATTEMPTS LIMIT'. Below these are two checkboxes: 'Allow Use With EasyCode' and 'Device Has Bluetooth Beacon', both of which are currently unchecked.

14

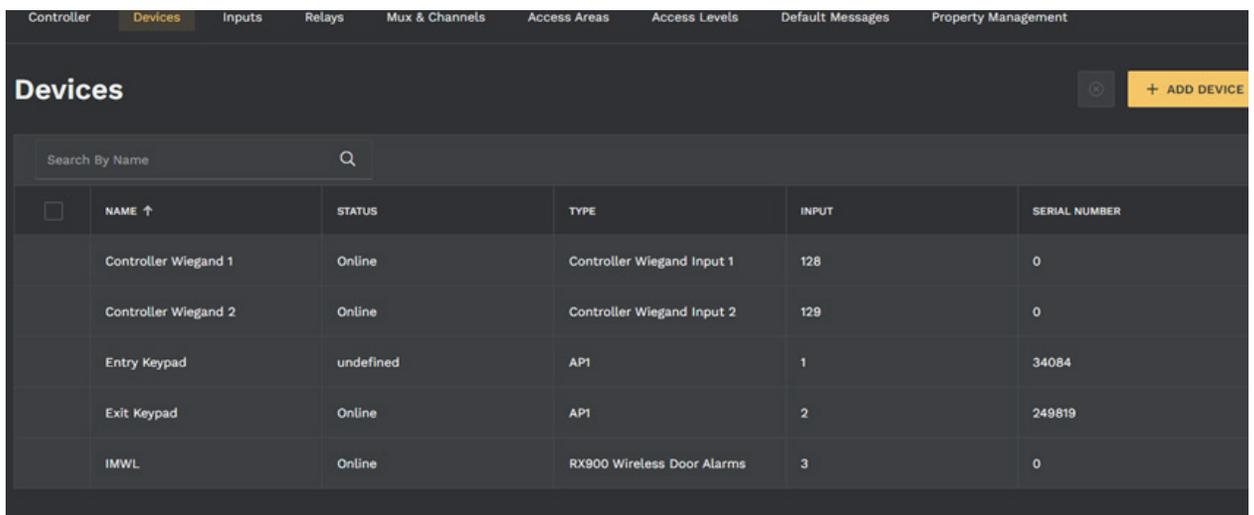
Select the device to be used as a request to exit input. Click **Submit** to finish adding AP1 to the StorLogix Cloud.



Request To Exit	Search By Name		
<input type="checkbox"/>	NAME ↑	DEVICE	INPUT
	Entry Keypad - Input 1	Entry Keypad	1
	Entry Keypad - Input 2	Entry Keypad	2
	Falcon XT Input 1	Controller	1
	Falcon XT Input 2	Controller	2
	Falcon XT Input 3	Controller	3
	Falcon XT Input 4	Controller	4
	Falcon XT Input 5	Controller	5
	Falcon XT Input 6	Controller	6
	Falcon XT Input 7	Controller	7
	Falcon XT Input 8	Controller	8

15

After set-up, the AP1 will appear in the **Devices List** in StorLogix Cloud.

