PTI Security Training Manual

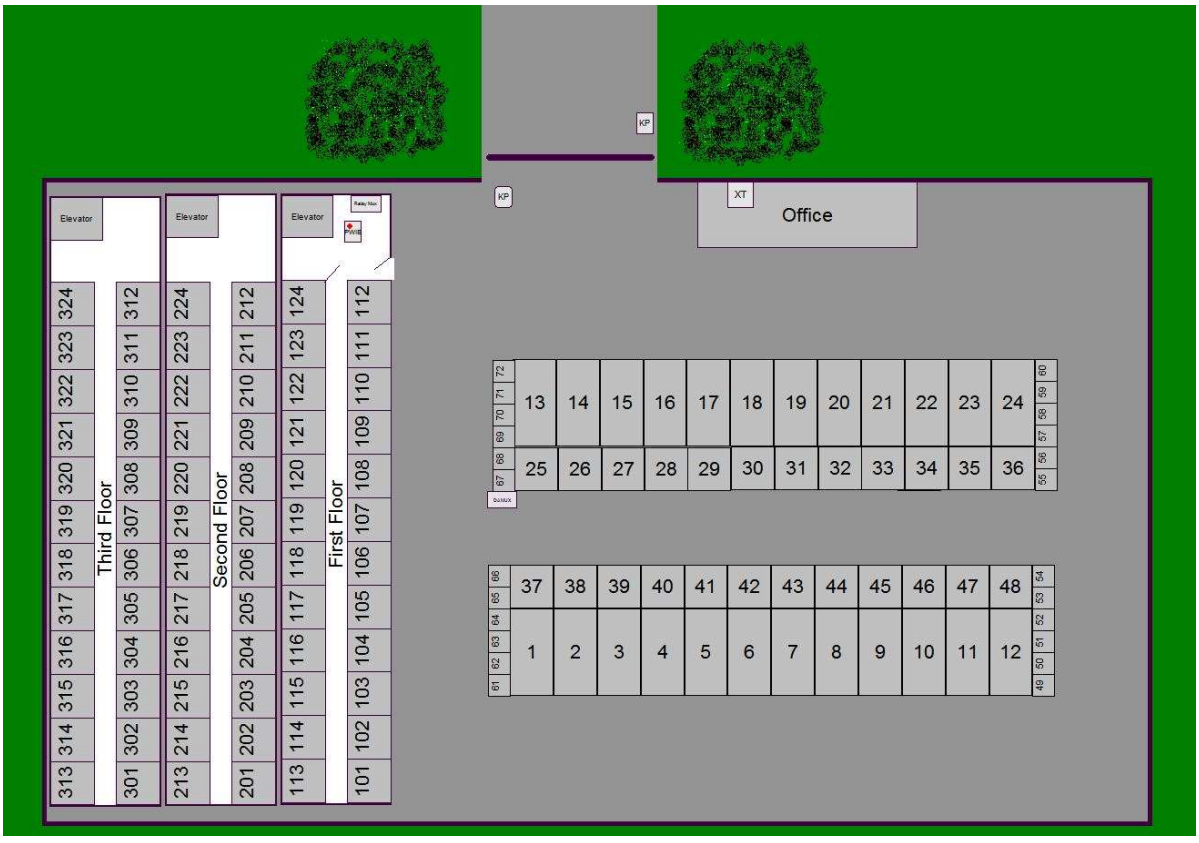
Table of Contents

Training Overview

Site Installation Process

1. **Install Hardware** – installing the hardware first allows the equipment to auto-enroll and speeds up the installation process
2. **Install Software** - After the installation of the hardware, we can install the software
3. **Setup Software** – create the connections and define how the devices within the system functions
4. **Test Setup** – test whether the current settings cause the system to function as expected
5. **(As Needed) Make Corrections and Retest** – no one gets it right the first time, every time

Our Training Site Layout



Picture 1 : Training Site Layout

Topics to Know Before Beginning

- **RS-485 Communications Protocol** – used for communication between the different devices
- **Power Configuration** – what is needed to power the different devices

RS-485 Communications Protocol

- A differential voltage or balanced communications protocol
- The Falcon XT compares plus (+) and negative (–) voltages for a voltage difference
- The total network must be less than 4000 feet 1220 meters
- A daisy-chained system from one device to the next
- A polled system from the controller to the devices
- Each device must have a unique address assigned
- For our system, we recommend 18 AWG, stranded 4 conductor wire (power and data)

Power Configuration

- Current draw depends on the device (see table)
- Can determine whether a single or multiple power supplies are needed
- The formula for calculating power drop (18 AWG)
  - $V = D \; x \; I \; x \; 0.0128$
    - V = voltage drop at this device
    - D = length of wire in feet
    - I = sum of the amperage for the device plus any devices after it

Device	mA
Keypads	300
Door Alarm Mux	200
8 Channel Relay Mux	500
PTI Wiegand Device	300
Wireless Door Alarm Mux	250
Keypad Camera	204
Prox Reader	30-260

Table 1: Device Current Draw

Review

1. Is it okay to home run all devices back to the Falcon XT?

2. Do all devices need to be addressed in the same order they are wired?

Power Calculation Example

You have 4 Apex keypads that are 40 feet apart. The power at the Falcon XT is 14 VDC. The goal is to have less than a 2 V drop.

Keypad 1

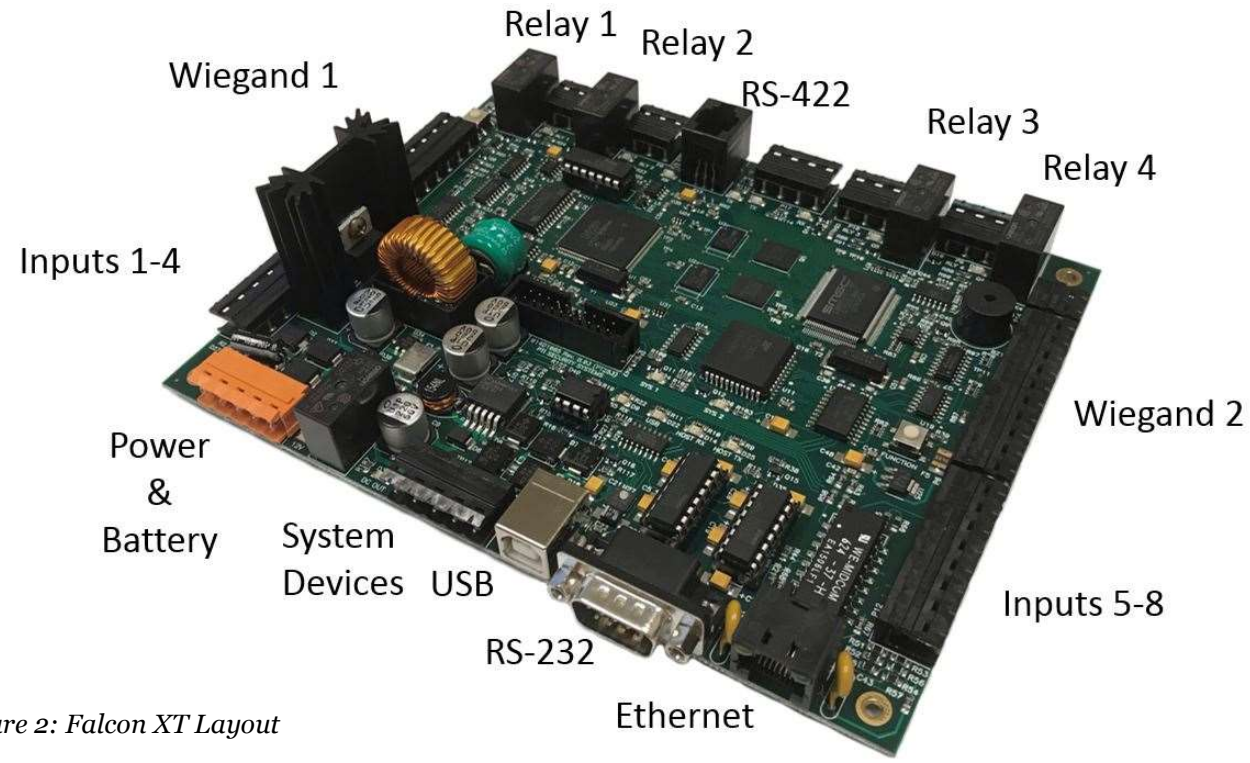
Keypad 2

Keypad 3

Keypad 4

Falcon XT Controller

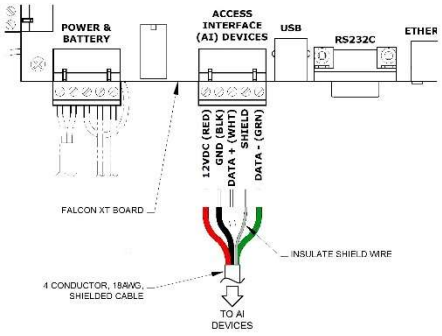
The controller is where system devices connect. We recommend using an 18 AWG stranded/4 conductor wire with bare drain wire, giving you 2 conductors for power, and 2 and the bare drain for data. The connector outputs 12-14 VDC / 2 A max.



Picture 2: Falcon XT Layout

Connections on P13

1. DC + output
2. DC – output
3. Data +
4. Data shield (bare drain)
5. Data –



Drawing 1: P13 Connection Wiring

Relay Output

The Falcon XT provides 4 relay output connections. Each relay has an LED that indicates the state of the relay. The relays on the Falcon XT, as well as most relays on the PTI devices, can handle 30 V AC\DC. The amount of current the relay can handle depends on the voltage type and the connection type (See Table 2). A three-position connector provides the connections to the relay (See Table 3). Relays are dry contacts (they do not produce a voltage).

	AC	DC
NO	10A	5A
NC	3A	3A

Table 3: Relay Amps for Connection Type

NO	Normally Open Contact
C	Common
NC	Normally Closed

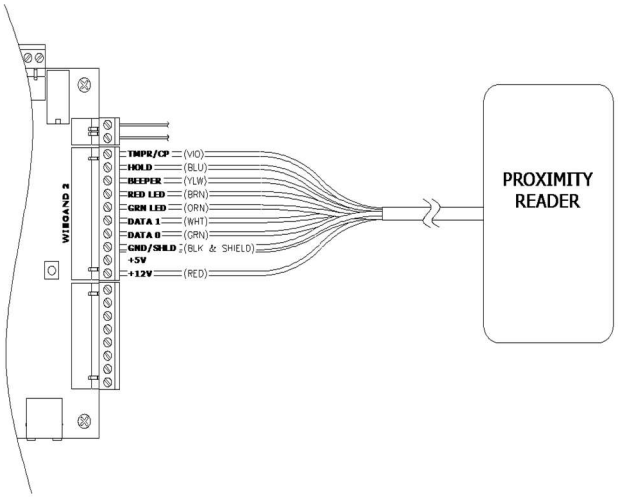
Table 2: Relay Connections

RS-422 Connector

The DoorBoss transceiver connects to the RS-422 connector on the Falcon XT. There are two LEDs associated with the RS-422 connector. The D31 LED is the receive indicator, and D32 is the transmit indicator. The pigtail provided with the transceiver is the only device that connects to this port. The DoorBoss system allows up to four transceivers connected in series to the Falcon XT.

Wiegand Inputs

The Wiegand inputs allow you to attach Wiegand devices like proximity readers, card readers, and biomedical readers. The inputs allow these devices to interface with the PTI system. The two most common Wiegand devices used in the PTI system are the HID proximity reader and the Chamberlain Passport remote reader. The connections for Wiegand 2 are the reverse of Wiegand 1, which means you can pull the connector off Wiegand 1 and connect it to Wiegand 2 without rewiring the connector.



Drawing 2: Wiegand Input

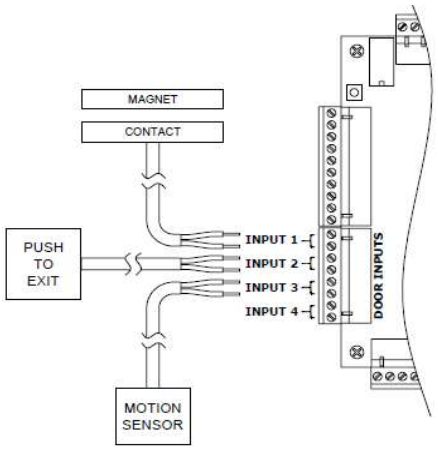
NOTE: How a device wire varies from device to device. Refer to the device's manual for the correct wiring.

Inputs

The Falcon XT has 8 inputs. You can think of inputs as trigger points used to signal an event has occurred. Inputs are wet (they put out a signal) contacts and must connect to a dry (no voltage output) device.

One of the most common uses for inputs is to read the closure of a door switch used for door alarms, but you can use inputs to trigger other things as well. Some examples include a push-button for a request to exit, motion sensors, glass break sensors, and other dry contact closures. You can use a relay to trigger an input, or input to close a relay.

Each of the inputs on the Falcon XT has two connection points side by side on the connector.



Drawing 3: Inputs

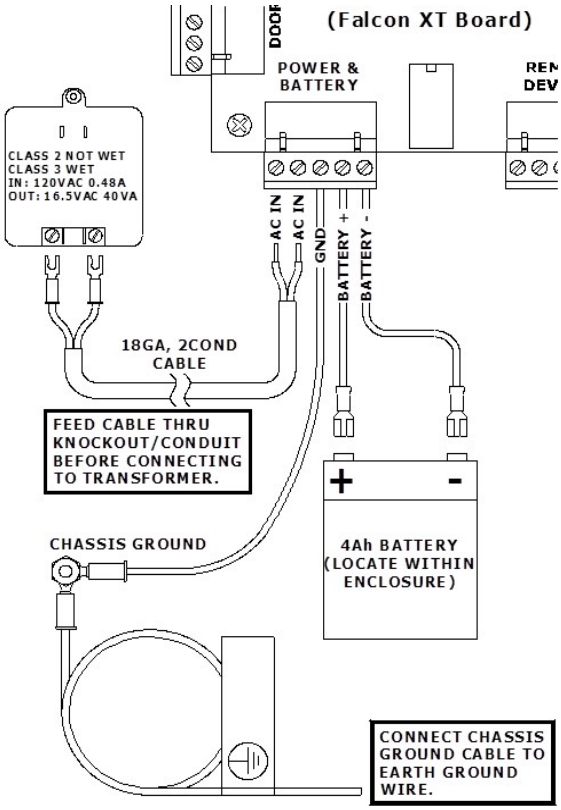
Power and Battery

The power and battery connections to the Falcon XT connect the AC power transformer and the backup battery. The power transformer outputs 24 VAC / 40 VA.

The battery is a 12 V 4 AH sealed battery. The battery is not enough to maintain communications with the computer but can keep the controller running for a short period. How long the battery lasts depends on the power demand by the system.

Power and Battery Connections

1. AC In
2. AC In
3. Earth Ground
4. Battery +
5. Battery –



Drawing 4: Power Connector

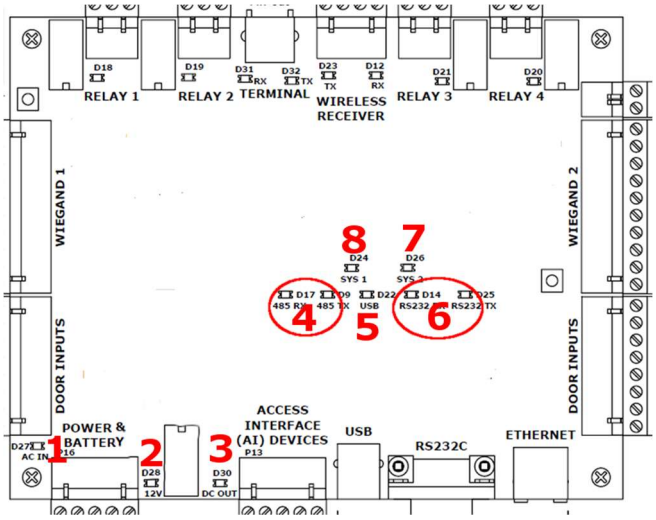
PC Connections

The Falcon XT provides 3 different methods for connecting to the PC running the StorLogix program.

- **USB** – the USB connection connects through the USB port on the Falcon XT. USB has a limited distance of 3 meters (approximately 15 feet). We do not recommend you exceed this limitation.
- **Ethernet** – the Ethernet connection is made through the Ethernet port on the Falcon XT. The max distance is 100 meters (328 feet). We recommend that you connect the computer and the Falcon XT to the same network router or switch unless setting up for a remote connection.
- **RS-232** – the RS-232 connection connects through the 9 pin RS-232 port. Most modern computers do not include an RS-232 port built into the PC, which requires using a USB to serial adapter to make the connection. RS-232 has a limit of 50 feet / 15 meters and requires a special cable purchased through the PTI sales department.

Falcon XT Diagnostic LEDs

1. (D27) AC IN on P16 pins 1 & 2
2. (D28) Onboard Power Supply or battery providing DC power
   - If D27 is off and D28 is on, the battery is supplying the power
   - Keep in mind that the battery is not enough to keep the Falcon XT communicating with the computer



Drawing 5: Falcon XT LED's

3. (D30) DC OUT to the Remote Devices on P13 pins 1 & 2.
   - If you hear a click and this light goes out, then the watchdog circuit is protecting the Falcon XT from an overload on the Remote Devices output power or data (P13). Troubleshoot the RS-485 network for a shorted wire, defective power supply, or defective device.
4. D9 and D17 indicate data transmission and reception for the RS-485 network.

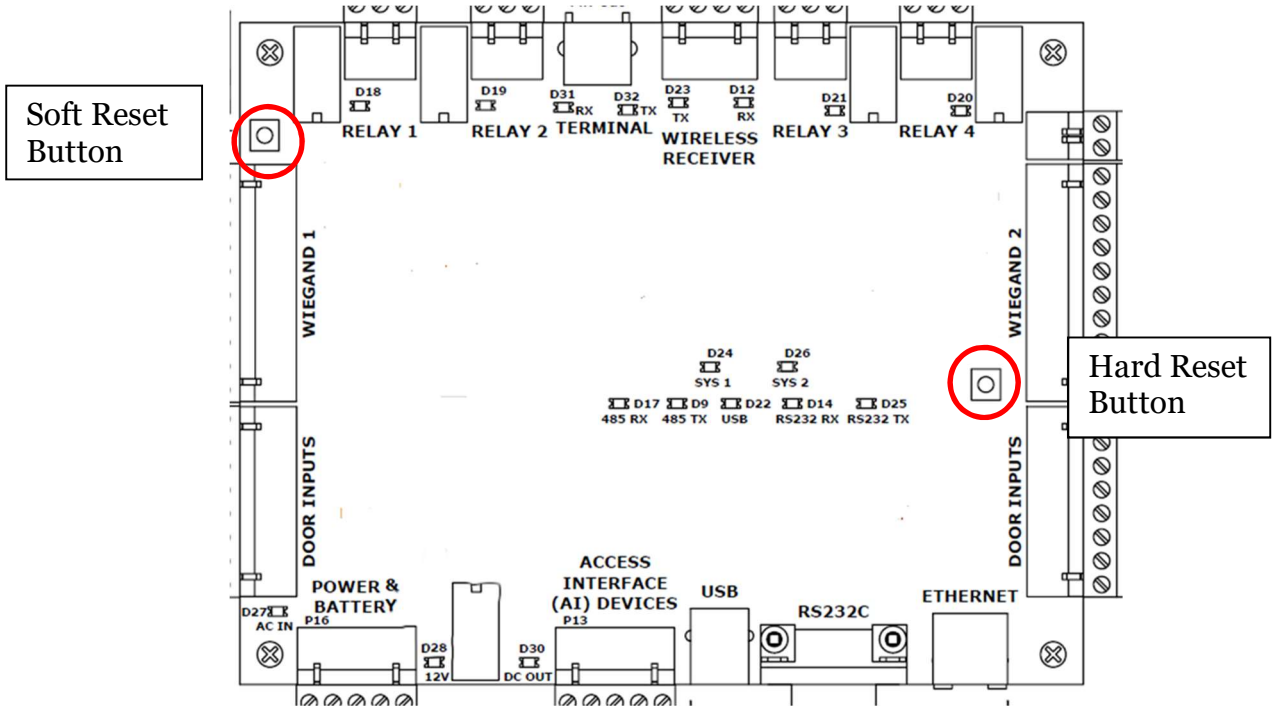
5. D22 illuminates when the Falcon XT detects a USB connection.
6. D14 and D25 indicate data transmission and reception for the RS-232. The LED's flash when the Falcon XT is communicating with the computer through USB or the RS-232 port.
7. D26 (SYS2) shows the communication status with the LogixServer.
   - Off – the LogixServer is idle or not running
   - Flashing – the Falcon XT is in baud sensing mode for RS-232/USB
   - On – LogixServer detected and active unless using Ethernet
8. D24 (SYS1) shows the status of the Ethernet connection. When blinking, count the number of blinks between the pauses to determine the status.
   - Off means, there is no Ethernet link
   - 1 blink means, the Falcon XT is looking for a conflicting IP address
   - 2 blinks mean the Falcon XT is waiting for the DHCP configuration from the router.
   - 3 blinks mean the Falcon XT is attempting to connect, this can also indicate a firewall is blocking the signal.
   - 4 blinks mean the Falcon XT has connected to the LogixServer.
   - 5 blinks mean the Falcon XT has encountered an IP conflict.
   - LED illuminated, no blinks, means the Falcon XT has connected to the LogixServer and is communicating, which is the state you want.

Falcon XT Reset Buttons

The Falcon XT has the capabilities to be reset. The reason a Falcon XT would need a reset to correct or troubleshoot an issue. The Falcon XT two types of resets, a non-destructive soft reset, or a destructive hard reset.

- Soft Reset
  - The soft reset button is in the upper-left-hand corner of the Falcon XT. The button is a small white button with a silver square collar. Pressing the button preserves any data on the Falcon XT. To perform a soft reset, press and release the button in the upper-left-hand corner of the board. One everyday use for the soft reset is re-establishing of connection to an Ethernet after a power failure.

- Hard Reset
    - The hard-reset button is in the middle-right side of the Falcon XT. Like the soft reset button, it is a small white button with a silver square collar. Pressing and holding the button destroys any data on the Falcon XT. To perform a hard reset, press and hold the button on the middle-right side of the board. The Falcon XT's buzzer sounds. Release the button once the buzzer has stopped. The buzzer sounds again, for a second, and this completes the hard-reset. It is advised not to do this unless directed by PTI Tech Support.



Drawing 6: Falcon XT Reset Buttons

Review

1. How many Wiegand inputs on the XT?
2. True or False: You should always connect an electrical ground.
3. What is the max length for a USB connection?
4. What type of contacts should you use for the inputs on the XT?

PTI Keypads

Keypad Comparison

	Apex	VP
Relays	2	1
Prox Reader	Yes	No
Inputs	4	0
Wiegand	Yes	No
Rubber / Metal Keys	Metal Only	*Both Types

**Metal Only on New Purchases*

Table 4: Keypad Comparison

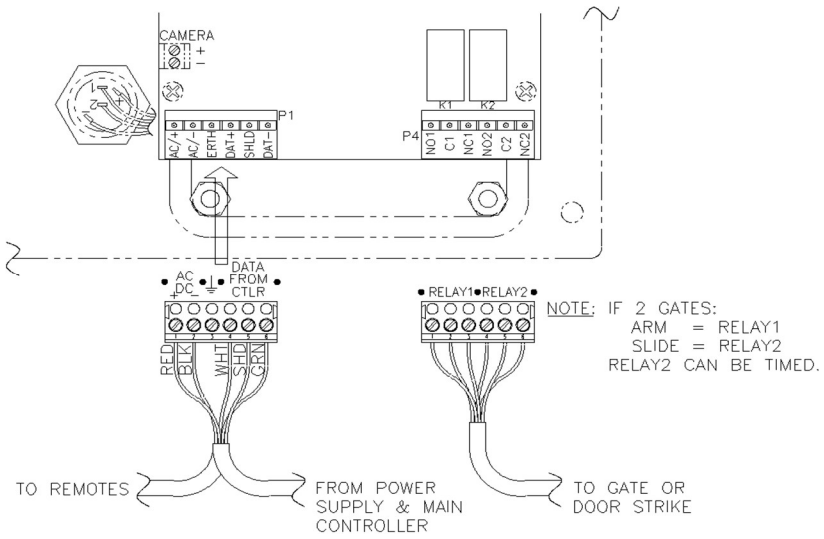
Apex Keypad

The Apex keypad is the latest and most featured of the keypads. The Apex comes in several configurations, including with card swipe, proximity reader, intercom, color camera, or elevator faceplate without an intercom. The Apex requires 12-18 V AC/DC to operate. When connecting, make sure the earth-ground connects to electrical earth ground.

Apex Power / Data / Relay Connections

P1 – Power and Data

1. DC + / AC In
2. DC – / AC In
3. Earth Ground
4. Data +
5. Shield (bare drain)
6. Data –



Drawing 7: Apex Connections

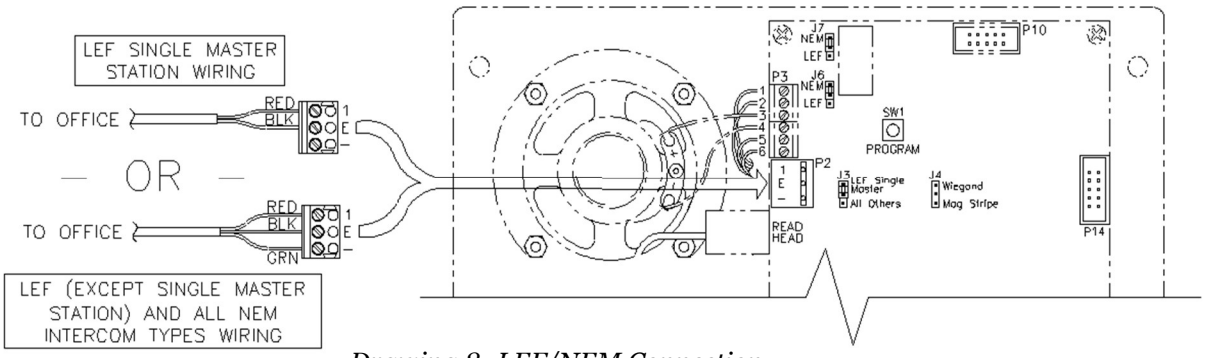
When using relays to trigger a door strike or magnetic lock, make sure you put a diode or MOV across the power supply leads to prevent the collapsing magnetic field from feeding back into the keypad.

P4 – Relays

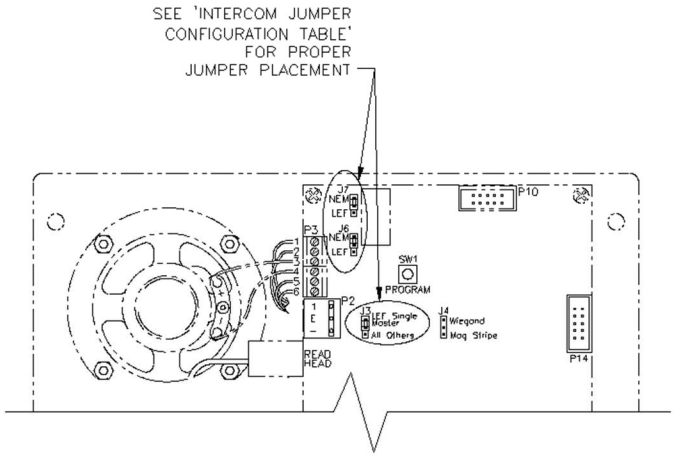
1. NO Relay 1
2. C Relay 1
3. NC Relay 1
4. NO Relay 2
5. C Relay 2
6. NC Relay 2

Apex Intercom Connection

PTI designed the Apex series keypads to work with both Aiphone's LEM and LEF intercom master stations. The LEF single master uses a two-wire connection, and the LEM or LEF multi-master uses a 3-wire connection.



Drawing 8: LEF/NEM Connection



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

Drawing 9: Intercom Jumpers

Configure the jumpers to match the type of intercom master. Use the configuration table in the drawing to set the jumpers.

Apex Inputs

The Apex has 4 inputs. You can think of inputs as trigger points used to signal an event like a door opening. Inputs are wet contacts (they put out a signal) and must connect to a dry contact (no voltage output).

On the Apex, the most frequent usage for the inputs is a door contact, request to exit, presence sensor, or intercom call.

- **Door Contact** – in the case where the keypad is controlling access through a door, you can use the keypad inputs for the door contact — allowing the software to detect whether the door is being held open or forced open.
- **Request to Exit** – in the case where the keypad is controlling access through a door. You can connect a push button or sensor on the inside of the door. The push-button or sensor triggers the relay to open the door.
- **Presence Sensor** – with this turned on, and in use, the door is disabled until it senses a closure on the input.
- **Intercom Call** – with a closure on the input, the log reports an intercom call. You could connect this to the actual intercom button to have it report in the log the activation of the intercom button. You get the advantage of a message when the intercom is not connected and having a record of the intercom usage.

Each of the inputs on the Apex has two connection points side by side on the connector.

Apex Programming

You can access some of Apex's functionality programming through the keypad. This brief guide shows some of the available in the Apex keypad programming. For a complete description of settings, refer to the Apex user manual.

Accessing the Apex Keypad Programming

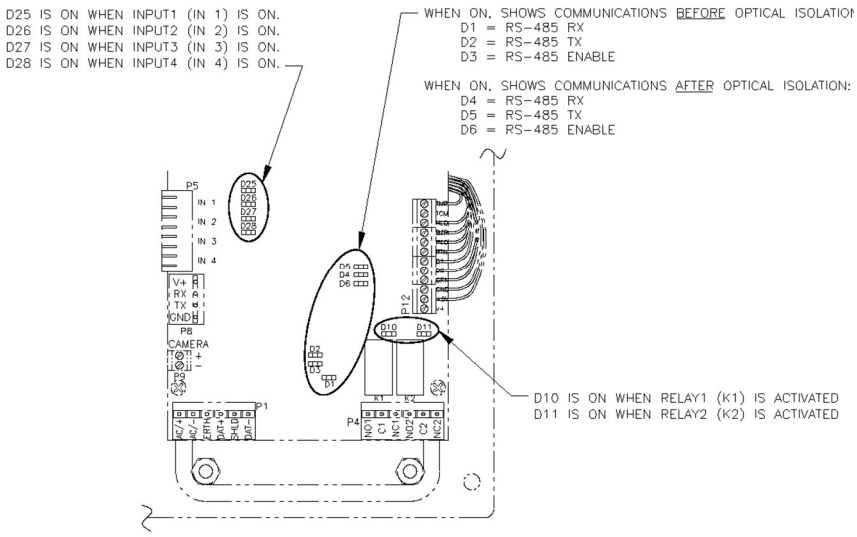
1. Simultaneously press the keys *, 0, and #
2. 8898 is the default password
3. Press the # key
4. # advances through the options
5. * changes options except where it expects a numeric value like the address

Setup Options

- **Address** – this is the unique address assigned to the device. Each device must have a different address. All numbers up to 127 are valid except for 0 and 22.
- **Communications Rate** – this is the speed at which the device communicates with the Falcon XT. The default is 9600. Use the * key to cycle through the choices. All devices in the system must communicate at the same baud rate.
- **Change Setup Password** – this allows you to change the setup password from the default 8898. Press the * key to change, use the number pad to enter the new numeric password and press #. The keypad prompts you to enter the numeric password again to confirm and press #. The setup password can contain any combination of digits up to 10 digits in length.
- **Tamper Sensor Enabled** – this setting toggles the tamper switch between enabled and disabled. Press the * key to change the setting.
- **Secure Code Entry** – this setting controls how the access code shows on the keypad's display. When set to *Yes,* the display shows a * for each digit in the code. When set to *No*, the display shows the actual number entered (not recommended).
- **Beep with Key Press** – controls whether the keys beep when pressed. Use * to change.
- **Beep with Access** – determines if the keypad beeps after entering an access code. For a valid entry, the keypad emits one long beep, and for an invalid entry, the keypad emits four short beeps. Use * to change the status.
- **Sound Buzzer with Alarm** – when on, the buzzer in the keypad sounds when there is an alarm condition. By default, this setting is *No*. Use * to change the setting.
- **Language** – changes the language the keypad uses to communicate with the user. The Apex keypad has the following languages available: English, French, Italian, Deutsch (German), Dutch, Portuguese, and Danish. Press * to cycle to the language you need.
- **Date Format** – Sets the date format. US MM/DD/YY or European DD/MM/YY. Use * to change.
- **Time Format** – set the time format. The options are 12-hour clock with AM/PM or a 24-hour European clock. Use * to change.
- **Trip Relay Offline** – allows the keypad to trip relay 1 when unable to communicate with the Falcon XT with any code entered using the pattern *<code>#. This setting is handy when you are having communication issues with the keypad. Use * to change the setting.

Apex LEDs

- D25-D28 inputs 1-4
- D1-D3 show communication before optical isolation
- D4-D6 show communication after optical isolation
- If D1-D6 are flashing, you are communicating with the Falcon XT
- D10-D11 show status of the relays



Drawing 10: Apex LED's

When mounting a keypad enclosure to a wall or pedestal, use silicon to seal the openings around the holes for the wires and the mounting bolts.

VP Keypad

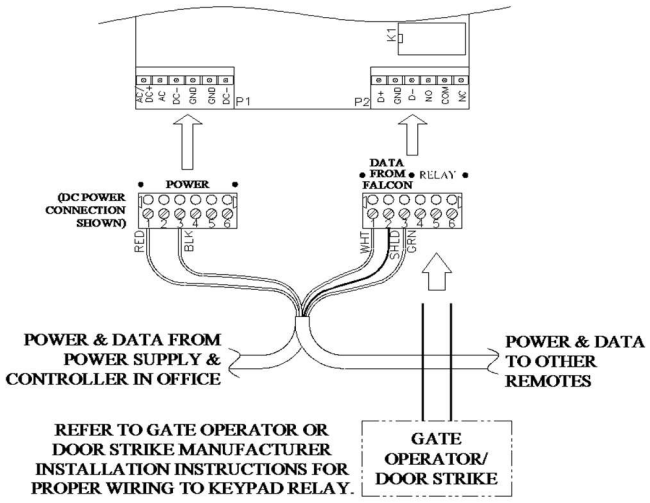
The VP keypad is a basic keypad. See the website or contact your sales representative for more information. The VP keypad requires 12-18 V AC/DC. Like the Apex keypad, connect the grounding wire to electrical earth ground. VP Power / Data / Relay

P1 – Power

- AC – Pins 1 & 2
- DC – Pins 1 & 3

P2 – Data and Relay

1. Data +
2. Shield (bare drain)
3. Data –
4. Relay NO contact
5. Relay C contact
6. Relay NC contact



Drawing 11: VP Connections

VP Intercom Connections

The VP connections for the intercom are the same as the Apex intercom connections. Refer to information on Apex intercoms, page 17.

VP Programming

The programming for the VP keypad is a subset of the Apex programming. Refer to page 19 for more details about programming the keypads. See the VP User Manual for full details on the programming options. The languages for the VP are English, French, Spanish, Italian, Deutsch (German), Danish, Dutch, and Norsk (Norwegian).

VP LEDs

D4 and D5 flash when the VP is communicating with the Falcon XT. D6 lights when the relay is active.

Review Questions

1. How many relays on an Apex keypad?
2. Relays on a VP?
3. Inputs on an Apex?
4. True or False: The location of the data wires is connector P2 on the Apex keypad.

Door Alarms

Door alarms are increasingly popular at self-storage facilities because they provide an additional layer of individual unit security for tenants and allow facilities to charge higher rental rates. PTI offers both wired and wireless door alarms. Wired alarms are very reliable and are a more cost-effective option for new facilities. Wireless alarms can be installed on occupied units, making them ideal for retrofits.

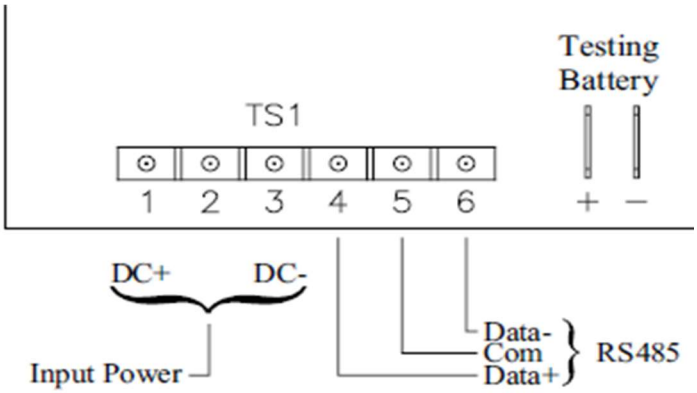
Wired Door Alarms

The wired door alarms come in configurations for 16, 32, 48, 64, 80, and 96 doors, allowing you to order the smallest block of units needed and not have a lot of excess contact points. The wired Door Alarm multiplexer requires 12 V AC/DC.

Power / Data

TS1 Connector

1. DC +
2. No Connection
3. DC –
4. Data +
5. Shield (bare drain)
6. Data –



Drawing 12: Wired Mux Connections

Dip Switch Pack SW1

The switch pack sets the address, switch type, and tamper switch status for the door alarm multiplexer.

- The value of switches 1-6 adds together to set the address of the door alarm multiplexer. Each switch is a position in the binary table. Refer to Table 5 for the values of each switch. If the switch is in the on position, the value adds to the total for the door alarm multiplexer's address.

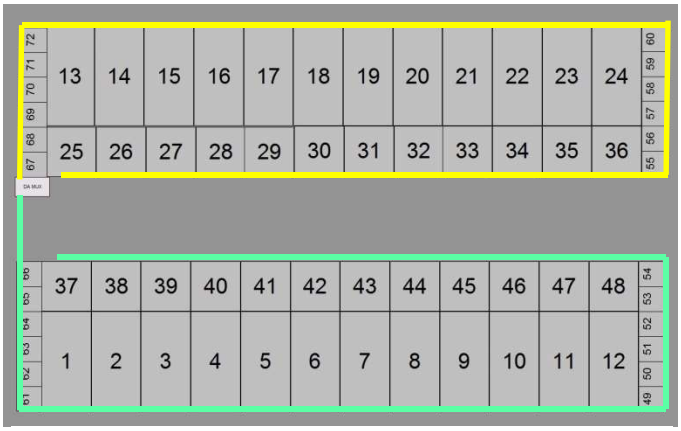
Switch	Value
1	1
2	2
3	4
4	8
5	16
6	32

Table 5: Wired Mux Dip Switch Block

- Switch 7 is for "supervised" switches. "Supervised" switches are a special kind of switch with resistance in line with the switch, causing the system to see a voltage drop rather than a short. "Supervised" switches rarely get used in self-storage.
- Switch 8 sets whether the tamper switch notification is active or not. If the switch is off, the tamper switch is active. If the switch is on, the tamper switch is disabled.
- LED 1 flash when the multiplexer is online with the Falcon XT.

Running Trunk Lines

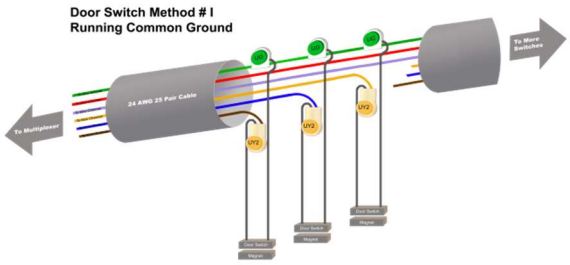
Before running trunk lines, it is a good idea to take a drawing of the site and layout the location of door alarm multiplexers. From there, you can pencil in where to run the trunk lines. See Picture 3: Running Trunk Lines for an example of laying out the trunk lines. The starting is the multiplexer, and one trunk is run clockwise around the first building (yellow line). The second trunk runs counterclockwise around the second building (green line). Refer to the multiplexer and Channel list handout for an example of the connections to the channels on the board.



Picture 3: Running Trunk Lines

Connecting Switches to Trunk Line

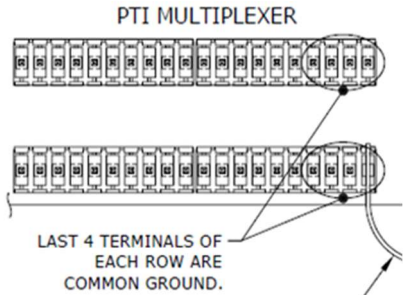
The trunk line is a 24 AWG / 50 conductor wire. When connecting to the trunk line, use a UG connector to crimp on to the common wire for that switch, and use a UY2 connector to splice into the channel wire. While there are other methods for connecting switches to the door alarm multiplexer, the method shown here maximizes the wiring and coverage of 48 doors per trunk line.



Drawing 13: Connecting Switches

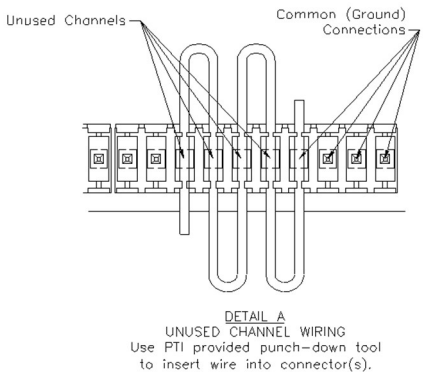
Connecting Trunk Line to Door Alarm Multiplexer

Each row on the board can handle 16 switches. Always remove the connectors from the board before punching the wires down on the connector, and always use the correct punch down tool. The last four positions on each row are commons, and all the common are electrically connected. Common grounds allow for the uses of just two commons in the 50-conductor wire. With each 50-conductor covering 48 doors, you can fill a 96-channel multiplexer with just two 50 conductor trunk lines.



Drawing 14: Common Ground

For any unused channels, you need to tie them to a common. You can accomplish this by looping a piece of wire through the unused channels to one of the commons. ***If ignored, radio signals can cause false alarms on these unused channels.***



Drawing 15: Unused Channels

Wired Door Alarm Display

The multiplexer display shows you information about the multiplexer and its status. The items in the list below rotate on the screen.

- Time
- Last Activity (Channel and status)
  - C = closed
  - O = open
- Revision (r)
- Baud Rate (b)

Wireless Door Alarms

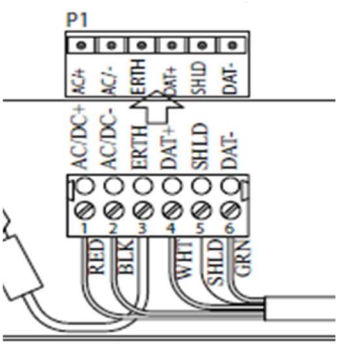
The wireless multiplexer and receiver run from 12 VDC and draw 250 mA of current. The transmitters use 900 MHz, spread spectrum, frequency hopping. In a perfect line of sight conditions, the transmitters have a range of 1000'. The typical range in less than ideal conditions is closer to 400'. The transmitters use CR123A, 3 V lithium batteries, giving them a battery life between 2-5 years. There are two different generations of PTI wireless door alarms. The FA system is the older generation and is not compatible with the newer system, the EchoStream system. You cannot mix the two different styles. When ordering replacement transmitters, make sure you know which type the site is using.

Each transmitter has a unique ID number that it transmits: the wireless receiver records this ID and the wireless multiplexer associates this ID with a channel. Finally, the StorLogix software associates the channel number to a unit.

Wiring the Wireless Multiplexer

Power and Data (P1)

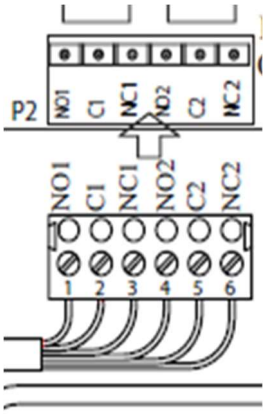
1. DC +
2. DC –
3. Earth Ground
4. Data +
5. Shield (bare drain)
6. Data –



Drawing 16: Power & Data Connector

Relays (P2)

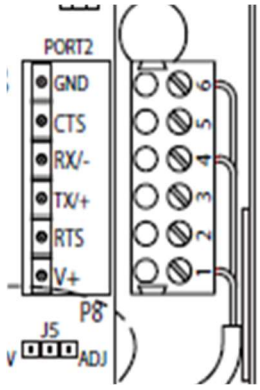
1. NO Relay 1
2. C Relay 1
3. NC Relay 1
4. NO Relay 2
5. C Relay 2
6. NC Relay 2



Drawing 17: Relay Connector

Receiver (P8)

1. V+
2. No Connection
3. No Connection
4. RX / –
5. No Connection
6. GND



Drawing 18: Receiver Connector

Wireless Repeaters

In some cases, you may need a wireless repeater to get the signal from the transmitter to the receiver. A 14 VAC power transformer powers the repeater. The repeater also has a battery backup and a weatherproof enclosure. We recommend you use a site survey kit to determine the number of repeaters for a site. Contact sales for information on renting the survey kit.

Installation of the Transmitters

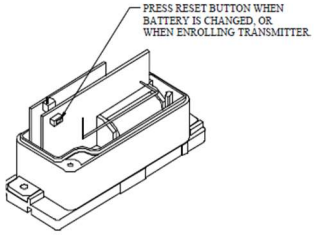
Transmitters can mount on roll-up doors, swing doors, and slide doors. With the roll-up door, you can mount the transmitter to the door jamb or the door header. For swing and slide doors, mounting to the header is usually the best option. See the Wireless Door Alarm System manual for detailed drawings and instructions on mounting the transmitters. The mounting plates stack together and allow you to move the transmitter out to get better alignment with the magnet.

When positioning the transmitter, you can use a test transmitter that lights an LED once the transmitter and magnet are aligned. The test device helps you position the transmitter mounting plate. The transmitter has alignment markings on the case for horizontal and vertical mounting. For the transmitter to work correctly, there must be less than a ½ inch gap between the magnet and the transmitter.

Register a Transmitter

When ordering a new system with wireless door alarms, PTI registers the transmitters for you. However, if you need to add or replace transmitters on a system, you need to register the transmitters with the system. If you are replacing a transmitter, the system asks you whether to replace the existing transmitter already registered for the channel.

1. On the wireless multiplexer, select the option to register a new transmitter
2. Enter the channel number to register
3. Press the “Reg A” button on the receiver
4. Press “Reset” on the transmitter



Drawing 19: Wireless Transmitter

Programming the Wireless Door Alarm Multiplexer

The wireless multiplexer has several programming options. You must use the keypad on the front of the multiplexer to complete programming, just like the Apex and VP keypads. The default programming password is 8898.

- **Address** – this is the unique address assigned to this unit
- **Communications Baud Rate (RS-485)** – this is the communication speed to the Falcon XT. Set to the same baud rate as the other devices in the system
- **Backup Baud Rate** – the communications speed for the RS-232 port for communicating with the RX900 backup utility
- **Tamper Enable / Disable** – Enable or disable the reporting of the status of the multiplexer's tamper switch.
- **Keypad Beeps** – determines whether the keys beep when you press them
- **Check-in Time** – is the number of minutes before the StorLogix counts a transmitter as failing to report in. In most cases, you leave this at the default

LED Lights on the Wireless Multiplexer

- D1 – D6 flash when communications with the Falcon XT is good
- D39 and D41 flash when there is communication with the wireless receiver
- D10 and D11 show the status of the two relays

Review

1. What switches do I turn on to set a wired door alarm mux to address 3?
2. How many door switches can I connect on each row of the wired door alarm mux?
3. How many commons are there on each row on the door alarm mux?
4. True or False: You cannot use Wireless transmitters with swing doors.

Other PTI Devices

8 Channel Relay Multiplexer

The 8 Channel Relay multiplexer adds a bank of relays to the system for triggering devices. It is useful for elevator control and lighting control because it provides a central location to tie in the elevator or other control devices. In addition to the 8 relays, the multiplexer has 8 inputs. You can use 12-18 V AC/DC to power the Relay Board and address the multiplexer using a bank of switches.