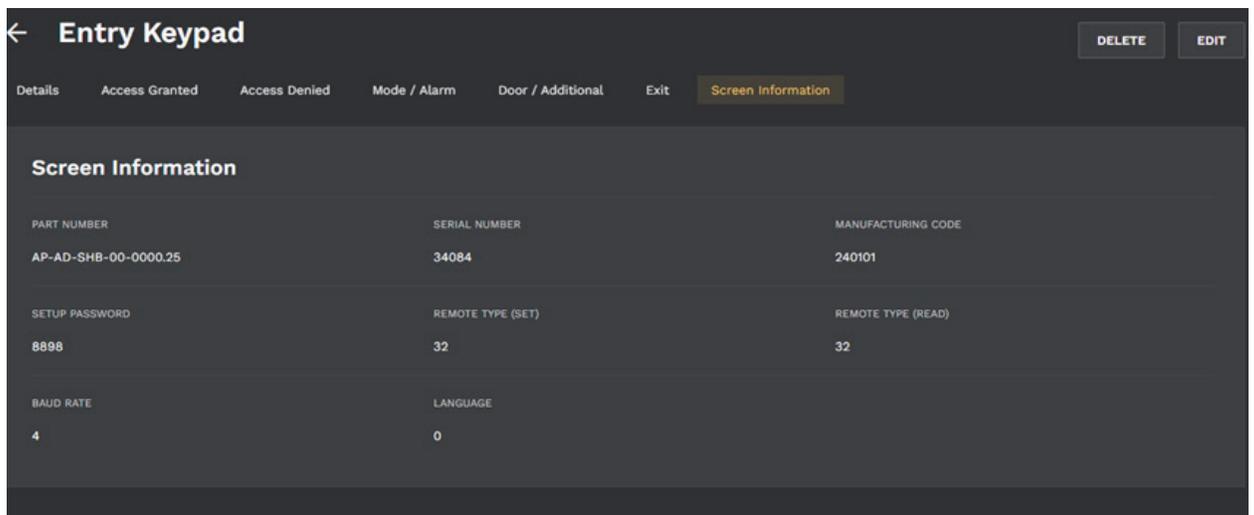


Controller	Devices	Inputs	Relays	Mux & Channels	Access Areas	Access Levels	Default Messages	Property Management
<input type="checkbox"/>	NAME ↑	STATUS	TYPE	INPUT	SERIAL NUMBER			
	Controller Wiegand 1	Online	Controller Wiegand Input 1	128	0			
	Controller Wiegand 2	Online	Controller Wiegand Input 2	129	0			
	Entry Keypad	undefined	AP1	1	34084			
	Exit Keypad	Online	AP1	2	249819			
	IMWL	Online	RX900 Wireless Door Alarms	3	0			

16

Details, Access Granted, Access Denied, Mode/Alarm, Door/Additional, and Exit pages have already been configured through this set up process.

**Screen Information** displays part number, serial number, manufacturing code, setup password, remote type (set), remote type (read), baud rate and language of the keypad.



The screenshot shows a mobile application interface for configuring an 'Entry Keypad'. At the top, there is a navigation bar with a back arrow and the title 'Entry Keypad'. On the right side of the navigation bar are 'DELETE' and 'EDIT' buttons. Below the navigation bar is a horizontal menu with several options: 'Details', 'Access Granted', 'Access Denied', 'Mode / Alarm', 'Door / Additional', 'Exit', and 'Screen Information'. The 'Screen Information' option is currently selected and highlighted in a light blue color. Below the menu, the 'Screen Information' section is displayed, showing a table of configuration parameters.

Screen Information		
PART NUMBER	SERIAL NUMBER	MANUFACTURING CODE
AP-AD-SHB-00-0000,25	34084	240101
SETUP PASSWORD	REMOTE TYPE (SET)	REMOTE TYPE (READ)
8898	32	32
BAUD RATE	LANGUAGE	
4	0	

# PTI SECURITY SYSTEMS

# ASSA ABLOY

SHAPING THE INDUSTRY  
SINCE 1979

With PTI Security Systems, operators can easily customize all of their facility's access areas, review site activity, and monitor zones and alarms from one cloud-based account. Create a world-class operation with the most advanced enterprise access control solution from the trusted industry leader with over 40 years of experience.

Since 1979, PTI Security Systems™ has provided the self-storage industry with proven security and access control systems. Known for our complete and innovative solutions that deliver advanced and cost-effective security systems, self-storage owners and operators can efficiently manage their facility from anywhere, lower operating costs, and enhance the tenant experience.

For more information about PTI Security Systems, please contact a PTI representative or visit our website.

PTI is a trademark of Preferred Technology Systems, LLC

 [ptisecurity.com](https://ptisecurity.com)

 [sales@ptisecurity.com](mailto:sales@ptisecurity.com)

 800.523.9504