Relay Connections

Each relay uses three positions on the punch down, NO, C, and NC. As with the door alarm board, remove the connector before punching the wires down on the connector and use the correct punch down tool. These relays are dry contact (no output voltage) relays.

Addressing the Multiplexer

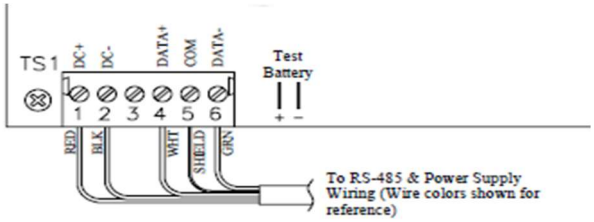
- Turning on a switch adds its value to the address
- Each switch acts as a binary placeholder
- Remember not to duplicate addresses
- Switch 6 controls the baud rate for the RS485 communications. Off for 9600 (default) and on for 1200.
- Switches 7 and 8 have no function on the Relay multiplexer

Switch	Value
1	1
2	2
3	4
4	8
5	16

Table 6: Relay Mux Dip Switch Block

Power / Data Connections

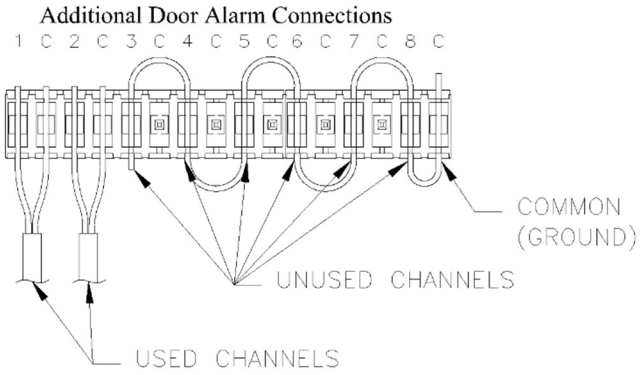
1. DC + / AC
2. DC – / AC
3. No Connection
4. Data +
5. Shield (bare drain)
6. Data –



Drawing 20: Power & Data Connector

Input Connections

The inputs on the 8 Channel relay multiplexer work the same way as the inputs on the Falcon XT and the wired door alarm multiplexer. They expect closure from a dry contact. Unlike the door alarm multiplexer, each input has its common. On the punch down, the common is after the input connection. Just like with the alarm multiplexer, you want to tie unused inputs to a common.



Drawing 21: Unused Channels

8 Channel Relay Multiplexer Display

- Time
- Last Activity (Channel and status)
  - C = closed
  - O = open

Extra Features

- There is an LED for each of the 8 relays, showing when they activate.
- D15 blinks when the multiplexer is communicating with the Falcon XT
- Key lock override switch – when activated, reverses the state of all the relays, allowing you to bypass the system.

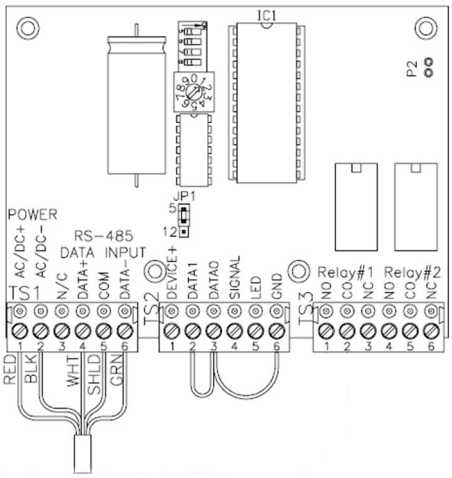
PTI Wiegand Module (PWIE)

The PTI Wiegand Module allows you to connect to Wiegand devices when using the Wiegand inputs on the Falcon XT is not practical. You can also use the PWIE as a 2-relay device in situations where using an 8 Channel Relay multiplexer is too much. The PWIE requires 12-18 V AC/DC to operate.

PWIE Connections

TS1 – Power / Data

1. DC + / AC
2. DC – / AC
3. No Connection
4. Data +
5. Shield (bare drain)
6. Data –



Drawing 22: PWiE

TS2 – Wiegand Connection

1. + voltage output (5 or 12 sets by jumper JP1)
2. Data 1
3. Data 0
4. Signal
5. LED
6. Ground

The exact connections and wiring are dependent on the Wiegand device used. At the very least, you need the Data 0, Data 1, and Ground connection. Some devices do not have a signal or an LED connection. *If you are no using the Wiegand port, do not remove the jumper wires in connectors 2, 3, and 6; however, if you are using the Wiegand port, remove these jumpers.*

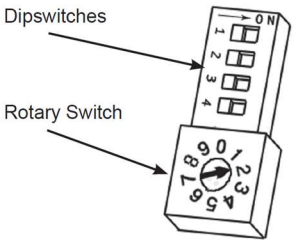
TS3 – Relays

1. NO Relay 1
2. C Relay 1
3. NC Relay 1
4. NO Relay 2
5. C Relay 2
6. NC relay 2

PWIE Address

To set the address for the PWIE, you turn the rotary switch to set the one's place. The dip switches add to this value:

- Switch 4 adds 10
- Switch 3 adds 20
- Switch 2 adds 30



Dipswitches	
OFF	ON
1 Terminating Off *	Terminating On *
2 Address + 0	Address +30
3 Address +0	Address +20
4 Address +0	Address +10

Rotary Switch
0 – 9 adds 0 – 9 to the Address

Drawing 23: PWiE Address Block

Switch 1 turns the termination on or off. Leave this set to off unless told to switch on by PTI technical support.

Core Graphics

PTI Core Graphics is a visual representation of the site, using colors to show the rented, vacant, suspended, open, on-site, and alarm status for each unit. PTI designed Core graphics to operate on a separate computer rather than running on the computer with StorLogix installed. The Core Graphics connects to the Falcon XT through a USB to RS-485 converter. A wireless remote allows you to control the Core Graphics.

Picture 3: Core Graphics Adapter

The USB to RS-485 converter shows as a communications port in the computer's device manager. You need to know what port was assigned to configure the Core Graphics software. The manufacture of the converter marked it with +, –, and S, which correspond to the Data +, Data –, and Shield on the Falcon XT's Remote Devices connector.

Core Graphics Software Setup

1. Install the Core Graphics software from the media on the designated Core Graphix computer. Note: this is not the same computer with StorLogix installed.
2. Copy the site's PTI graphics file to "C:\Program Files\Site Builder."
   - If a 64-bit system "C:\Program Files (x86) \Site Builder."
   - Sample site file name: MySite.ptix
3. Rename or delete the demo.ptix file

4. While in "C:\Program Files(x86) \Site Builder", open "Licensing Tool.exe."
   - Click the Register Button
   - Enter the Registration code found on the inside of the CORE Graphics Case.
   - Enter the name of the site.
   - Click the Register Button
5. On the computer desktop, open the Core Graphix Program
   - Press the "S" key on the keyboard.
     1. **COM Port**: select the port for the RS-485 converter
     2. **Com Speed**: set to match the same baud rate as the other devices in the system (default 9600)
   - Press the "S" key on the keyboard.
6. Press the "ESC" to close the CORE Graphics program and reopen it

PTI included a Site Builder program with the Core Graphics software. Site Builder allows you to modify or create site maps. Always make a backup of the existing site map before making changes to it.

Review

1. If you do not use some of the input channels on the 8 Channel Relay Mux, what should you do?
2. What switches would you turn on to set the 8 Channel Relay Mux to address 11?
3. True or False: You should always remove the two wires from the Wiegand input of the PWIE even if you do not plan to use the Wiegand input.
4. What switches would you turn on to set the PWIE to address 11?

Hardware Troubleshooting

We designed this module to give you some ideas of the things to look for when there are hardware issues. When troubleshooting, work through one stage at a time until you can identify the cause of the problem. Being able to eliminate potential causes of the problem helps better identify the issue. Programming issues and setup issues usually cause a device to always fail rather than intermittently fail.

4 Most Common Problems

1. **Duplicate addresses** – duplicate addresses can cause devices to misbehave and give erratic results. For instance, if you have two devices addressed as "1," the system cannot distinguish between them. When the system gives the command for "1" to fire a relay, it is difficult to predict which of the two devises get the command first.
2. **Wiring** – wiring gets old and corroded. The new wire gets pinched and stretched. Never underestimate the possibility of the issue being in the wiring.
3. **Power** – just because a device has a display and shows light blinking doesn't mean the device has the proper power input. Make a habit of always testing the power at each device to make sure it is getting the proper voltage.
4. **Improper Grounding –** make sure all devices are connected to earth ground as outlined in the manuals.

RS-485 General Troubleshooting

At the Falcon XT, you can use a volt/ohm meter set to the DC scale to test the data voltages. Between the Data + and the shield, or the Data – and the shield, you should read between 1.5-5 VDC. At the device with the data line connected, you should read about the same, which means the wiring is proper, and the data signal is getting through. If not, you have a wiring issue, or the device is overloading the system. Disconnect the data line and do the same test at the end of the wire to eliminate the device. If you still do not get a voltage reading, you have a problem with the wiring.

Never underestimate the value of swapping a working device with a similar device that is not working. If the problem follows the device, you have an issue with that device; however, if the problem stays at the location, you have a problem with the wiring or power.

Short-Wire

Another useful troubleshooting method is short-wire. Disconnect all devices from the Falcon XT's Remote Devices connector. Take a 1 to 4-foot piece of 18 AWG 4 conductors with bare drain and connect one of the devices to the Falcon XT using this known good wire. If the device works on this short-wire, the device is probably okay. For keypads, you probably want to disable the tamper switch when using this method.

Socketed IC Replacement

- ISL3152EIPZ – RS-485 Transceiver used for the RS-485 communication between devices. If defective can impact the communication between devices. See Table 7.

Device	Socket
Apex	U2
VP	U3
XT	U9
Door Alarm Mux	UU16
Relay Mux	IC8
Wireless Door Alarm	U2
PWIE	IC3

Table 7: RS-485 IC Sockets

Relay Problems

If a relay is not triggering a device, first check to make sure that the software has the correct relay assigned, and the device is assigned the correct type. See (page 71) for details on relay assignments. Make sure the software is not holding the relay closed or open.

Over time, relays can become pitted or fused. Disconnect the wires from the relay's connector and use a volt/ohm meter on the ohm range to test the relay for open and close when it is triggered. If the meter shows the relay is working, short the wires at the relay together. Doing so should trigger the device. If not, the issue is with the wiring or the device.

Keypad Problems

Problems with keypads are probably the most reported issues. Refer to page 33, as this outlines the best approach to communication problems.

- Online / Offline messages indicate a problem with the devices or wiring in the RS-485 network (see page 33).
- "Please Wait" message and nothing happens points to either an intermittent communications problem (see page 33) or a duplicated address.
- "Out of Service" message at the keypad means the keypad is offline.

Keypads Troubleshooting

Keep in mind that even when the keypad display is on, the power could be below spec. Power below 12 V causes issues. Always look for loose, shorted, or broken connections on your wiring. You want to double-check the baud rate and address configuration. In rare instances, there is the possibility that the board is defective; this is one reason we recommend swapping with a "known-good" device.

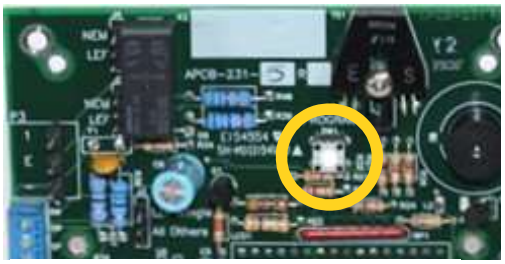
Keypad Tamper Alarm

Tamper alarms or a message from the keypad saying "Device Has Been Tampered With" can indicate that some tampering has occurred device or that the optical tamper sensor needs cleaning. You can temporarily disable the tamper sensor in the keypad's programming until the resolution of the problem.

Picture 4: Apex Buzzer

Keypad Factory Reset

Sometimes, it becomes necessary to reset the keypad back to factory defaults.



Picture 5: Keypad Reset Button

1. Remove the keypad power
2. While holding down the “Program” button, plug-in the power.
3. The keypad beeps and displays a message about restoring the defaults. Press the * key to answer yes.
4. The keypad takes you directly into the setup settings.

REMEMBER: A factory reset sets everything back to defaults including the address to 1 and the baud rate to 9600.

Wired Door Alarms Troubleshooting

Wired Door Alarm issues are a little less ordinary. Always keep in mind the (page 33) as this outlines the best approach to communications problems.

- Online / Offline messages indicate a problem with the devices or wiring in the RS-485 network (see page 33).
- When there are issues with the trunk line wires, you can get false alarms. Shorted wires through the trunk line or at the end can create shorted connections. Always make sure the wires are isolated from each other at the end of the trunk line.
- When doors get older, they start to get sloppy and move when the wind is blowing, and this can cause false alarms when the gap between the magnet and the switch becomes higher than the recommendations.
- On some older systems, you can try replacing the punch down the connector.

Testing Switch Connections at the Multiplexer

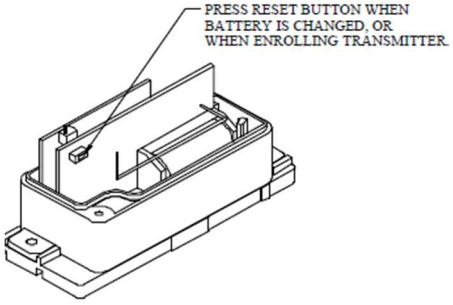
Using your volt/ohm meter on the DC scale, you can determine whether the switches are working correctly. When the contact is open, you should read between 4.9-5.0 VDC between the channel and one of the commons. When the contact is closed, you should read 0 VDC. A reading between 2.5-3 VDC points to a bad connection or a faulty switch.

Wireless Door Alarms Issues

Besides the usual communications issues, you can have issues with communication with the transmitters. When the gap between the transmitter and the magnet is wider than ½ inch, you can get false alarms. If you get a "Check-in Fail" message on a transmitter, try replacing the battery. If that does not resolve the issue, try replacing the transmitter. If you have a large group of transmitters in the same area failing to check-in, you may need to add a repeater.

Wireless Transmitter Battery Replacement

1. Open the transmitter case (this reports a tamper on the transmitter)
2. Remove the old battery
3. Snap the new battery in place (pay attention to polarity)
4. Press the reset button on the transmitter
5. Close the case back up



Drawing 24: Wireless Transmitter Reset Button

Transmitter Replacement

1. Clear the channel in the wireless multiplexer
2. Register the new transmitter in the multiplexer and receiver

Refer to the Wireless Door Alarm System installation manual for details.

Review

1. Name the 4 most common issues?
2. True or False: Swapping a non-working device with a working device is a useful troubleshooting method.
3. True or False: Two devices with the same address do not affect the system.
4. What are you trying to accomplish by short-wiring a device to the Falcon XT?

StorLogix Install/Setup Wizard

How the Software Components Work Together

- **StorLogix** is the central player in the operation of the PTI software. StorLogix communicates to the other components through its various services.
  - The **LogixServer** service provides communications between the StorLogix software and the Falcon XT. The LogixServer allows the software to update the memory in the Falcon XT with setup changes to tenant and unit information as well as updating activity from the Falcon XT.
  - The **Microsoft SQL PTI Server** is the database instance that records all the settings and activities in the system. Event information is held in the Falcon XT's memory until it can update through the LogixServer to the database.
  - The **StorLogix Interface** service processes the information coming from the account management software. The service updates the database and passes the information on to the LogixServer to send it to the Falcon XT. StorLogix Interface does not send any information back to the account management software.
  - The **StorLogix Sync** service interfaces with the StorLogix Mobile App, sending information back and forth.
  - The **StorLogix Sync Push** service communicates with the EasyCode server, which communicates with the EasyCode App.

StorLogix Installation

When you insert the StorLogix CD, most computers autorun the installation. If, for some reason, you must manually start the installation process, you want to run the setup.exe file in the root folder of the StorLogix installation DVD ROM.

1. The first step of the installation installs all the prerequisites for the StorLogix program, including the Microsoft SQL and tools, drivers for the USB, and the .NET framework.
2. The most important of these prerequisites is the Microsoft SQL Server.
   - Select whether the computer is the StorLogix server computer or just a workstation.
   - The StorLogix server has the database installed.
   - All workstations must access the database on the server.

3. Once the prerequisites installation is complete, the StorLogix software installs.
    - The software installs the services: LogixServer, StorLogix Interface, StorLogix Sync, and StorLogix Sync Push.
        - If you are installing on a workstation, select custom installation, and only install the main StorLogix program.
    - The software also installs the main StorLogix program and the Graphical User Interfaces for the services.
        - **StorLogix** – the main program
        - **EventViewer** – a program for viewing events and creating custom reports.
        - **LogixServer Dashboard** – is the user interface for setting up the LogixServer service.
        - **StorLogix Interface UI** – is the user interface for the StorLogix Interface service.
        - **Overlock** – interface for setting up Overlocks.

The installation sometimes requests a computer reboot. For the best results, reboot when prompted. After the reboot, the installation process should continue automatically.

StorLogix Configuration Wizard

The first time you run StorLogix, the program presents you with the Setup wizard. First, the software prompts whether you want to restore from a backup or restore point. Clicking the **Yes** button takes you to the Restore wizard. This option is helpful when you are transferring to a new computer or replacing a computer.

If you are upgrading from Falcon 2000, you receive a prompt to import the Falcon data. If you only have a simple site with a few keypads and the site is using an accounting management program, you get a cleaner setup just using the Setup wizard.

Next, the software prompts as to whether the site has PTI or DigiGate devices. Select the correct setting for the devices in the site's system.

Site Information

Picture 6: Site Info Box

The site information screen is next. Fill in all the red boxes, with the necessary information about the site and the manager. The site information (except for the **Site Code**) is changeable at any time. Under the **Site Manager** section, the **Password** is the password used for the manager to log in to the StorLogix software. The **Gate Code** is the access code assigned to the manager.

Under the **Access Devices**, pick the closest layout to the system you are installing or make a good starting point. The choices cannot cover all situations. The **2 Line Display** is the VP style keypad, and the **4 Line Display** is the Apex. If you have a mix of keypads, select one and correct the types in the software setups.

Gate Access Hours

Picture 7: Time Schedule Box

The next screen is the normal gate access hours. Set the access hours for each day of the week. Use the double-arrow button to copy the "time-schedule" from Monday to the other days of the week.

A holiday is a particular time slot for days defined in the software as holidays.

Check **Closed** to mark any of the slots as closed (12 AM – 12 AM).

To set 24-hour access, set the open time at midnight and the close time at 11:59 PM.

Picture 8: Logix Server Setup Wizard

LogixServer Setup Wizard

Next is the LogixServer Setup Wizard. Select the connection type and click the Next button.

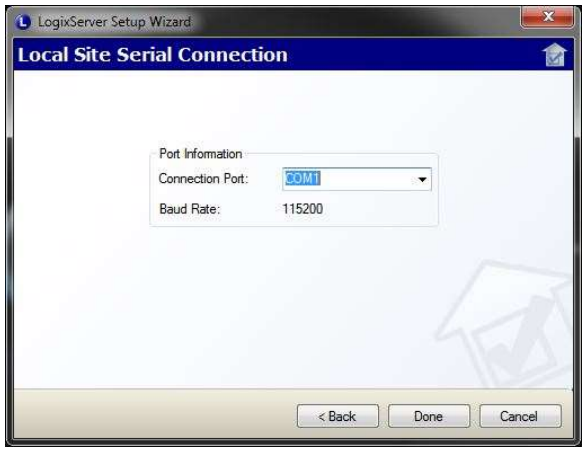
- Serial Port
- USB
- Local Network (LAN)
- Dial-up
- Internet (WAN)

Serial Connection

For a serial connection, select the serial port the Falcon XT is connected to and click the **Done** button.

The serial connection does require an RS-232 or USB-to-serial adapter at the computer to connect to the Falcon XT.

A serial connection requires a special cable purchased from PTI.



Picture 9: Serial Connection Box

Do not use a serial connection unless you have no other choice. The serial connection is an older technology included for legacy systems. Computers with serial ports are usually a order, costing more money. The site can use a USB to serial adapter, but the adapter adds another failure point to the system. Whenever possible, we recommend using a USB or Ethernet connection.

Picture 10: USB Connection Box

USB Connection

For a USB connection, make sure the USB cable is connected to the computer and the Falcon XT and make sure to install the USB drivers. The wizard prompts you with a reminder to connect the cable.

The wizard automatically detects the USB connection and place the correct port in the Connection Port. If the wizard does not detect the connection, double-check your connection and driver installation.

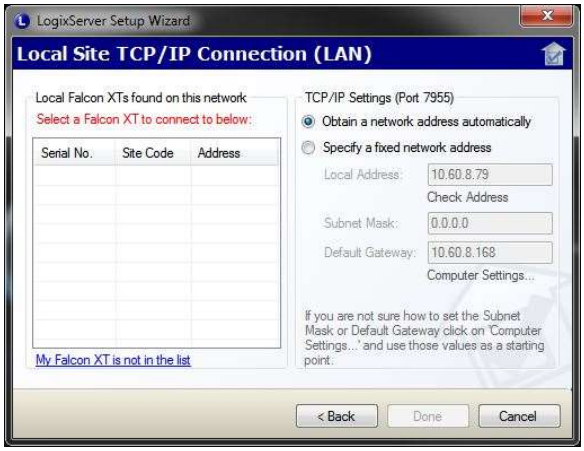
Click the **Done** button to save the settings.

Local Network Connection (LAN)

When you select a LAN (Local Area Network) connection, you might get a prompt from the firewall requesting access permission. Select **Allow**.

The list box shows the Falcon XT controllers located on the local network. Select the Falcon XT from the list box.

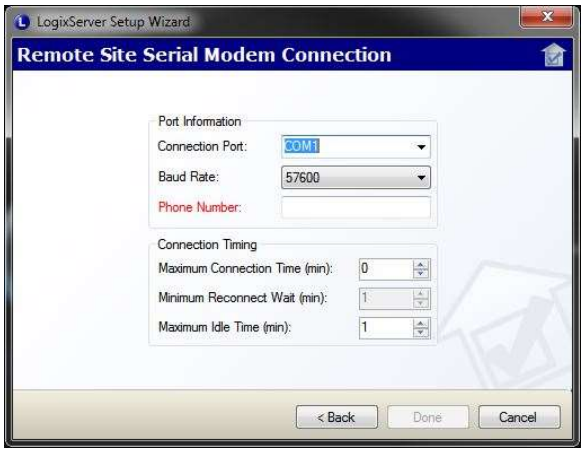
You can have the Falcon XT obtain its IP address automatically or specify a fixed IP address. Which one you choose depends on the site's network configuration.



Picture 11: Ethernet Connection Box

When specifying a fixed IP address, you need to fill in the **Local Address** to assign the Falcon XT, the **Subnet Mask** for the local network, and the **Default Gateway** for the local network.

Click the **Done** button to save the settings.



Picture 12: Dial-up Modem Connection Box

Remote Serial Modem Connection

When connecting to a remote site using a dial-up serial modem, select the **Communications Port** the modem uses to connect to the StorLogix computer. Select the highest **Baud Rate** the modem allows.

Leave the **Connection Timing** settings at the default unless told to change by PTI technical support.

Do not use a serial modem connection unless you have no other choice. The serial connection is an older technology included for legacy systems. Computers with serial ports and dial-up modems are usually an order, costing more money. Whenever possible, use a Broadband internet connection for remote sites.

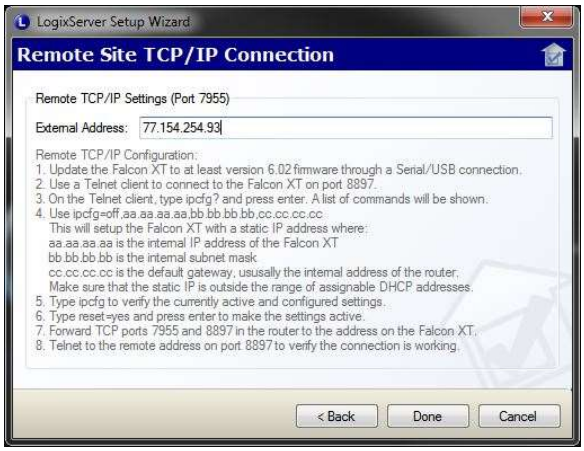
Click on the **Done** button to save the settings.

Remote Broadband Internet Connection

For a remote Broadband internet connection, obtain a static IP address, from the ISP, for the remote site.

Enter the static IP in the **External Address** text box.

Remote connections require programming the Falcon XT and the remote router for a remote connection.



Picture 13: Remote Site Connection Box

Remote Site Falcon XT Setup

1. Use a Telnet client (like Putty) to connect to the Falcon XT on port 8897.
2. Use ipcfg=off, aa.aa.aa.aa,bb.bb.bb.bb,cc.cc.cc.ccc
   - aa.aa.aa.aa is the internal IP address of the Falcon XT
   - bb.bb.bb.bb is the internal subnet mask of the local network where the Falcon XT is located
   - cc.cc.cc.cc is the default gateway of the network where the Falcon XT is located

3. Type ipcfg to verify the current active and configured settings.
4. Type reset=yes and press enter to make the settings active. (You can also press the Reset button on FXT)
5. Forward TCP ports 7950,7955 and 8897 to the internal IP address of the Falcon XT in the remote site's router.

Picture 14: Management Software Selection Box

Management Software Settings

Select the management software the site is using.

Each selection has its default settings, making the settings as simple as selecting from the dropdown list. If needed, you can adjust the setting later in the StorLogix Interface UI.

For SiteLink, select **SiteLink Navigator** to get the correct settings for the interface.

First Run After StorLogix Configuration Wizard

After going through the Configuration Wizard, the program closes. When you start StorLogix again, the software prompts you with the last remaining setup options.

Software License

When the Software Licensing window pops up, you have three options:

1. **Continue Demo** – this option allows you to continue in demo mode without registering the software. The demo mode is valid for 30 days after the software is first installed on the computer. Click the **Continue Demo** button to continue without registering or extending.

Picture 15: Software License Box

2. **Extend Demo** – this option allows you to enter an extension code to extend the demo mode. You can use this to allow the site to continue to operate after the demo mode expires but does not fully register the software. Enter the serial number in the **Extension Code** text box, using capital letters and dashes. Click the **Extend** button to activate the extension. You can obtain an extended serial number from the PTI Sales Department.

Picture 16: Extend Demo Box

3. **Register** – this fully registers the software to operate on the current computer. You can find the serial number on the back of the StorLogix installation CD case. Enter the serial number in the **Serial Number** text box, using capital letters and dashes, and the site name in the Name text box. Click the **Register** button to activate the registration.

Picture 17: Registration Box

Choose A View

PTI designed t**he Classic view** is a more familiar interface for those converting from Falcon 2000.

StorLogix's view has a modern interface and gives you access to more options. Unless you have a reason to do otherwise, you want to use this view.

Picture 18: Software View Selection Box

QMS Mode is a special mode that allows you to operate without the use of units for applications other than self-storage or where unit numbers are not practical. In "QMS Mode," StorLogix is the only view available.

Picture 19: Apex Description Box

Site Name for Keypad Display

Apex keypads can display the site name on their displays. Verify the site name is correct and click the **No** button to continue without making changes to the site name. Click the **Yes** button and get the window to make changes to the site name for these displays. The **Cancel** button closes the windows without making any changes.

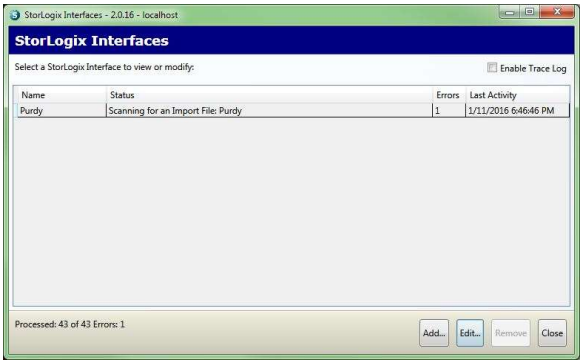
StorLogix Interface

Picture 20: Site Name Change Box

StorLogix Interface reads the information sent from the account management software into StorLogix. The StorLogix Interface runs as a Windows service, which starts automatically when Windows boots. You do not have to open the StorLogix Interface user interface window for the data to update. The window is just for checking the status and changing the setup. On the first download from the account management software, it shows a preview.

StorLogix Interface User Interface Window

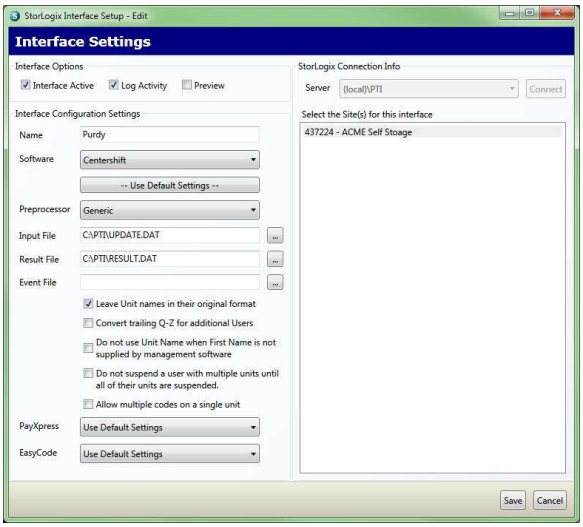
The main window displays the current set up interfaces. You only need one interface for each site, and when one database in the management software controls multiple sites, you only need one interface in the StorLogix Interface as well. The **Add** button allows you to add a new interface. To edit an existing interface, select the interface you want to edit and click the **Edit** button. The **Close** button closes the user interface window. The **Remove** button deletes an interface that is no longer needed. You must deactivate the interface before removing it.



Picture 21: Storlogix Interface Screen

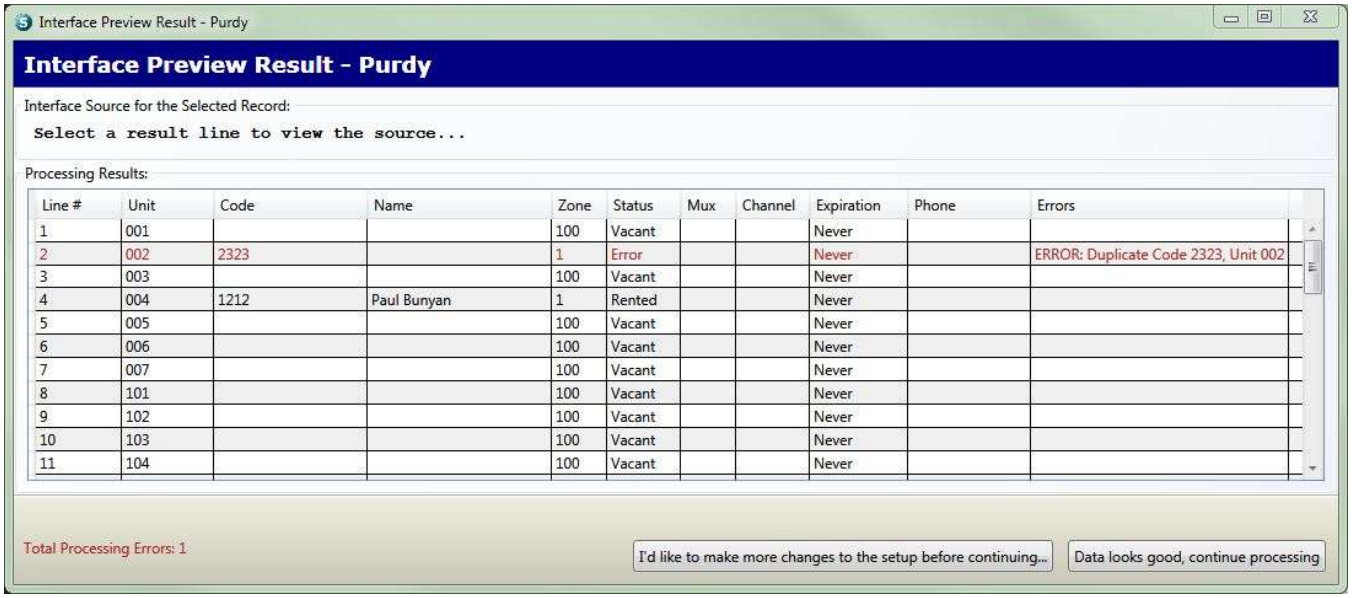
StorLogix Interface Setup Window

The setup window defines the settings for the interface. You can use the site's name for **Name**. From the **Software** dropdown list, select the account management program the site is using. In most cases, the **Preprocessor**, **Input File**, and **Result File** fill in with the correct settings. Select how the site wants to apply **PayXpress** and **EasyCode**. In the site list, select the site(s) that apply to the interface. Click the **Save** button to save the settings. You receive confirmation prompts from the program for saving the settings and preview if there is a check in the **Preview** box.



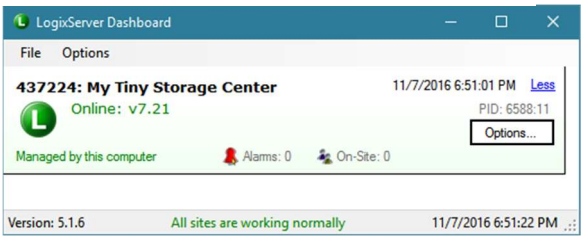
Picture 22: Storlogix Interface Settings

StorLogix Interface Preview



Picture 23: StorLogix Interface Preview Screen

StorLogix Interface creates a preview the first time the account management software sends information to StorLogix after the activation of the preview setting. Select the "**I'd like to make more changes to the setup before continuing...**" button to make changes to the interface setup. The setup window opens and allows you to make changes. Changes may include



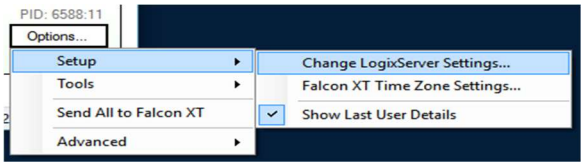
Picture 24: LogixServer Dashboard

formatting unit numbers, the management software program used, the processor, and other settings. Once you make your changes and save the new settings, the software generates a new preview. Select the **Data looks good, continue processing** button to accept the current settings. Once you accept the settings, the software turns off the preview, and StorLogix Interface automatically processes any information coming from the account management software.

LogixServer Dashboard

The LogixServer Dashboard allows you to see the current connections to the Falcon XT(s) for the site(s). The dashboard shows you the Site ID, site name, and connection status for each site in the system.

The **Options** menu button allows you to make changes or perform specific actions on the site. You can select **Send All to Falcon XT** to reset the data in the Falcon XT.

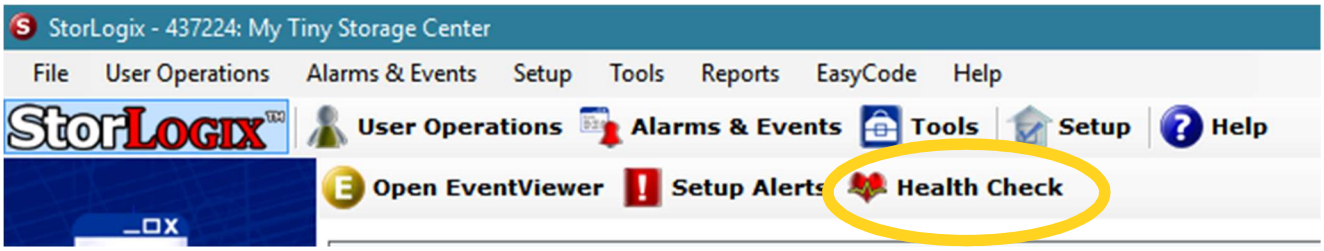


Picture 25: Accessing LogixServer Settings

Under the **Setup** menu, **Change LogixServer Settings** opens the **LogixServer Setup Wizard** (see page 41). **Falcon XT Time Zone Settings** allows you to change the time zone in the Falcon XT to a different time zone than the computer default.

Other options allow for restarting the Falcon XT or the LogixServer, and the ability to verify that the Falcon XT firmware is up to date.

Health Check



Picture 26: Accessing Health Check

The **Health Check** report gives you the status of all the devices, including the Falcon XT. If the Falcon XT is not connected, the report shows the last known status. The Falcon XT status includes the firmware version, serial number, and status of the input and output power. The report also shows the online status of all the devices, the type assigned in the software, and the type read from the device.

Health Check

Falcon XT Status

Site Code:	437224	**Power In:**	31.596000	**Power State:**	On
Model:	PXT-BU-UET-82-5P	**DC Out:**	13.818000	**DC Out State:**	On
Serial:	11960	**Battery:**	13.803000	**Battery State:**	Charged
Manufacture Date:	90423			**A/I Device Power:**	Devices On
Firmware:	7.21				

Device Online Status

Device #	Set Type	Read Type	Status	Description
1	Apex Series Keypad	Not Defined	Offline	Entry Keypad
2	VP Series Keypad	Legacy Code	Online	Exit Keypad
4	Relay Board, 8 Channel	Not Defined	Offline	Eleveator Control
5	Falcon Wiegand Module	Not Defined	Online	Elevator Prox
6	Legacy Input	Not Defined	Offline	Input Device 6
128	Controller Wiegand Input 1	Not Defined	Online	Falcon XT Wiegand 1
129	Controller Wiegand Input 2	Not Defined	Online	Falcon XT Wiegand 2

Communication On/Off Log (Last 30 Days)

Date	Time	Device	Description	Data
Monday, November 7, 2016				
	5:34:35 PM	6 - Input Device 6	Comm Error	
	5:34:40 PM	6 - Input Device 6	Comm On	

Picture 27: Health Check Report

The report also shows you the recent communication events with different devices in the system. You get a report of the users on-site, recent alarms, and the status on any open doors.

This Health Check report is a useful tool for quickly evaluating the status of the system.

Review

1. True or False: You can run StorLogix on multiple computers on the local network.
2. Name the methods for connecting the computer to the Falcon XT.
3. What is the quickest way to determine the online status of the devices connected to the Falcon XT?
4. True or False: It is necessary to have the StorLogix Interface window running for it to update StorLogix.

DoorBoss

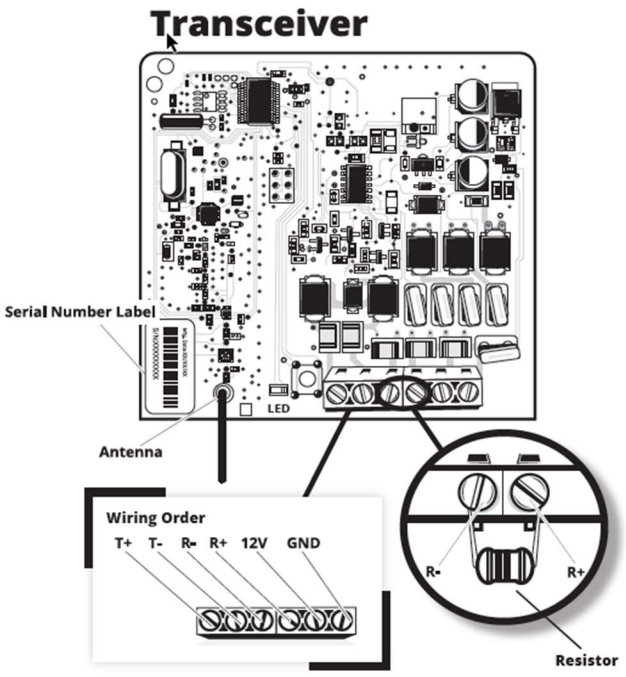
The PTI DoorBoss System is composed of DoorBoss locks, transceivers, and repeaters. The system provides additional access and security control that integrates with a PTI Falcon XT Access Control system. The DoorBoss lock is a battery-powered, radio-actuated, locking device that controls access to the storage unit. Once extended, the actuator blocks the door hasp, providing a positive lock that effectively prevents the door from being opened. The DoorBoss System helps to protect storage units from unauthorized use or vandalism and assists in preventing access to storage units for delinquent payments.

Transceiver

The transceiver is a radio frequency (RF) device that is wired to the Falcon XT Access Control System. The transceiver allows communication between the Falcon XT Access Control System and the DoorBoss locks used to control individual doors.

Components

- LED
  - The LED illuminates when the transceiver has power.
- Antenna
  - Used to communicate with the repeaters and DoorBosses
- Pigtail
  - Pigtail assembly used to connect the transceiver to the Falcon XT controller.
- Resistor
  - 100-ohm ¼ watt
- Serial Number Label
  - Each transceiver is assigned a five-digit serial number used in adding the transceiver to the Overlock software.
- Weather-Proof Enclosure
  - Allows the transceiver to be mounted outside.

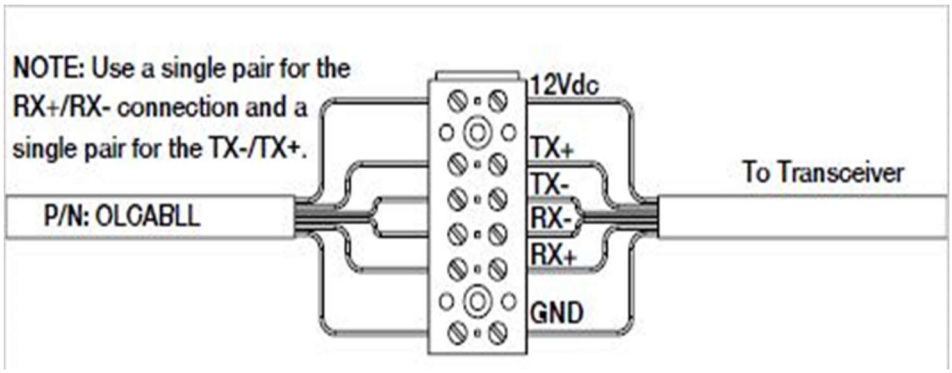


Drawing 25: DoorBoss Transceiver

Installation

Wiring

- 12VDC
  - Yellow Wire
- TX+
  - Red Wire
- TX-
  - Green Wire
- RX-
  - Black Wire
- RX+
  - White Wire
- GND
  - Bare Drain



Drawing 26: Transceiver Connection to Falcon XT

Other Considerations

The maximum wiring distance from the start of the pigtail to the last transceiver, on the RS-422 network, is 2000ft or 610m. The maximum number of Transceivers that can connect to the Falcon XT is four, with the 100-ohm ¼ watt resistor getting installed on the last transceiver in the chain. Finally, the signal range for a DoorBoss transceiver is 1500ft or 457m.

Repeater

Repeaters can be added to the DoorBoss System to extend the range of the transceiver up to 1500ft or 457m, depending on the conditions of the site. The repeater provides a secure, reliable wireless mode of communication with the transceiver and the DoorBoss locks.

Components

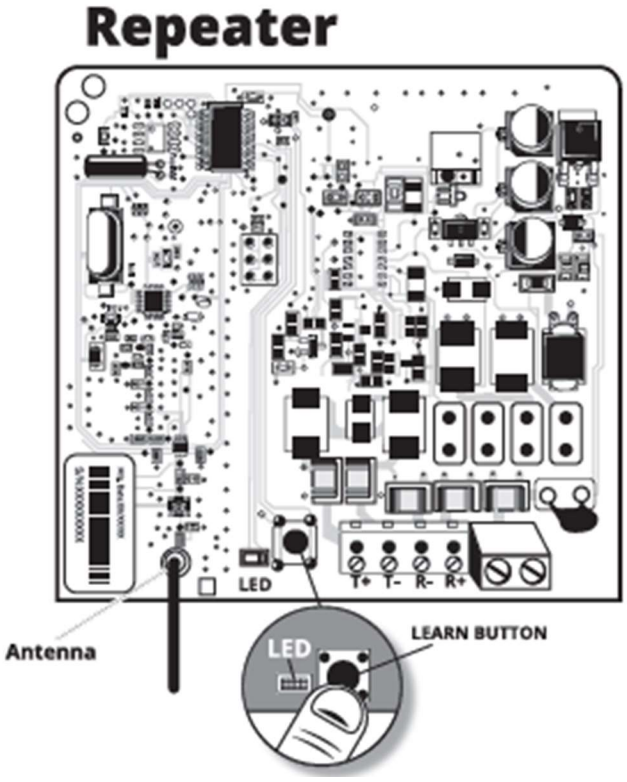
- LED
  - Used to determine if the repeater can connect to the transceiver.
- Antenna
  - Used to communicate with transceiver and DoorBosses.
- Power Supply
  - 16 VDC Wall Wort
- Backup Batteries
  - Used in case the power supply loses power.
- Program Button
  - Used to Learn into the transceiver.
- Serial Number Label
  - Each repeater is assigned a unique serial number, used to learn it into the transceiver.
- Weather-Proof Enclosure
  - Allows for the repeater to be mounted outside.

Installation

Every DoorBoss system installation needs at least one repeater. The repeater needs power. When you receive a repeater, it comes with a 16 VDC power supply; when installing it, the power supply up to 1000ft or 305m from the repeater. Four Lithium-Ion AA batteries come with the repeater and which act as a backup power supply for the repeater. The batteries have a life of two years and are not the primary power source for the repeater.
The signal transmission range of the repeater is up to a 1500ft or 457m. Install the repeater within the range of the transceiver or another repeater. The LED on the repeater denotes if the device is picking up a signal from the Transceiver. The repeater receiving a signal from the transceiver is known as "On Beacon." When the repeater is "On Beacon," the LED blinks once every four seconds. If the LED gives one long blink, this means the repeater is "Off Beacon" or not receiving a signal from the Transceiver.

Mounting Transceivers and Repeaters

- Transceivers and repeaters should be installed vertically with the antenna pointing down.
- Do not mount inside of medal, enclosures, beams, or door headers.
- Place each transceiver and repeater close enough to overlap signals.



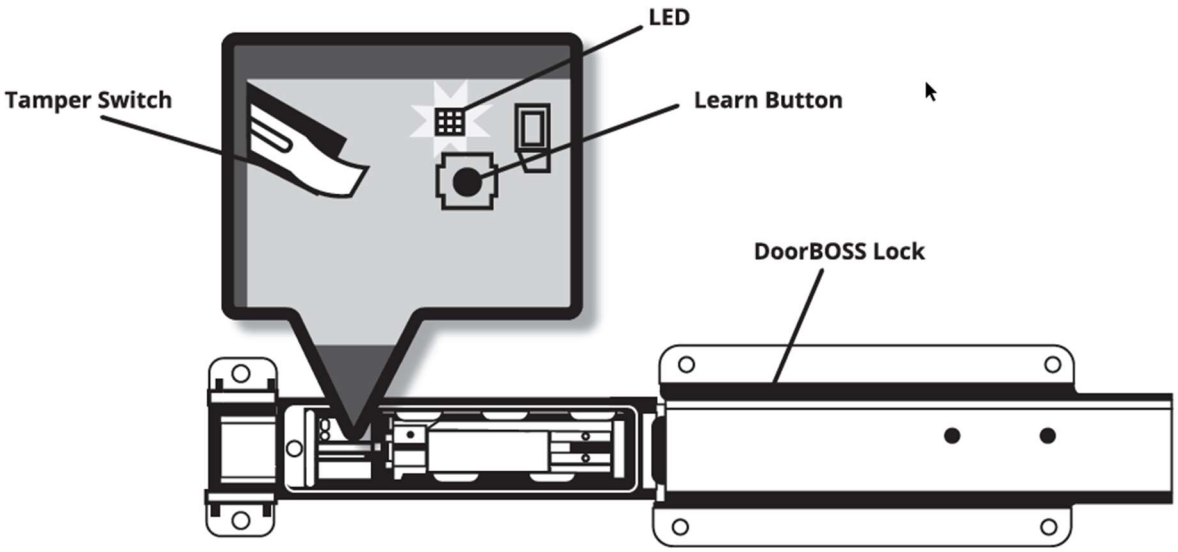
Drawing 27: DoorBoss Repeater

DoorBoss

The DoorBoss lock is a battery-powered, radio-actuated, locking device that controls access to the unit.

Components

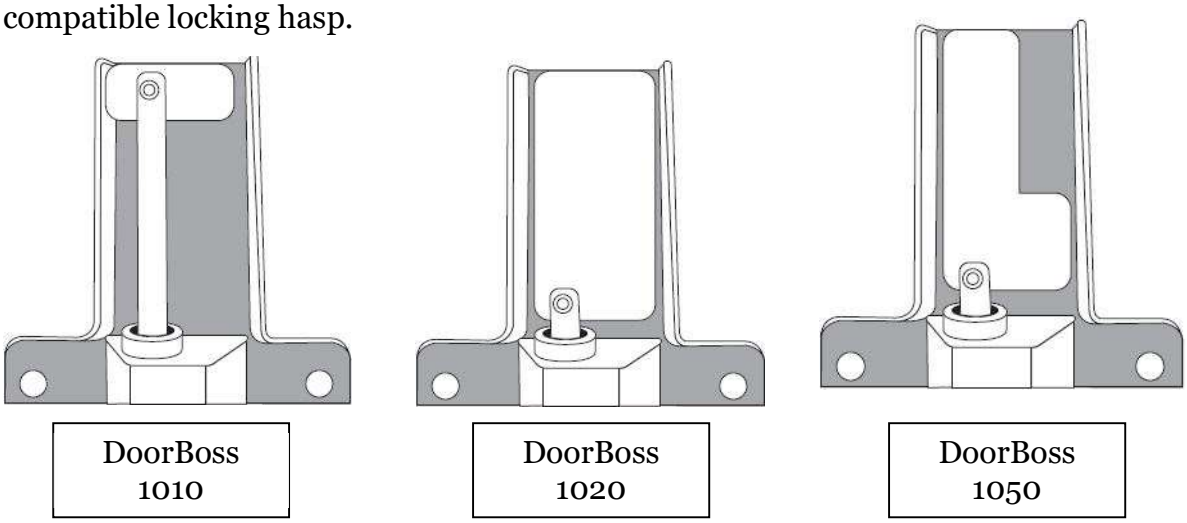
- Program Button
  - Used to learn the DoorBoss into the transceiver.
- Tamper Switch
  - Used to show when the battery door opening and testing of the device.
- Battery Assembly
  - Used to house the four Lithium-Ion AA batteries.
- LED
  - Used to determine if the DoorBoss can connect to the transceiver.
- Antenna
  - Used to communicate with the transceiver.



Drawing 28: DoorBoss Lock

Different Models

You can determine the model of the DoorBoss lock by the locking tab installed on the device. The hasp on the unit determines the locking tab for the DoorBoss. See Appendix A for a list of compatible locking hasp.



Drawing 29: DoorBoss Models

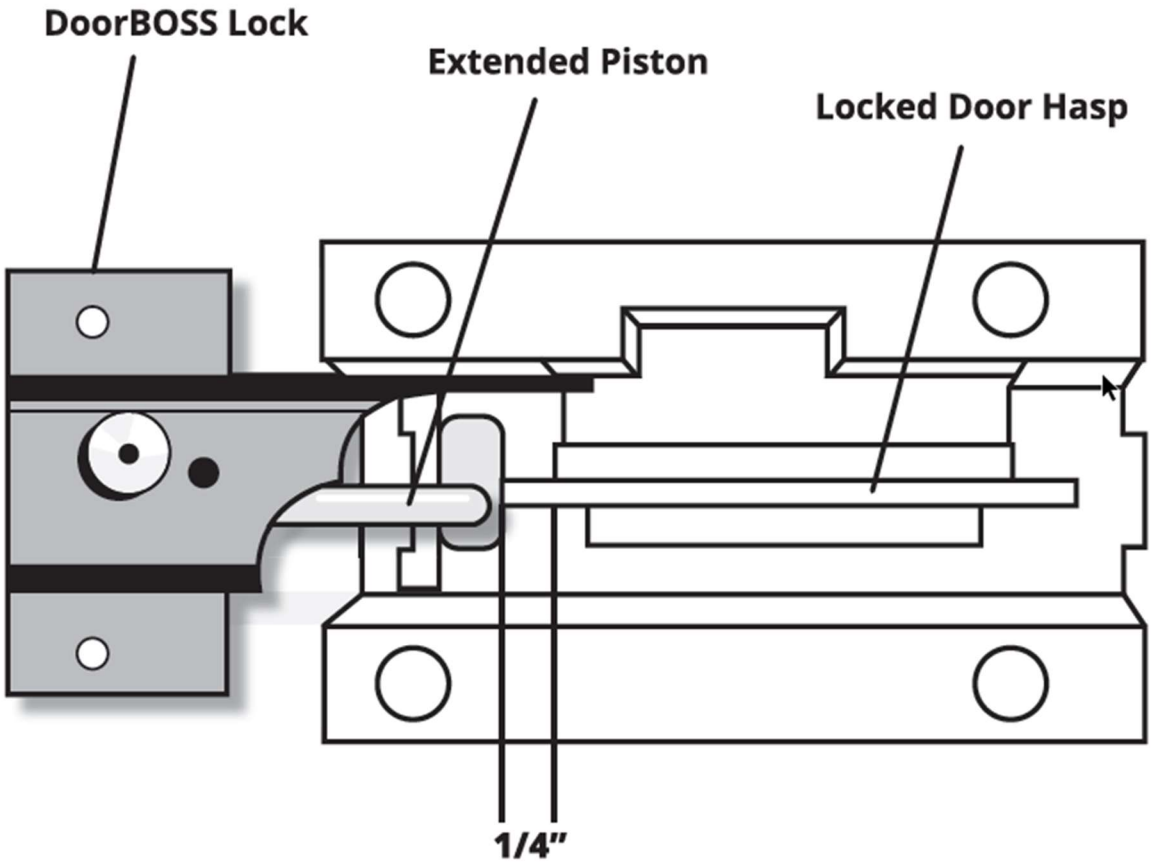
Mounting DoorBoss

To accurately mount DoorBoss, the following tools are required.

- Drill
- 3/16 Drill Bit
- #10 or #20 Security Torx
- Electric or Pneumatic Riveting Gun with a 3/16 riveting head

Mounting the DoorBoss

Any installation of the DoorBoss locks starts with closing the storage unit, then moving the locking hasp to the locked position. Once the storage unit is secure, remove the battery door from the DoorBoss lock, and install the batteries. Press and release the tamper switch on the DoorBoss extend the DoorBoss's piston. Slide the DoorBoss against the locked hasp, then move the DoorBoss lock 1/4 of an inch from the back of the hasp. At this point, mark and drill the mounting holes. Fasten the DoorBoss lock to the storage unit using the rivets. Once attached, retract the piston by pressing the tamper switch. Finally, unplug the battery assembly and reattach the DoorBoss battery door. Unplugging the battery assembly prevents the DoorBoss from going into a deep sleep and having to be re-learned into the system.



Drawing 30: DoorBoss/Hasp Spacing

Overlock Software

The Overlock software is one of four additional programs installed during the StorLogix installation. The Overlock software manages the DoorBoss hardware.

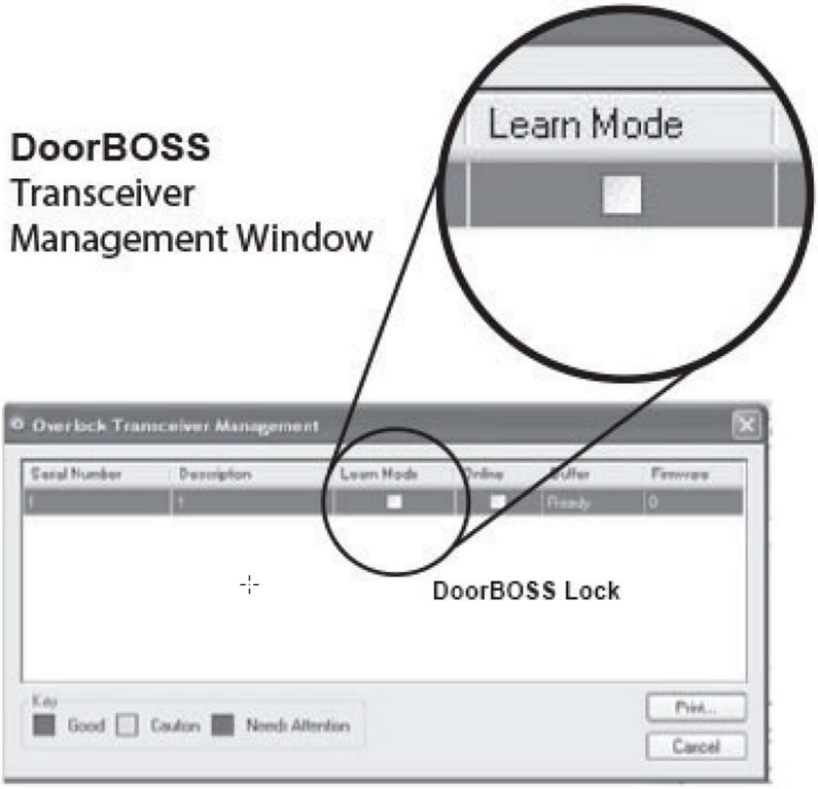
Adding A Transceiver

Every DoorBoss install starts with adding a transceiver to the Overlock software. To start, click "Setup" then "Manage Transceiver." In the window that appears, click the add button. The "Add Transceiver" dialog appears. In the "Add Transceiver" dialog box, type the Transceiver serial number in the "Serial Number" field. In the "Description" text box, the final mounting location of the device.

Learn Mode

Entering Learn Mode

To place the transceiver into Learn mode. Select "Tools," then "Manage Transceivers." Right-click on the transceiver, select extended commands, and select "Enable Learn Mode."



Picture 28: Learn Mode Check Box

Learning Repeaters

To learning a Repeater into the DoorBoss System, power up the Repeater and press the "program" button. The LED blinks while the device is learning and stops the blinking once the learning process is complete.
In the Overlock software, select "Setup" then "Repeaters." In the window that pops up, select the "Add" button. In the "Description" field, enter the final mounting location of the Repeater. In the serial number text box, enter the serial number of the repeater.
Complete this process before mounting the repeater.

Learning DoorBoss Locks

To learn the DoorBoss Lock into the DoorBoss System, power up the lock. When you see the DoorBoss lock's LED give four short blinks, press the "Program" button. Reattach the battery door.
In the Overlock software, the DoorBoss lock information appears. Right-click the DoorBoss entry and select "Edit Overlock." In the pop-up window, select the unit from the Unit drop-down list.
Mount the DoorBoss on the unit, before completing this step.

Picture 29: DoorBoss Details

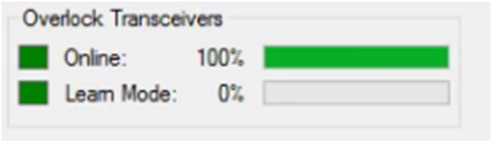
Exiting Learn Mode

The transceiver only stays idle in the "Learn" mode for 15-minutes before returning to normal mode. The 15-minute timer resets when a new repeater or DoorBoss lock learns into the system.
You can also manually exit the "Learn" mode. Select "Tools" and "Manage Transceivers." Right-click the transceiver, which is in "Learn" mode, and select "Extended Commands," and select "Disable Learn Mode."
When the DoorBoss transceiver's "Learn" mode is enabled, the status for the devices does not change. Nor are commands sent to the devices. The transceiver must be returned to regular operation either by time out or manual exit.

Software Layout

Percentage Bars

The Overlock software shows the overall health of your DoorBoss system using percentage bars.
Transceivers have a total of two percentage bars. The online bar shows the percentage of transceivers online. Since you can only have four transceivers attached to a DoorBoss system, this percent bar shows information in increments of 25%. The Learn bar shows the total number of transceivers in learn mode. Example: The site has four transceivers, and the "online" and "learn" percentage bars are showing 50% each. This means of two of the four transceivers are online, and in "learn" mode.

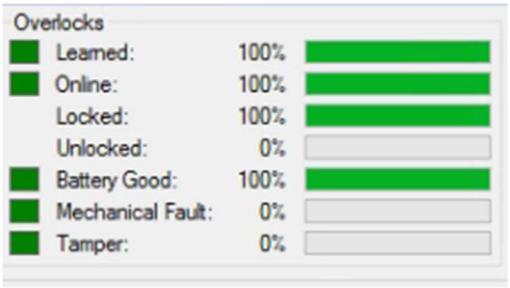


Picture 30: Online Percentage Bar

Repeaters have one percentage bar, showing the percentage of repeaters online at one time. The bar shows its information in increments of 6.25%. Example: A site with sixteen repeaters

and the repeater percentage bar is showing 25%. The 25% means only four of the sixteen repeaters are online.

The DoorBoss locks have a total of seven percentage bars showing a different health metric. The "Learned" percentage bar shows the total DoorBoss locks learned into the system.



Picture 31: DoorBoss Percentage Bars

- The "Online" percentage bar indicates the DoorBoss locks communicating with the transceivers.
- The Locked percentage bar shows the total DoorBoss locks in an engaged state.
- The Unlock percentage bar shows the total number of DoorBoss Locks in a disengaged state.
- The Battery Good percentage bar shows the total DoorBoss locks where the battery power is over 5 VDC.
- The Mechanical Fault percentage bar shows the total locks reporting a mechanical fault. When the lock reports a fault, this could be due to motor, piston, or door locking-hasp issues. The Tamper percentage bar shows the total DoorBoss locks with the battery cover removed.

DoorBoss Window

The main section of the Overlock software contains the list of all DoorBoss locks "Learned" into the DoorBoss system. The section shows the health of the individual DoorBoss locks and allows for control of each lock. The window displays different information for the DoorBoss locks using columns. By default, the user sees five columns.

1. "Unit" is the physical storage unit with the DoorBoss lock attached.
2. "User Status" displays if the site's customer is onsite or offsite.
3. "Serial Number" the individual serial number of the DoorBoss lock.
4. "Mode" the state of a single DoorBoss lock. This column displays serval different messages "Normal," "Locked by Software," "Unlocked by Software," and "Service Mode."
5. "Mechanical State" shows if the DoorBoss lock is physically engaged or disengaged.

Unit	User Status	Serial Number	Mode	Mechanical State
1	Offsite	25180087	Normal	Locked

Picture 32: DoorBoss Columns

The user can add or remove up to twenty-seven columns from the DoorBoss window. The twenty-seven columns cover a range of information. A few examples are "Battery Voltage," which is the voltage reading from the DoorBoss batteries, "Temperature," which displays the temperature at the DoorBoss lock, and "Suspend," which shows the status of the customer renting the storage unit in the StorLogix software.

Operating the DoorBoss Lock

Locking/Unlocking DoorBoss Lock

Picture 33: DoorBoss Command Buttons

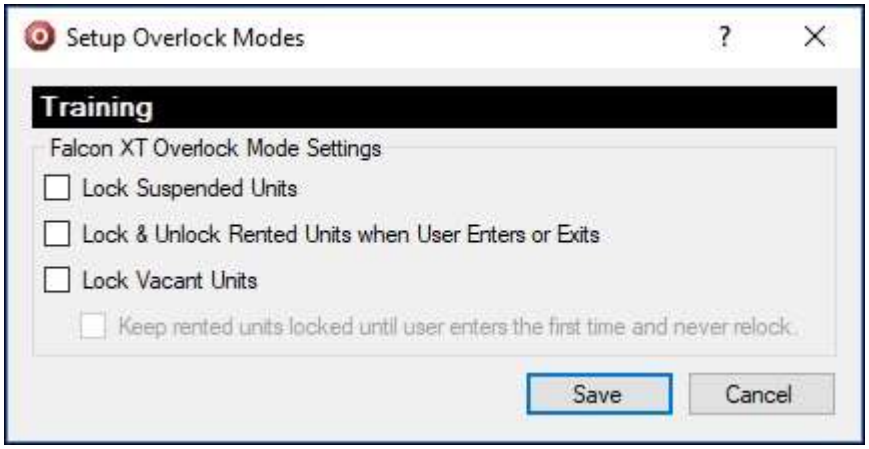
The Overlock software allows for manual operation of DoorBoss locks, a group of DoorBoss locks, or all the DoorBoss locks. To operate a single DoorBoss lock, right-click on the device. Click on "Lock" or "Unlock" to move the lock to the desired position. To operate a group of locks, select the first lock, and use CTRL-click to select the locks out of sequence. To operate a series of locks, select the first lock, hold down the shift key and select the last lock in the series. After selecting all the locks, right-click, and choose “Lock” or “Unlock.”

Operating all the DoorBoss locks uses much of the same process, instead of clicking lock or unlock, the user would click “Unlock All” or “Lock All” to move the locks to the desired position. Note: When manually operating locks, it is out of “Normal” mode and disregards all commands from the keypad. To put the lock back in “Normal” mode right-click one of the DoorBoss locks and select “Reset” or “Reset All.”

Another option the user has is the command box, on the right-hand side of the window. Operating the locks using this method starts with selecting the DoorBoss locks, then click the “Lock” or “Unlock” button to move the DoorBoss to the desired position. To place the DoorBoss lock back in “Normal,” click “Reset” or “Reset All.”

DoorBoss Mode

The DoorBoss locks have three distinct operational modes, which allow the DoorBoss lock to work in the situation desired by the site. To change the mode, click “Setup,” then “Overlock Modes.”



Picture 34: DoorBoss Modes Box

“Lock Suspended Units” only engages the DoorBoss lock if the unit is in suspension. “Lock & Unlock rented Units when User Enters or Exits” disengages the lock when StorLogix registers the customer enters the site and reengages it when the customer exits the site. “Lock Vacant Units” engages when it is attached to a vacate storage unit.

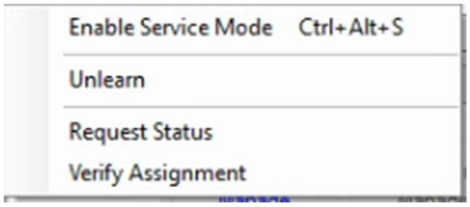
Troubleshooting

Service Mode

Service mode allows for changing the DoorBoss lock Batteries by turning off the tamper alarm and testing the piston on the individual device. When a DoorBoss lock is in "Service Mode," removing the battery, the door retracts the piston, and reinstalling the battery door extends the piston. Unlike "Learn Mode," there is no time limit for the device to stay in this mode.

Entering/Exiting Service Mode

To enter "Service Mode" right-click on the individual DoorBoss lock, then select "Extended Commands, select "Selected Overlock," and click "Enable Service Mode." Exiting "Service Mode" is the same process, except the final step is clicking "Disable Service Mode."



Picture 35: Extended Command Box

DoorBoss, not Locking/Unlocking

If you have a non-operational DoorBoss Lock, follow these following Troubleshooting steps.

1. Check if the customer's entry/exit registered in the software.
    a. If StorLogix does not see the customer enter/exit the site. The DoorBoss not engaging/disengaging.
        i. Have customers re-enter the code at the keypad.
2. Check to see if the Transceiver/Repeater is online.
    a. If the DoorBoss lock is unable to communicate with the Falcon XT, the lock is not engaging/disengaging.
        i. Check the wiring to the Transceiver or power supply for the Repeater.
3. Check to see if the DoorBoss lock is online.
    a. If there is an issue with the DoorBoss lock, it moves to fail open position.
        i. Check the signal, using the number of blinks of the DoorBoss LED, and check the batteries of the DoorBoss lock.
4. Check the DoorBoss Mode.
    a. If the DoorBoss mode is incorrect, the DoorBoss is not operating as expected.

Unlearning/Relearning a DoorBoss Lock

At some point, a DoorBoss lock might need to be removed and reinstalled into the software. Most of the time, this is to troubleshoot the device. Here are the steps for "Unlearning" a DoorBoss lock.

1. Hard Reset the DoorBoss Lock
    a. Press and hold the "Learn" button in the DoorBoss lock. While pressing the "Learn" button, remove power from the DoorBoss lock. Reapply power to the DoorBoss lock and release the "Learn" button.
2. Unlearning the DoorBoss lock from the Transceiver
    a. Right-click on the DoorBoss lock, in the software, and select "Extended Commands," "Selected DoorBoss," and "Unlearn."
3. Removing/Adding DoorBoss to the Software
    a. Click "Setup" then "Overlocks" and find the DoorBoss lock on the list that appears. Select the DoorBoss lock from the list and click the "Remove" button.
    b. Proceed to "Learn" the DoorBoss into the system as if it was a new DoorBoss lock.

Review

1. What is the maximum number of DoorBosses one system can have installed?
2. What is the maximum number of Transceivers connected to a Falcon XT?
3. Are the DoorBoss repeaters physically connected to Falcon XT?
4. Can you check the battery voltage, for each DoorBoss, in the Overlock software?

StorLogix Basic Setup

The basic setups are the minimum settings for getting most new sites up and running. The basic setups include the setup of the keypads, the access control (except for elevators, see page 76), and the setup of the door alarms.

How StorLogix Access Control Works

The system uses **Time Schedule** to define time slots for the different days of the week and holidays. Each unit has a unique name/number that identifies it in the system. The unit name can be any combination of letters and numbers up to 6 characters. The user assigns to an **Access Area**. The **Access Level** brings the **Time Schedule** and the **Access Areas** together to define how and when a customer can access the site. The **Access Levels** give you the ability to require tenants to have a unit in the area they are trying to access. We recommend adding keypads for entry to wine storage, climate-controlled areas, elevators, employee-only areas, and vault storage. In most **Access Levels**, you have a **Time Schedule**/**Access Area** combination for each **Access Area** defined in the system.

Access Setup Components

- **Enroll AI Devices** defines the basic definitions of the devices in the system.
- **Time Schedule** defines the time slots used by the system.
- **Access Areas** defines the units associated with the area and the devices used to access the area.
- **Access Levels** defines the access control given to users.
- **AI Device Properties** defines the behavior of the access devices.

Enroll AI Devices

Enroll AI Devices takes care of the initial settings for each of the devices, focusing on the device name and the device type. It is a companion to **AI Device Properties**.

With the hardware connected and correctly addressed, each device auto-enrolls and show as a device in the **Enroll AI Devices**. The list shows the address number, device description, and device type auto-enrolled.

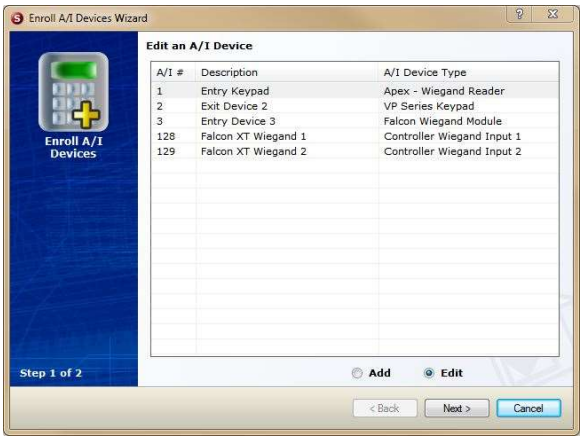
Some devices may show in red, indicating their types are undetermined and need changing.

Select a device from the list, click **Edit**, then click the **Next** button.

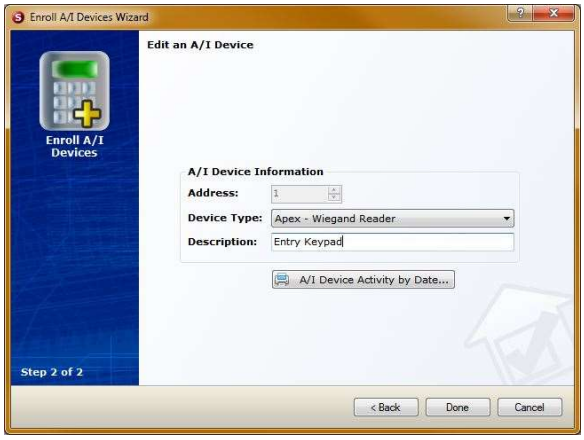
The **Address** reads from the device during autoenrollment. You cannot change the address in the software only through the device settings.

Device Type is the definition of the type of hardware the address represents. For the Wired Door Alarms, select the correct number of channels to match your device.

Give the device a good **Description** that describes how the device functions in the system.



Picture 36: Box 1 Enroll A/I Devices



Picture 37: Box 2 Enroll A/I Devices

Click the **A/I Device Activity by Date** button to generate a report of activity for this device.

Click the **Back** button to return to the device list, click the **Done** button to save the settings, and click the **Cancel** button to close the wizard without making any changes.

Time Schedules

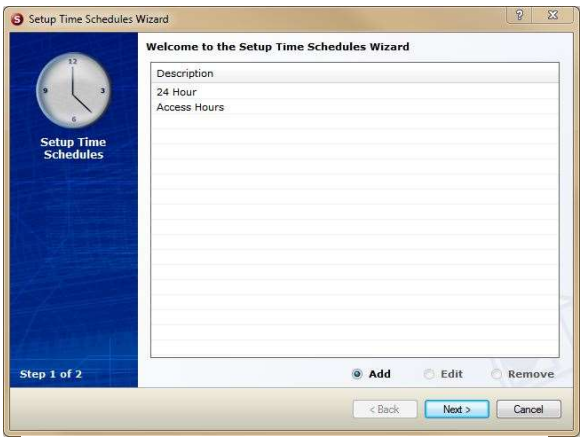
Time Schedules are time slots or time tables used for access permission or scheduled functions. The software creates two schedules by default.

- **24 Hours** – this default is for access all the time.
- **Access Hours** – this is the access hours you assigned in the StorLogix Configuration Wizard.

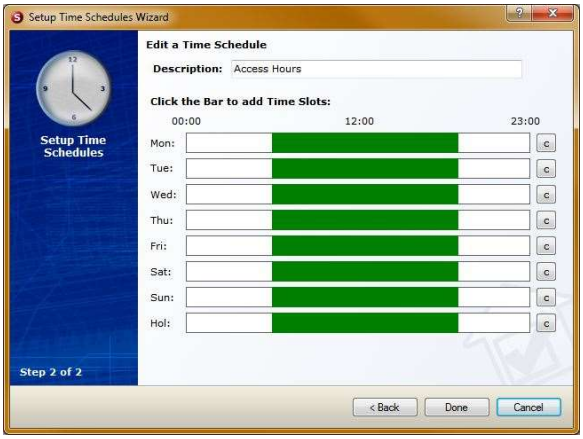
To close a site on a specific day, set the time slot to 12 AM to 12 AM. Select **Add** to add a new schedule, **Edit** to edit an existing schedule, and **Remove** to delete a schedule. You cannot delete a schedule that is assigned somewhere else in the setups.

The window shows the time slot for each day of the week. **Hol,** for a holiday, is a slot defining access hours on holidays defined in StorLogix. To edit one of the time slots, click on the day you want to edit.

To edit a **Time Span** select it and adjust the sliders for **Start Time** and **End Time** or edit the text boxes directly. Once you have the times set the way you want, click the **Edit** button to change the selected **Time Span**.

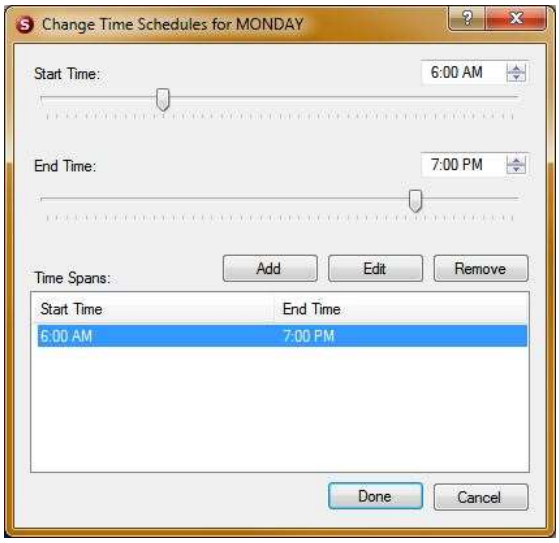


Picture 38: Box 1 Time Schedule



Picture 39: Box 2 Time Schedule

To add a new **Tim Span**, adjust the sliders or edit the text boxes directly. Click the **Add** button to add the **TimeSpan**. *The system does not allow* **Time Spans** *to cross over each other, but different* **Time Spans** *for one day.*



Picture 40: Time Span Box

To delete a **Time Span,** select it and click the **Remove** button.

Leaving the **Time Spans** empty is the same as 24-hour access and is not recommended.

Click the **Done** button to save and the **Cancel** button to exit without saving.

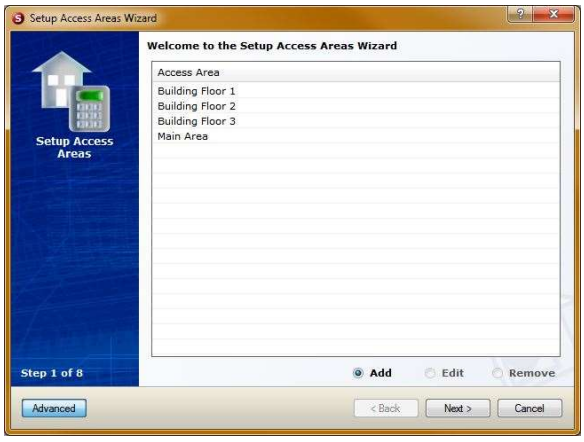
Use the **C** button to copy the time slots from one day to another. Check the days that you want to copy. Click the **Done** button to perform the copy. Click the **Cancel** button to cancel the copy.

Picture 41: Time Schedule Copy Box

Once you have all the time slots defined the way you want them, the **Done** button in the wizard saves the settings. The **Back** button returns you to the **Time Schedule** list. The **Cancel** button closes the wizard without making any changes.

Access Areas

Access Areas control a section of units and the devices that allow access to those units. You can have several reasons for creating more than one area, including climate-controlled buildings, multiple floors in a building controlled by an elevator, or separate gated areas. This section explains how to set up areas. This book covers elevator controls on page 76.

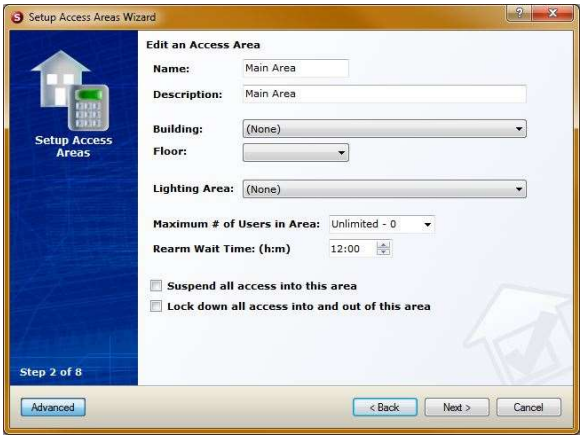


Picture 42: Box 1 Access Area

On step 1, select **Add** and click the **Next** button to add a new area. Select an area, select **Edit**, and click the **Next** button to edit an area. Select an area, select **Remove**, and click the **Done** button to delete an area. You cannot delete an area if other settings are using it. The **Advanced** button activates the advanced settings for the wizard. The **Cancel** button closes the wizard.

In Step 2, the **Name,** you are limited to 10 characters, but for the **Description**, you can use a name that more fully describes the area. The **Name** is an abbreviated version of the **Description** used in the logs and other places.

For the **Building**, **Floor**, and **Lighting Area** settings refer to How Lighting Areas Work (page 80).

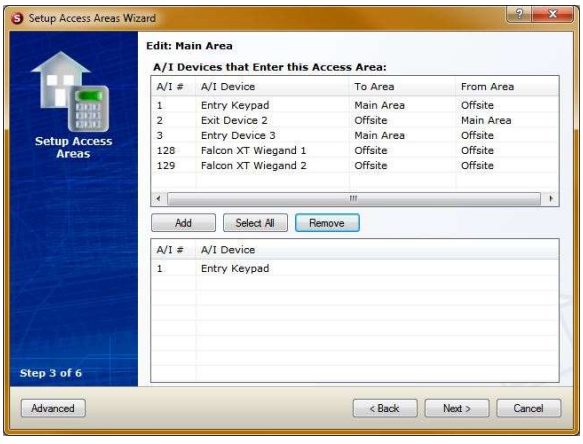


Picture 43: Box 2 Access Area

Maximum # of User in Area allows you to control how many people can access the area. The default is unlimited and should not change unless there is a local occupancy code that requires you to change it.

Rearm Wait Time is the amount of time before an area alarm rearms after being disarmed by access.

The two check-boxes allow you to control access to the area regardless of the tenant's status. **Suspend all access to this area** locks the area down so no one can enter the area, but they can exit. **Lockdown all access into and out of this area** prevents access into and out of the area. These two settings are for emergencies where you need to lock down an area.



Picture 44: Box 3 Access Area

Click the **Next** button to advance to step 3.

The top list is a list of all devices in the system, and the bottom list is a list of all the devices used to enter the area.

Select a device from the top list and click the **Add** button to add it to the bottom list.

Select a device in the bottom list and click the **Remove** button to dissociate it from the area.

Click the **Back** button to return to the previous step and click the **Next** button to move to step 4.

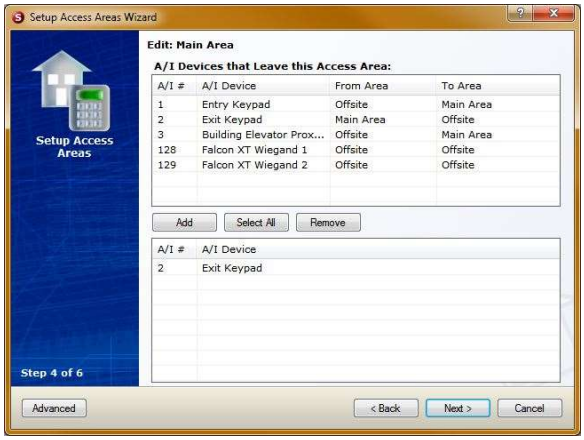
Step 4 is much the same as step 3, except it is for devices exiting the area. The top list is a list of all devices in the system, and the bottom list is a list of all the devices used to exit the area.

Select a device from the top list and click the **Add** button to add it to the bottom list.

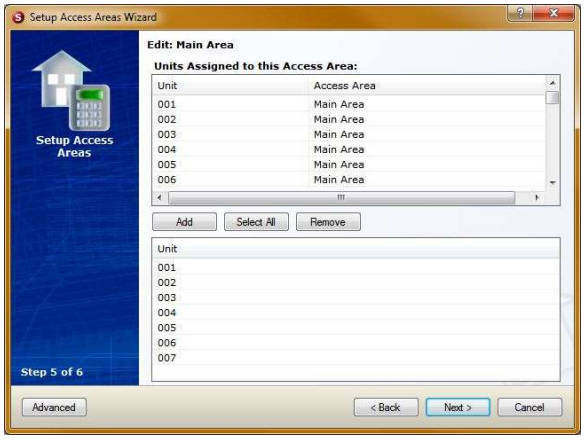
Select a device in the bottom list and click the **Remove** button to dissociate it from the area.

Click the **Back** button to return to the previous step and click the **Next** button to move to step 5.

For both steps 3 and 4, you can assign a device to only one area.



Picture 45: Box 4 Access Area



Picture 46: Box 5 Access Area

Step 5 is the assignment of the units inside the area you are defining. The top list is all the units in the system, and the bottom list is the units assigned to this area.

When selecting unit names from the top list, you can Shift-click or Ctrl-click to select multiple units at one time.

Select units from the top list and click on the **Add** button to assign them to the area.

Select units from the bottom list and click the **Remove** button to dissociate the units from the area and assign them back to the default area.

Click the **Back** button to return to the previous step and click the **Next** button to move to step 6.

Step 6 is just a review of the settings for the area. Click the **Done** button to save the settings.

Access Levels

Access Levels combine the **Time Schedules** and the **Access Areas** to control access to different areas. Under normal conditions, you only need an **Access Level** for each of the **Time Schedules** used for access. Sometimes, it is necessary to create a unique **Access Level** to give managers access to all areas.

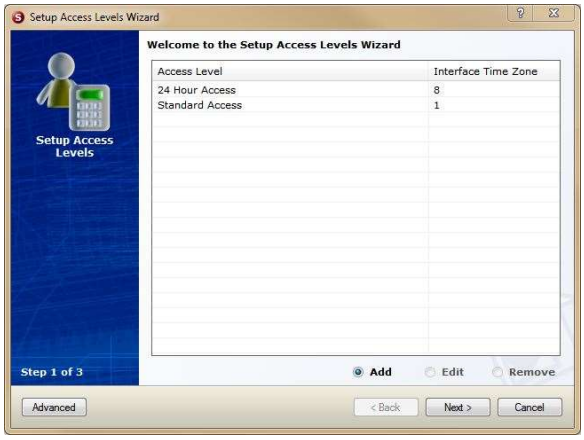
Each **Access Level** is assigned a number used by the account management program to assign users to the **Access Level**. Most account management programs reference the number through the **Time Zone** field. The assignment of the **Access Level** controls what access the user has, depending on the **Access Level** and unit assignment of the user.

Step 1 shows a list of all the currently defined **Access Levels**.

The system defines two **Access Levels** by default:

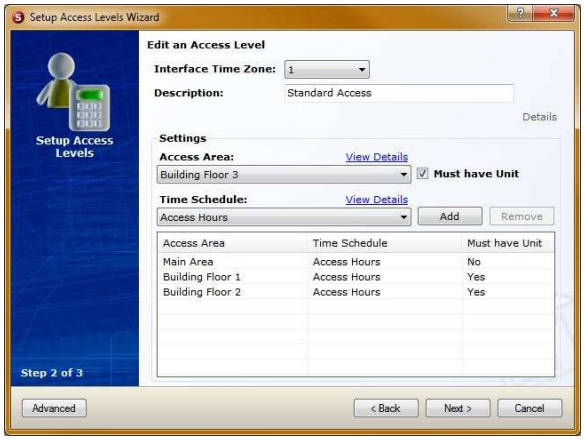
- **Standard Access** (1) defines access using the **Time Schedule** defined during the (page 39).
- **24 Hour Access** (8) defines access using the default 24 hours' **Time Schedule**.

The **Interface Time Zone** is the number used by the account management software to assign the **Access Level** to a tenant.



Picture 47: Box 1 Access Level

To create a new **Access Level**, select **Add** and click the **Next** button. Change an **Access Level** by selecting it from the list, clicking on **Edit**, and clicking the **Next** button. Click the **Cancel** button to close the Access Levels Wizard without making any changes.



Picture 48: Box 2 Access Level

On step 2, the **Interface Time Zone** is the number used by the account management program to assign this **Access Level** to a user.

As with any setting, create a good **Description** that defines the **Access Levels** function in the system.

When creating the access, select the **Access Area** and **Time Schedule** from the dropdown lists. Check **Must-Have Unit** to restrict access to only those who have units in the area. For areas where everyone needs access, **do not** use this setting. Click the **Add** button to apply the settings to the **Access Level**.

Select a setting from the list and click on the **Remove** button to dissociate the setting.

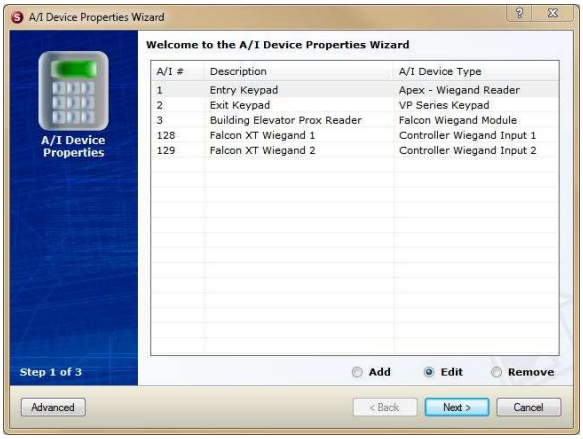
Click the **Back** button to return to the **Access Levels** list. Click the **Next** button to advance to Step 3.

Step 3 is just a preview of the settings. Click the **Done** button to save the settings.

A/I Device Properties

You use **A/I Device Properties** to program the functionality of keypads and other access devices by defining the role the access device plays in the user entering and leaving the different areas of the facility. The **A/I Device Properties** also defines the relays used to trigger external hardware such as gate operators, door strikes, magnetic locks, and sliding doors.

The list in the **A/I Device Properties** is the same as the list in (page 63). Devices 128 and 129 are the two Wiegand inputs on the Falcon XT.



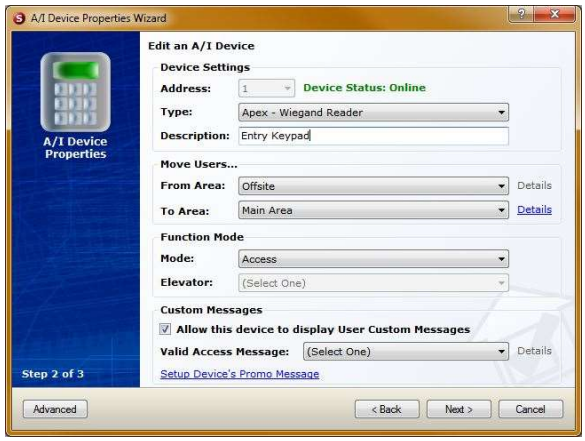
Picture 49: Box 1 A/I Device Properties

Select the **Add** button and click the **Next** button to create a new device. Since the device's auto-enroll, this is rarely necessary.

To change a device's settings, select the device in the list, select **Edit**, and click the **Next** button.

To eliminate a device, select the device from the list, select **Remove**, and click the **Done** button. *You cannot remove a device referenced in other settings.*

Click the **Cancel** button to close the A/I Device Properties Wizard.



Picture 50: Box 2 A/I Device Properties

The **Address** is programmed into the device and cannot be changed.

Select the correct "**Type**" for the device. Failing to select the correct device type can result in issues with the device.

The **Description** can describe the role or location of the device in the system (example: main gate entry keypad).

Move User controls how the device affects the user's on-site status. "**From Area**" is where the

user is exiting. **To Area** is where the users are going. For either, the choices are any areas defined in the software or offsite. In most cases, these settings default to the correct settings when the user assigns the device as an entry or exit device in the setup (page 67).

The **Function Mode** controls the default behavior for keypads and access devices like the Wiegand inputs and the PWIE.

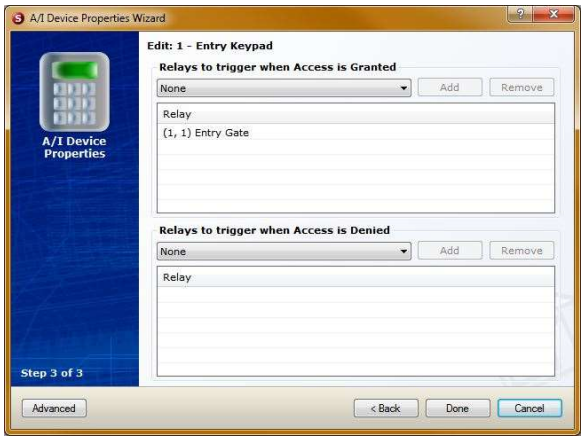
- is the default mode and, in most cases, the mode you want to use? All the other modes are individual cases designed for specific purposes.
- **Entry / Exit** rotates between entry and exit depending on the number of times the user has used the keypad. The first time the user enters their code in the keypad, the system recognizes it as an entry; the second time the user enters their code, the system sees it as an exit.
- **"Elevator"** sets the access device for use with elevator control settings.
- **Check-In / Out** works like the Entry / Exit but works on the concept of check-in and check-out. You can set other access devices not to work unless the user checks-in. For example, the management wants all tenants to check in at a Kiosk where the site displays the rules before proceeding to their units.
- **PayXpress Only** allows a keypad to take payments, but not to be used for any other purposes (like entry or exit). This only works for an Apex keypad with a mag-stripe reader.

By checking **Custom Messages**, you set the keypad to show custom messages. These custom messages can include tenant balances and sales promotions. Use the dropdown list to select the message to display on this keypad. The custom message shows after the customer enters a valid code.

Setup Device's Promo Message (Apex keypads only) allows you to set up a promo message for the keypad. In the dialog, check **Use Custom Promo Message** to activate it. Enter your custom message in the four text boxes provided. Use the alignment buttons to adjust the spacing of lines as needed. Click the **Apply to All** button to set this message for all the Apex keypads in the system. Click the **Done** button to save the settings. Click the **Cancel** button to exit the dialog without saving the promo message.

Picture 51: Custom Message Box

On the main wizard screen, click the **Back** button to return to the previous step. Click the **Next** button to advance to Step 3. Click the **Close** button to exit the wizard without saving any changes.



Picture 52: Box 3 A/I Device Properties

The top list is for relays to trigger when the system grants access; the bottom list is for relays to trigger when the system denies access.

Use the dropdown list to select the relay to trigger and click the **Add** button to add it to the list. To take items off the list, select the relay in the list and click the **Remove** button.

The top list is for relays to trigger when the system grants access; the bottom list is for relays to trigger when the system denies access.

Click the **Back** button to return to the previous screen. The **Done** button saves the settings. The **Cancel** button closes the wizard without saving the changes.

How Basic Unit Door Alarms Work

The unit with a switch gets to an access area. Each wired door alarm multiplexer has a certain number of positions called channels. In the software, you assign the multiplexer channel to the unit. You create alarm zones that have relays assigned to it. The alarm zone is associated with the access area. You can also associate an alarm zone with the auxiliary zone responsible for triggering all the relays on the wired door alarm multiplexers.

Door Alarm Setup Components

- **Alarm Zones** – used to control the triggering of alarms in a particular area
- **Access Areas (advanced settings)** – assigns an alarm zone to an area
- **Mux and Channel Assignments** – assigns installed switches to the unit
- **Falcon XT** – sets the alarm zone that triggers the auxiliary zone relays

Alarm Zones

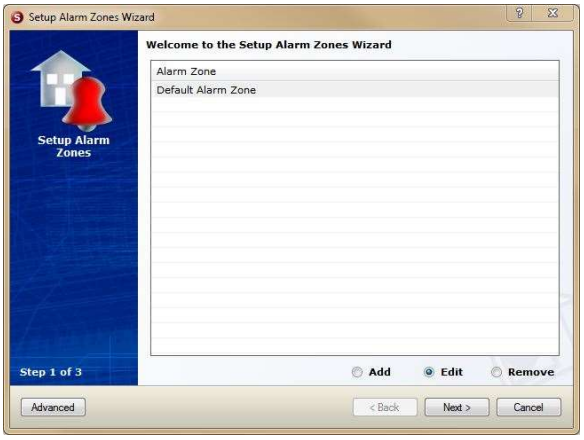
The software uses **Alarm Zones** to trigger relays for the sounding of sirens, triggering burglar panels, and other alarm related devices. In the alarm zone, you set how long the relays latch when the zone goes into an alarm condition. The alarm zone also defines the relays to trigger.

Step 1 shows the currently defined alarm zones in the system. One alarm zone, **Default Alarm Zone**, is created for you during software installation. In many cases, this is the only zone you need.

To create a new zone, select **Add** and click the **Next** button.

Select an existing zone, select **Edit**, and click the **Next** button to make changes to a zone.

To eliminate a zone, select the zone, and select **Remove**. Click the **Done** button to remove the zone. *If a zone is used elsewhere in the settings, you cannot remove it.*



Picture 53: Box 1 Alarm Zones

Click the **Cancel** button to close the wizard without making any changes.

Picture 54: Box 2 Alarm Zones

In Step 2, the **Description** should explain how the system uses the zone.

The **Sound Alarm Until Silenced or Cleared** causes the relays to latch until someone silences the alarm or clears it. Only use this setting when the customer insists, they want it.

Alarm Day Mode and **Alarm Night Mode** control the time and how long the relays latch. The **Start Time** is when the mode begins. The **Sound Time** is how long the relays latch in *hours:minutes: seconds* format.

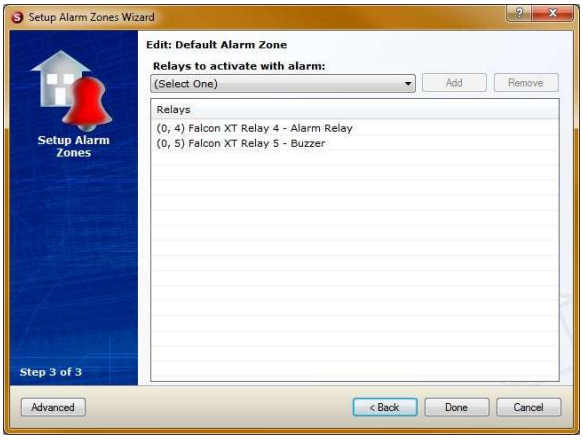
Click the **Back** button to return to the list of zones. Click the **Next** button to advance to step 3. Clicking **Cancel** closes the wizard without making any changes.

The list contains the relays that fire when this alarm zone is activated.

To assign a relay to the zone, select the relay from the dropdown list, and click the **Add** button.

Select a relay in the list and click the **Remove** button to eliminate it from the list.

The **Back** button takes you back to the previous screen. Click the **Done** button to save the settings. The **Cancel** button closes the wizard without saving any changes.



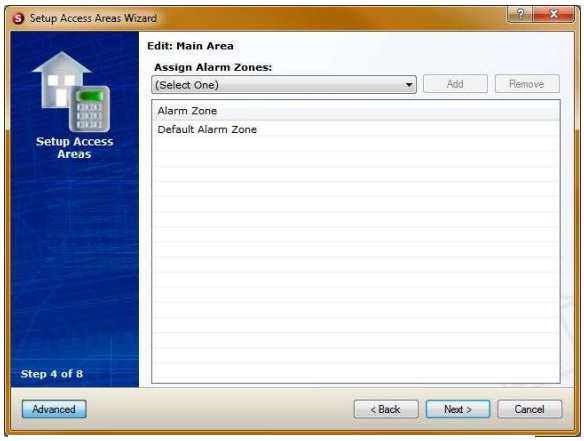
Picture 55: Box 3 Alarm Zones

Access Areas (Advanced Settings)

To activate the advanced settings, click the **Advanced** button in the lower-left corner of the wizard.

On step 4 of the advanced settings, select the alarm zone from the dropdown list, and click the **Add** button to add a defined zone to the list.

Select a zone in the list and click the **Remove** button to eliminate it from the list.



Picture 56: Box 3 Alarm Zones

Mux and Channels

Mux and Channel Assignment wizard assigns door alarm switches to units. The list includes every unit assigned in the software. If a unit is missing, it is not in the StorLogix Database.

The **Mux** column is the address number of the wired or wireless door alarm multiplexer. The **Channel** column is the position on the multiplexer; the unit's switch connects, or the wireless transmitter assignment. Checking **Alarmed** makes the unit armed.

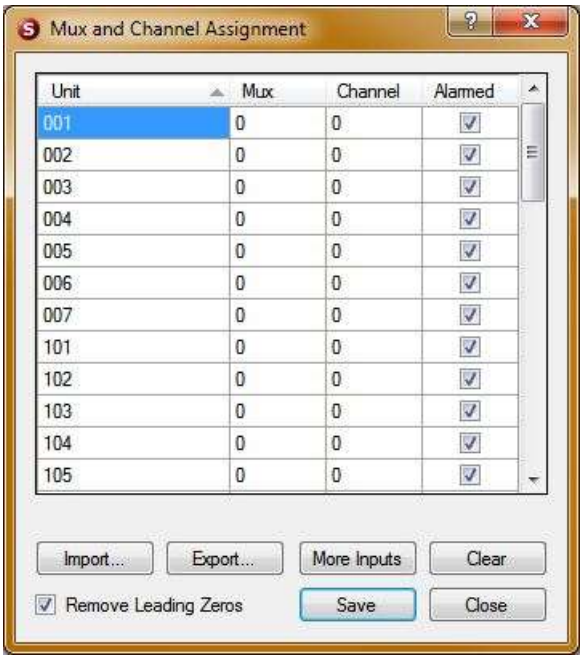
The **Import** button reads mux and channel assignments from an alarm.alm file from legacy Falcon 2000 software or generated by the **Export** button in StorLogix. Checking the **Remove Leading Zeros** before importing the file eliminates any padding zeros at the start of the unit number. The **Export** button saves the mux and channel assignments to an "alarm.alm" file. The file is a comma-delimited text file.

Use **More Inputs** to add more than one switch to a single unit. Select the unit that has multiple switches and click the **More Inputs** button. The software creates a new blank record for the unit where you can add another mux and channel assignment.

The **Clear** button sets all selected assignments to 0 (zero).

Use the **Save** button to save the assignments.

The **Close** button exits the dialog. Make sure to save settings before closing the window, or your changes are lost.



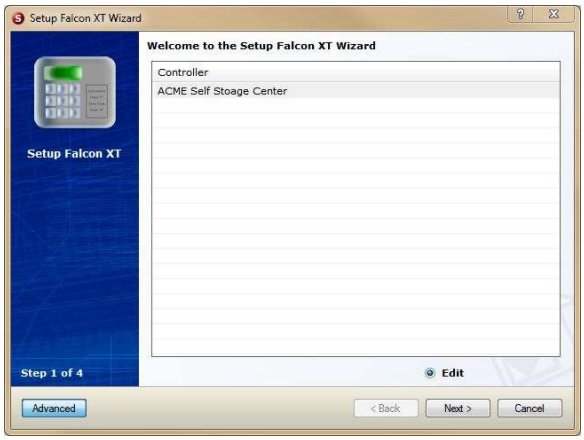
Picture 57: Mux & Channel Box

Falcon XT

The list shows the Falcon XT controller associated with the system. Here we only cover settings related to door alarms. Click the **Advanced** button for these settings.

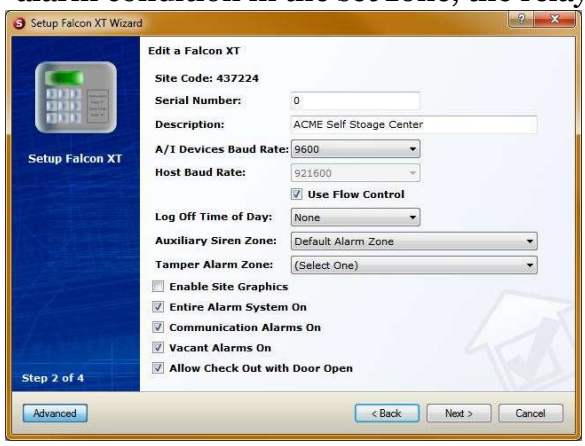
Select the Falcon XT listed and click the **Next** button to make changes to the settings.

Click the **Cancel** button to close the wizard without making any changes.



Picture 58: Box 1 Falcon XT

The **Auxiliary Siren Zone** allows you to set which alarm zone is responsible for triggering the relays on the wired door alarm multiplexers. When there is an alarm condition in the set zone, the relays on the wired door alarm multiplexers latch with the other relays assigned to the alarm zone.



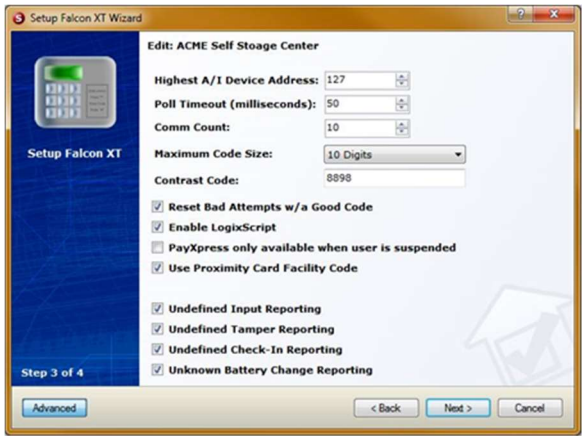
Picture 59: Box 2 Falcon XT

The **Tamper Alarm Zone** associates the selected zone with tamper alarm conditions.

Entire Alarm System On enables the alarm system when checked. Uncheck to disable the alarm system.

With the "**Communication Alarms On"** has a check, the software creates an alarm condition when devices lose communication with the Falcon XT.

To arm vacant units, check **Vacant Alarms On**.



In unusual cases, you may need to allow tenants to check out without closing their units. Check **Allow Check Out with Door Open**. The four undefined settings are related to the RX900 wireless door alarms. If you are not using wireless door alarms, these checkboxes do not affect your system.

The checkboxes report activity on transmitters that are not assigned to a unit in the system but are seen by the wireless multiplexer.

Picture 60: Box 3 Falcon XT

If you change any of the settings, make sure to click the **Next** button and click the **Done** button on the last screen of the wizard to save the changes.

Elevator and Lighting Control

How the Elevator Control Setup Works

When setting up elevator controls, you start by defining the building. The building definition states how many floors the building has. The number of floors should include the basement when necessary. The building and floor numbers are associated with an access area.

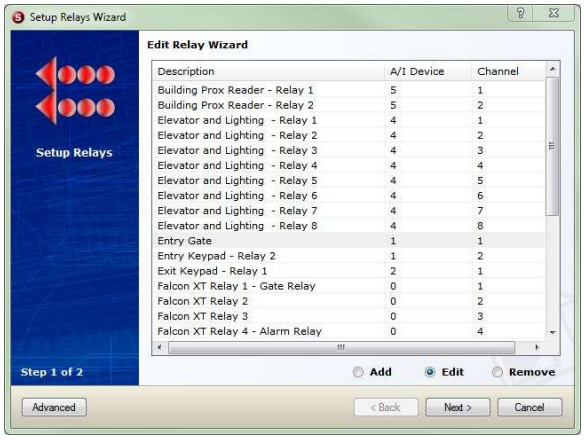
Along with the building, you define an elevator. In the elevator setup, you associate relays in the system to the different floors of the building. Finally, you associate the keypad or another access control device to the elevator setup.

Elevator Control Components

- **Relays** – used to trigger the elevator controls
- **Buildings** – defines the building and number of floors
- **Elevators** – defines the relays that control each floor of the building
- **Access Areas** – assign the building and floor to the areas
- **A/I Device Properties** – assign the device to the elevator control

Relays

The system uses relays to provide open and close triggers for devices in the system. The step 1 screen shows a list of all the relays defined in the system. This list generates when the device auto-enrolls in the system.



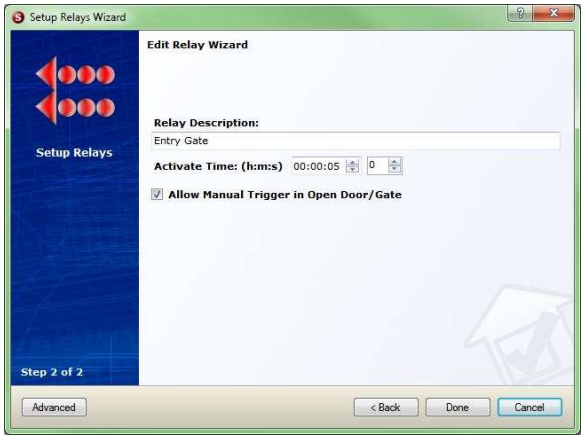
Picture 61: Box 1 Relay

Select **Add** and click the **Next** button to add a new relay. Rarely will you manually add relays, the exception is when making virtual relays.

To change the settings on a relay, select the relay, select **Edit**, and click the **Next** button.

Eliminate a relay from the system by selecting the relay, select **Remove**, and clicking the **Done** button. *If a relay is used elsewhere in the system, you cannot remove it. You first need to dissociate the relay from other settings in the system.*

Click the **Cancel** button to close the wizard without making any changes.



Picture 62: Box 2 Relay

In the "**Relay Description,"** give the relay a name that defines its function in the system.

Active Time is the length of time the relay latches when triggered. The time is defined as *hours:minutes: seconds* and tenths of a second.

Check **Allow Manual Trigger in Open Door/Gate** to have the relay shown in the **Open Door/Gate** option.

Click the **Back** button to return to the previous screen.

The **Done** button saves the relay settings.

To close the wizard without saving the settings, click the **Cancel** button.

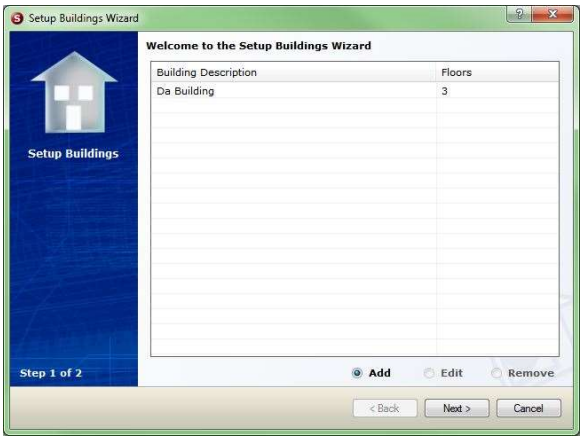
Building Setup

The Building Setup defines a building and the number of floors in the building. The number of floors should include the basement if the basement contains storage units.

The list is the currently defined buildings in the system. No buildings are defined by default.

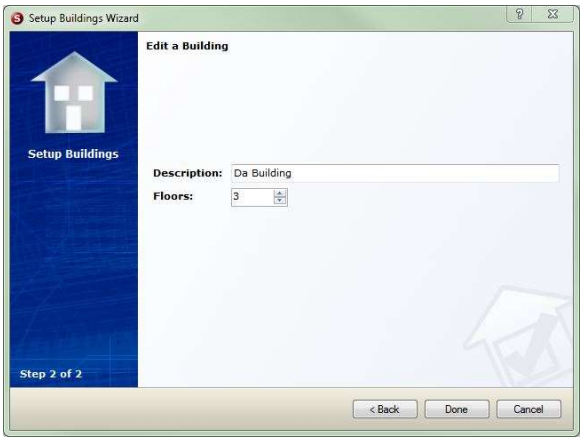
To define a new building, select **Add** and click the **Next** button.

Select a building from the list, select **Edit**, and click the **Next** button to make changes to the building.



Picture 63: Box 1 Building

The **Cancel** button closes the wizard without making any changes.



Picture 64: Box 2 Building

The **Description** should describe the building. Examples include Building A and Climate Control Building.

Enter the number of floors in the **Floors** text box, remembering to account for the basement if necessary.

Click the **Back** button to return to the previous screen.

To save the settings, click the **Done** button.

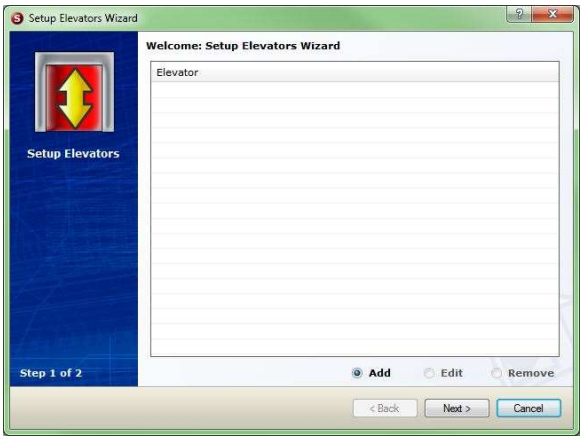
The **Cancel** button closes the wizard without saving any changes.

Elevators

The screen shows a list of currently defined elevators. The software does not create elevators by default.

To define a new elevator, select **Add** and click the **Next** button.

Select an existing elevator, select **Edit**, and click the **Next** button to change settings of an existing elevator setup.



Picture 65: Box 1 Elevator

Delete an elevator set up from the system by selecting the elevator from the list, selecting **Remove**, and click the **Done** button.

Picture 66: Box 2 Elevator

The **Description** is a unique name for this elevator. Make sure the name avoids confusion with other devices and elevators. The description is especially important when more than one elevator exists.

Select the building with the elevator from the **Building Elevator is in** the dropdown list. The **Add Building** button starts the **Buildings** wizard.

Lowest Floor and **Highest Floor** defines the lowest and highest floor this elevator accesses. Depending on the needs of the site and the actual travel of the elevator, you could have a lower floor other than 1 or the highest floor other than the top floor.

Defining the Floors

In the **Floors** section of the wizard, select the floor to define from the **Floor** dropdown list. Give the relay a unique **Description** which defines its purpose like the elevator, building, and floor. Select the relay for the activation of the floor from the **Relay** dropdown list. Click the **Add** button to move the definition into the list. Repeat this action for each floor related to the elevator. You can only add one relay for each floor.

Click the **Done** button when finished to save the elevator settings. The **Back** button returns you to the previous screen. Click the **Cancel** button to close the wizard without saving any changes.

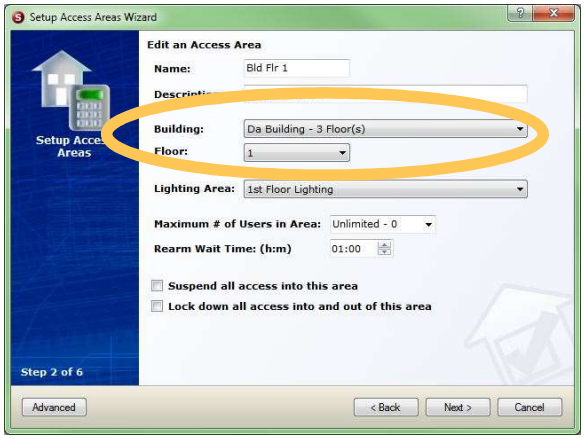
Access Areas (Step 2)

In the Access Areas wizard, you set the building and floor for the area, which means you want to create an area for each floor of the building.

From the **Building,** dropdown list, select the building for this area.

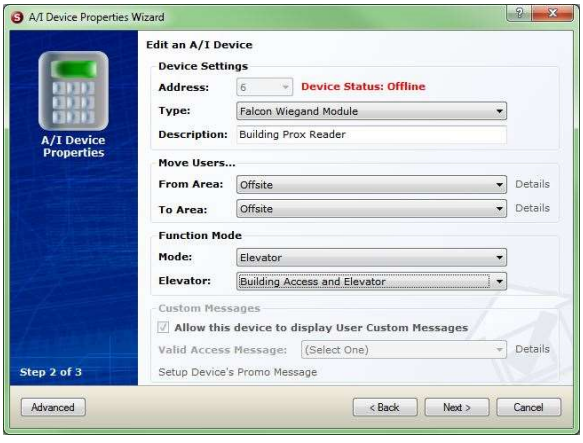
Use the **Floor** dropdown list to select the floor.

Click the Next button until you get to the last screen of the wizard. Click the **Done** button to save the settings.



Picture 67: Box 1 Access Area Advanced

A/I Device Properties (Step 2)



Picture 68: Box 1 A/I Device Properties Advanced

In the A/I Device Properties, you assign the elevator control to the access device on step 2.

Use the **Mode** dropdown list to select the Elevator mode.

In the **Elevator** dropdown list, you select the elevator setup for this device.

In most cases, you need to remove any relays from step 3 as the relays for the elevator are defined in the elevator setup. After removing the relays, click the **Done** button to save the settings.

How Lighting Areas Work

Lighting Areas are more than just lighting. With lighting areas, you can use relays to control devices such as lights that should remain active if tenants are in an area. You can assign lighting areas to areas or units depending on the needs and setup of the site.

You assign relays to a lighting area and assign the lighting area to an access area. In some cases, you want to assign the lighting area to the units rather than the access area, such as when using elevator controls. Because a tenant can have multiple units on different floors, the elevator control does not know what floor the tenant is going to; therefore, the elevator control leaves them in their current area. However, when the software assigns the lighting area to the unit, the system activates the lighting area if the tenant is on site.

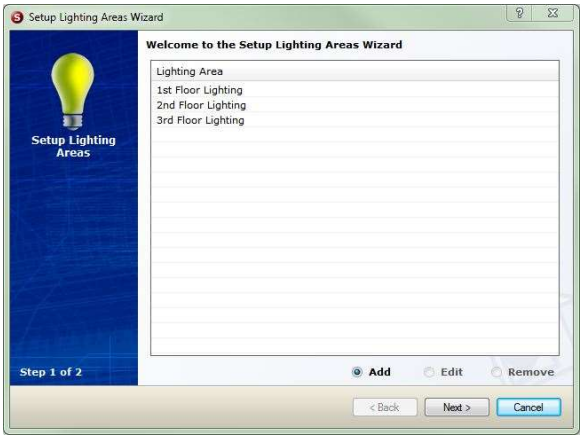
Lighting Areas

The first step of the lighting areas wizard shows a list of lighting areas already defined. By default, the software creates no light areas.

To create a new lighting area, select **Add** and click on the **Next** button.

Make changes to an existing lighting area by selecting the area, selecting **Edit**, and clicking the **Next** button.

If a lighting area is no longer needed, you can select the area, select **Remove**, and click the **Done** button. *You cannot remove a lighting area that is assigned elsewhere.*



Picture 69: Box 1 Lighting Area

Clicking on the **Cancel** button exits the wizard without making any changes.

Picture 70: Box 2 Lighting Area

The **Description** should explain the purpose of the lighting area.

Select the relays activated by this lighting area from the **Lighting Relays** and click the **Add** button.

To dissociate a relay, select it from the **Relay** list, and click the **Remove** button.

The **Pass-Through Lighting Area** allows you to define a lighting area the user must pass through when entering this area, thereby activating both lighting areas.

In some cases, the site wants the lighting area active during certain hours of the day, then controlled by the onsite status after hours. "**During Time Schedule"** allows you to assign a schedule defining these hours .

At other times, the site needs the lighting area to activate on an input closure. A relay on a sensor or another device could trigger this input. To use this feature, select the input from the **Trip on Input** dropdown list. The **On for Time** defines how long the lighting area is active when tripped by input in *hours:minutes: seconds* format.

Off Delay Time allows for setting a delay for deactivating once all tenants are out of the area. The time is entered in the *hours:minutes: seconds* format. Use this when the user needs to pass back through an area control by the lighting area when leaving.

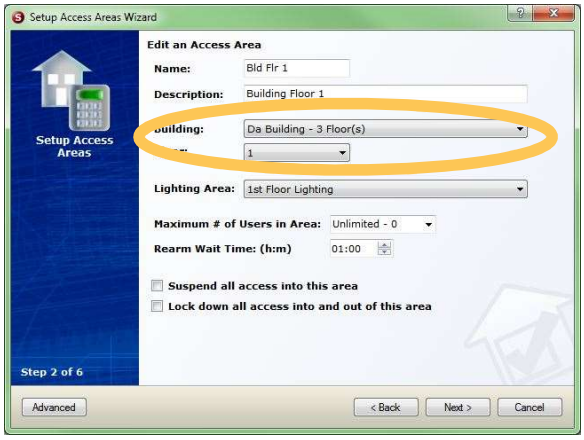
Assigning a Lighting Area to an Access Area

In those cases, which are most cases, when you need to assign the lighting area to an access area, the setting is found on step 2 of the access areas setup (see page 66).

Select the lighting area to apply to this access area from the **Lighting Area** dropdown list.

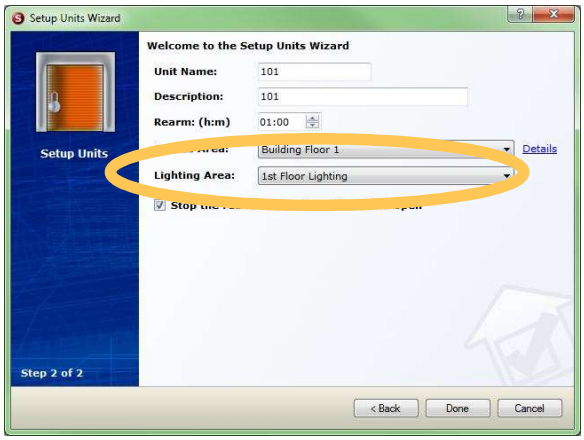
Make sure you advance through to the last screen of the wizard and click the **Done** button to save the changes.

If a user occupies the area, the lighting area remains active.



Picture 71: Assigning Lighting Area to Access Area

Assigning a Lighting Area to Units



Picture 72: Assigning Lighting Area to Units

In some cases, like elevators, you need to assign the lighting area to the units rather than the access area.

The lighting area is assigned in step 2 of the Units setup using the **Lighting Area** dropdown list.

You can select multiple units by clicking on the first unit, then click on the last one while holding the shift key. When doing multiple edits, select only units that are assigned to the same access area because you need to assign both the **Access Area** and **Lighting Area**.

If anyone assigned to a unit with that lighting area is on-site, the lighting area stays active. The lighting area deactivates once all users with units assigned to the lighting area exit the site.

Miscellaneous StorLogix Setups

This module covers the other setup options not covered in previous modules.

Company Info

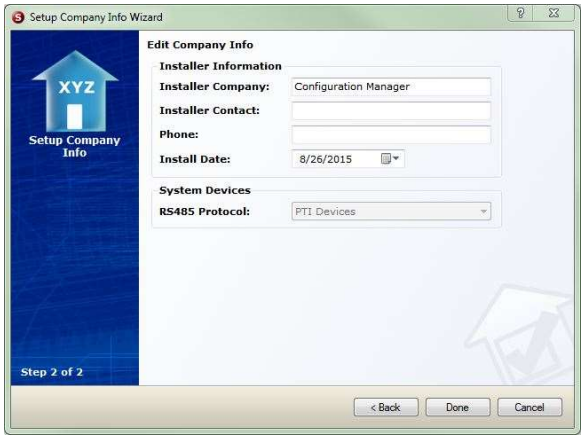
Picture 73: Box 1 Company Info

You cannot change the **Site Code** and is displayed here for informational purposes only.

The **Company Name** and address information is the site name and address. **Company Name** does not influence the name displayed on Apex keypads. The name for the keypad display is in the Falcon XT setup.

Click the **Next** button to advance to step 2.

The **Cancel** button closes the wizard without making any changes.



Picture 74: Box 2 Company Info

Step 2 is the information about the installer of the system.

Installer Company, **Installer Contact**, and **Phone** allow for entering information about the company that installed the system.

The **Install Date** is changeable through the dropdown calendar.

The **RS485 Protocol** is informational, and you cannot change it.

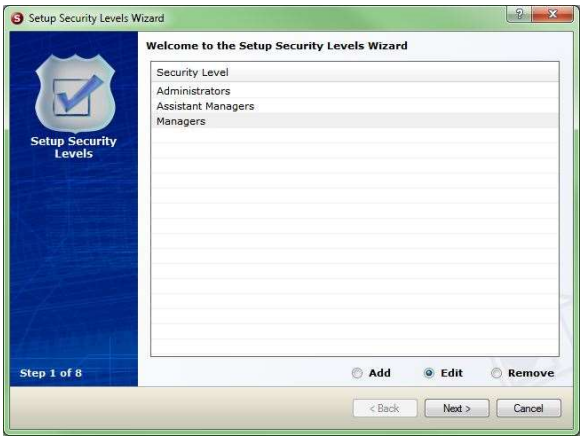
Click the **Back** button to return to the previous screen. The **Done** button saves any changes. To exit the wizard without saving changes, click on the **Cancel** button.

Security Levels

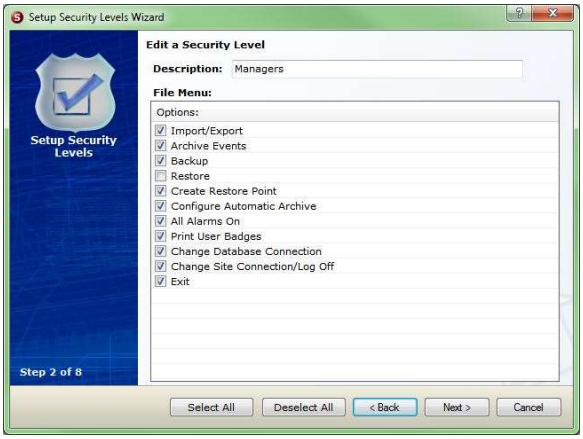
Security Levels control what functions operators have access to in the StorLogix program.

The software creates three levels by default:

- **Administrator** provides access to everything. At least one account should have this level. You cannot change settings at this level.
- **Manager** have less access than the administrator. Settings are editable.
- **Assistant Manager** – have access to only the most used functions. Settings are editable.



Picture 75: Box 1 Security Levels



Picture 76: Box 2 Security Levels

Each step allows you to modify the functions this level operator can use. Check to give access; uncheck to deny access. We recommend all levels can **Change Site Connection** and **Log Off**.

Use the **Select All** button to check all the items in the step. The **Deselect All** unchecks all the items in the current step.

Each step is one of the StorLogix menus. If a user deselects an item, it disables the item in the menu and its icon as well.

Operators

Operators are the users of StorLogix.

Select **Add** and click the **Next** button to create a new operator.

To modify an existing operator, select the operator in the list, select **Edit**, and click the **Next** button.

Delete an operator by selecting the operator from the list, choosing **Remove**, and clicking the **Done** button.

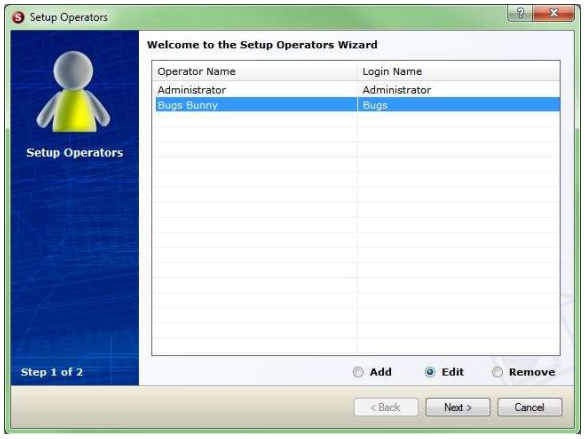
Click the **Cancel** button to close the wizard without making any changes.

Enter the **First Name** and **Last Name** for the operator. The **Login Name** can be different than the operator's name.

The **Security Level** dropdown list assigns the level to this operator.

Enter a **Password** for new operators. For existing operators, check **Change Password** and enter a new "**Password**."

You have an option to enter the operator's email address, which the software uses for email alerts. The **Event Groups** allow you to assign email groups to the user.



Picture 77: Box 1 Operators

Picture 78: Box 2 Operators

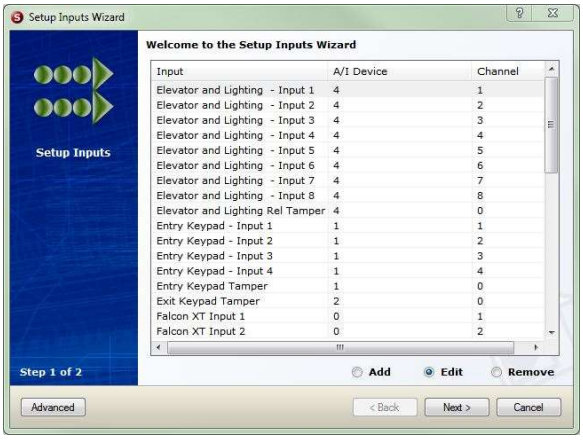
Inputs

Inputs are the opposites of relays. Rather than creating a closure, they sense a closure. They allow other devices like door switches, tamper switches, and sensors to trigger events in the system.

To modify an existing input, select the input in the list, select **Edit**, and click the **Next** button.

Delete an input by selecting the input from the list, choosing **Remove**, and clicking the **Done** button.

Click the **Cancel** button to close the wizard without making any changes.



Picture 79: Box 1 Inputs

Picture 80: Box 2 Inputs

Give the input a **Description** that describes its function within the system. The software always appends channel number to the description.

The **Input Sensor Type** helps to identify the role of the input further and is informational only.

The **Back** button takes you to the previous screen.

Click the **Done** button to save the settings.

To exit without saving, click the **Cancel** button.

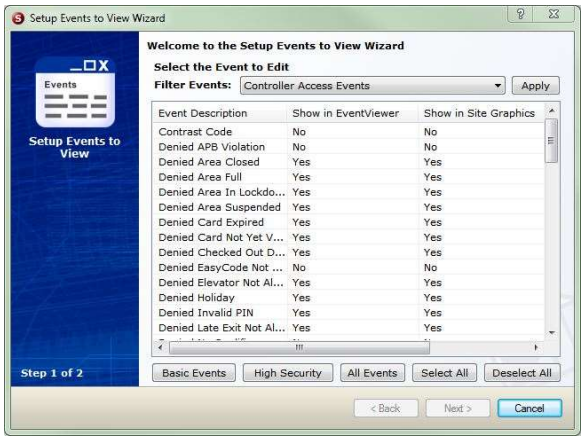
Events to View

Events to View allows you to edit what events show for each of the event log filters.

To edit a filter, select the filter to edit from the **Filter Events** dropdown list and click the **Apply** button.

The **Basic Events** button sets the filter to display only the primary access and alarm events.

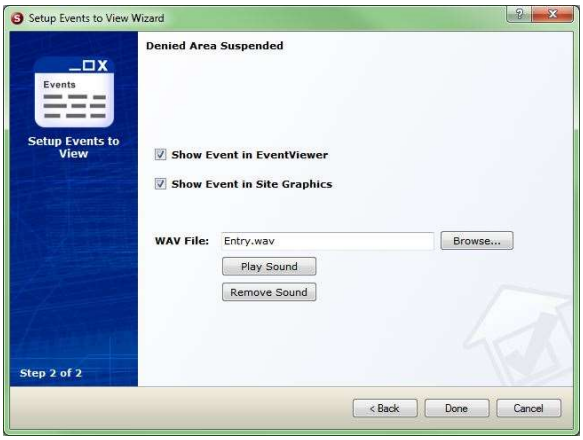
Clicking the **High-Security** button turns on all but some of the troubleshooting events.



Picture 81: Box 1 Events to View

Use the **All Events** button to make the filter display all the events.

Select an event from the list and click the **Next** button to edit the event. Click the **Cancel** button to close the wizard without making any further changes.



Picture 82: Box 2 Events to View

Check **Show Event in EventViewer** to have the event show in the StorLogix or EventViewer program under the selected event filter.

If you have Site Graphics and want the event to show on the Site Graphics event log, check **Show Event in Site Graphics**.

The **WAV File** is the sound file, if any, to play on the computer when the event occurs. Click the **Remove Sound** button to have no sound played. The **Browse** button allows you to search the computer for the sound file to play. The **Play Sound** button plays the sound on the computer.

Click the **Back** button to return to the event list. The **Done** button saves the settings. To exit without saving, click the **Cancel** button.

Classic View uses the All Events filter. For the StorLogix View, you can select a filter from the filter's dropdown list.

Preferences

The **Preferences** controls how the StorLogix software behaves. Access the **Preferences** options through the menus: **User Operations → Preferences**.

General Settings

Advanced Options Always On sets all the setup wizards to default to the advanced settings showing.

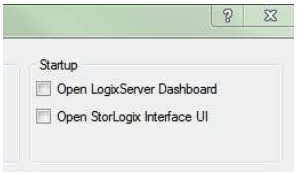
Picture 83: General Settings

To have events sounds to play when they occur and are assigned a soundcheck **Play Event Sounds**.

Checking **Show Main Tool Tips** causes help balloons to pop up when the mouse pointer hovers over an item.

Startup Settings

To have the LogixServer Dashboard automatically start up when StorLogix is running, check **Open LogixServer Dashboard**.

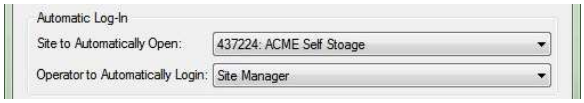


Picture 84: Startup Settings

Open StorLogix Interface UI does the same thing on for the StorLogix Interface user interface.

Automatic Log-In Settings

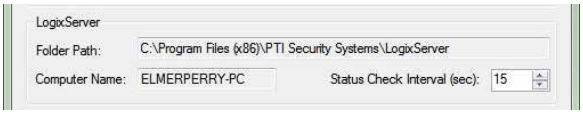
In the **Site to Automatically Open** dropdown list, select the site the software automatically log-in when opening the software. Choose the operator to log-in as from the **Operator to Automatically Login** dropdown list.



Picture 85: Automatic Log-in Settings

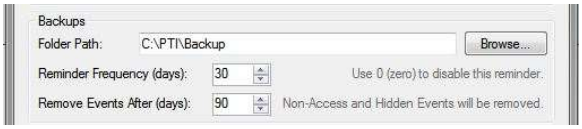
LogixServer Settings

Folder Path shows the path to the LogixServer program. You cannot change this path, and it exists for informational purposes only. You also cannot change the **Computer Name**. The **Status Check Interval** is how often the program checks the status of LogixServer.



Picture 86: LogixServer Settings

Backup Settings



Picture 87: Backup Settings

The **Folder Path** is the location on the computer where the backups are stored. Use the **Browse** button to select a folder for the backups. **Reminder Frequency** sets the number of days between prompts to backup StorLogix. To control how often the system event log is purged, set the number of days in **Purge Events After**. PTI recommends that the **Reminder Frequency** is less than the **Purge Events After**. You can set the **Purge Events After** to 0 to never purge. Setting the Purge to zero is not advisable as eventually, the database gets too big and begins to create problems.

System Performance Settings

To adjust how often the log refreshes, change the value in **Event Log Refresh Rate**. The default setting of 5 seconds works in most cases.

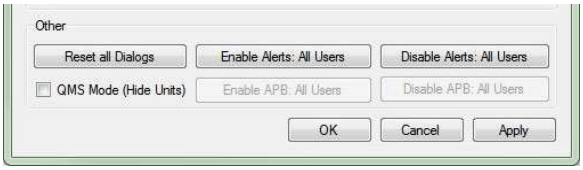
Picture 88: System Performance Settings

Alarm Status Refresh Rate sets how often the software refreshes the alarm status after the initial alarm. The default of 20 seconds works in most cases.

Setting these too low can bog down the system; setting them too high can cause delays in reporting. As a rule, do not change these settings unless PTI Technical Support recommends it.

Other Settings

The **Reset All Dialogs** button sets all pop-up dialogs to their default unchecked state. The checkbox can help in troubleshooting when someone has checked the box to **Not Show Again** on an error or information dialog.



Picture 89: Other Settings

To enable email alerts to all users, click the **Enable Alerts: All Users** button. The **Disable Alerts: All Users** remove email alerts for all users.

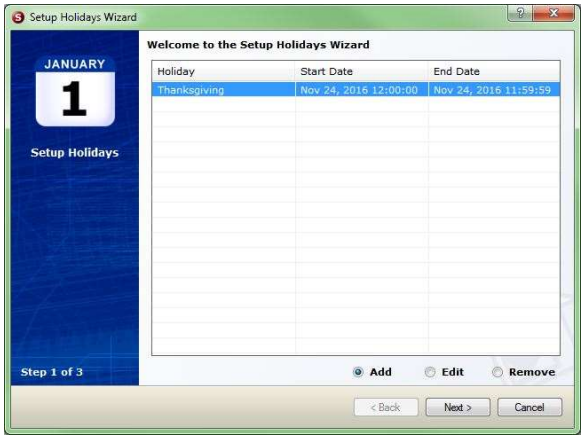
QMS Mode (Hide Units) puts the system into a special mode that does not use units. PTI designed this mode for special applications like office spaces.

To require all users to obey antipassback rules, click the **Enable APB: All Users**. Click **Disable APB: All Users** to exempt all users from antipassback rules. When enabling APB, make sure to setup APB in the Falcon XT Setup wizard (advanced settings).

Click the **OK** button to save the settings and close the dialog. The **Cancel** button closes the dialog without saving the changes. To save the settings without closing the dialog, click the **Apply** button.

Holidays

are for setting special days where access is different than usual. The list shows holiday the user created. By default, the software does not holiday.



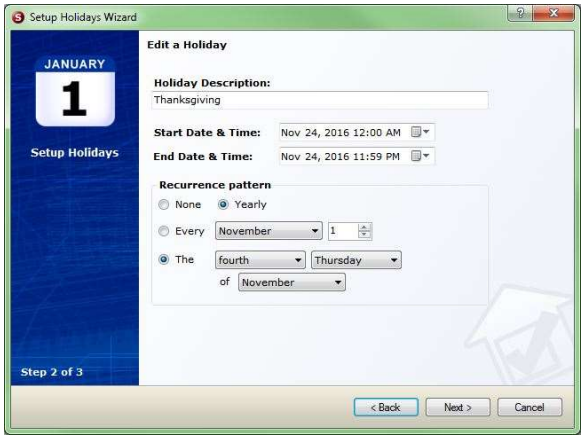
Picture 90: Box 1 Holidays

Select **Add** and click the **Next** button to add a new holiday.

Make changes to an existing holiday by selecting it from the list, selecting **Edit**, and clicking the **Next** button.

To delete a holiday, select the holiday, select **Remove**, and click the **Done** button.

Click the **Cancel** button to exit the wizard without making any changes.

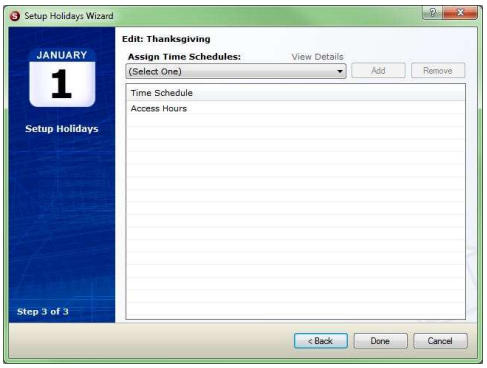


Picture 91: Box 2 Holidays

Give the holiday a name in the **Description** field.

Start Date & Time and **End Date & Time** define the next occurrence of the holiday. You can control the times involved, and the range can include multiple days.

In the **Recurrence Pattern** section, you can define if and how the holiday repeats. If the holiday does not repeat, select **None**, otherwise select



Picture 92: Box 3 Holidays

Yearly.

If the holiday repeats on the same day every year, select **Every**, pick the month from the dropdown list, and enter the day of the month in the number field. However, if the holiday repeats on a specific day of the

week in the month, select **The**, and select the week, weekday, and month from the dropdown lists.

From the **Assign Time Schedule** dropdown list, select the "Time Schedule" affected by this holiday. Click the **Add** button to add it to the list. Repeat for all schedules affected by this holiday.

To dissociate a schedule, select it from the **Time Schedule** list box and click the **Remove** button.

Click the **Back** button to return to the previous screen. The **Done** button saves the settings. To close without saving, click the **Cancel** button.

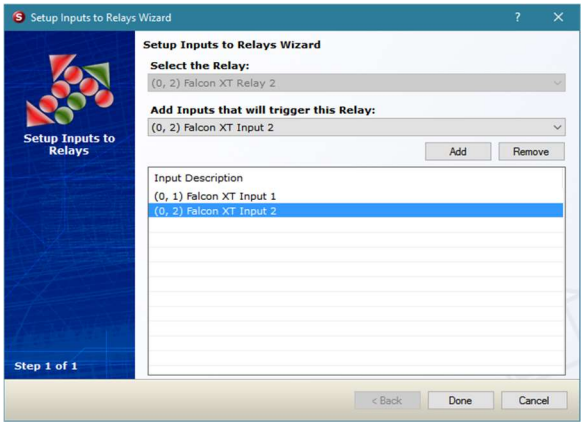
Inputs to Relay

Inputs to Relay allows you to trigger a relay on an input closure. You can use this for things like setting up a switch to manually trigger a relay. On input closure, the relay triggers for the time set in Relays (page 76) setups.

Select the relay you want to be triggered from the **Select the Relay** dropdown list. To add an input point, select the input point from the **Add Inputs that triggers this Relay** dropdown list, and click the **Add** button. Repeat for all inputs that can trigger this relay.

Dissociate an input by selecting it from the **Input Description** list box and clicking the **Remove** button.

Click the **Done** button to save the settings. To exit without saving, click the **Cancel** button.



Picture 93: Box 1 Input to Relay

Mobile Phone Apps

PTI offers two mobile apps, StorLogix Mobile 2.0 for the site managers and EasyCode 2.0 for the storage customer. Both applications are available for both iOS and Android. This module discusses the setup and basic troubleshooting of both apps.

StorLogix Mobile 2.0

PTI designed StorLogix Mobile 2.0 for use by site management. The app is available at Google Play and iTunes Store and works with StorLogix version 5. The app allows managers to open doors and gates, view events, look up tenants, suspend/unsuspend tenants, and control DoorBoss.

Gathering Needed Information

To set up StorLogix Mobile 2.0, you need to gather the following information:

- Device Phone Number
- StorLogix Operator ID
- StorLogix Operator ID Password
- StorLogix Site Code
- 10-Character Site Key/Easycode Site Key

Device Phone Number

During the setup process of StorLogix Mobile 2.0, the app asks for the 10-digit phone number of the phone where the installation is taking place.

StorLogix Operator ID/Password

PTI designed StorLogix Mobile 2.0 to make a direct connection to the site's StorLogix computer. When making the connection, the app logs into StorLogix. The manager installing the app uses the same login and password used to login to StorLogix. Note: The site cannot use the Administrator login and password.

StorLogix Site Code

The Site Code is a "4 to 6" digit number assigned to the site during the StorLogix installation. You can find the code in the upper-left-hand corner of the software.

Picture 94: Site Code

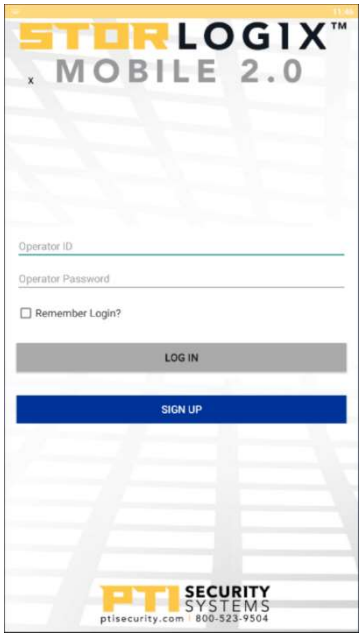
EasyCode Site Key

The EasyCode Site Key is a 10-digit alpha-numeric number assigned to the site during an Easycode installation. You can find the number in the EasyCode menu of StorLogix, under "Register EasyCode Site Key…" Note if the site does not have EasyCode they must contact PTI Tech Support.

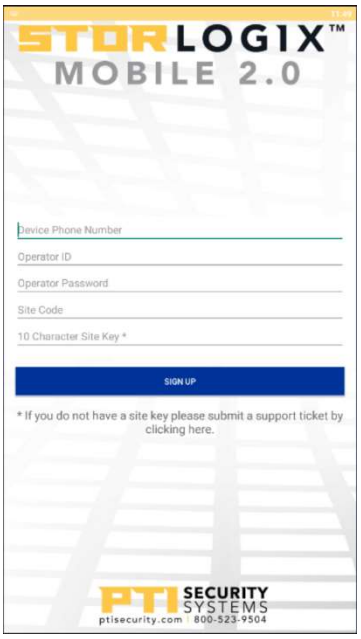
Picture 95: Site Key Location

Setting up StorLogix Mobile 2.0

Setting up StorLogix Mobile 2.0 starts with downloading the app from the Google Play Store or Apple App Store. After the app installation, open the app and click the blue "Signup" button. In the next screen, enter the device phone number, Storlogix Operator ID/Password, Site Code,



Picture 96: StorLogix Mobile 2.0 Login Screen



Picture 97: StorLogix Mobile 2.0 Setup Screen

and EasyCode site key. When you enter all the information into the app, click the blue "Signup" button. Once you click the signup button, the app moves over to the site information.

EasyCode 2.0

EasyCode is a mobile app designed for use by the self-storage customer. EasyCode 2.0 requires StorLogix version 5 or greater. EasyCode 2.0 has an annual service fee paid by the site. For details on registering and setting up EasyCode 2.0, see the video at *https://youtu.be/egAHlysiqHI*.

With the app, the customer can activate devices set to trigger with EasyCode 2.0, allowing them to open gates and doors. This activity is recorded in the event log, just as though they had used the keypad to enter their code. The customer can also view information on the units they have rented, and activity associated with their units.

EasyCode 2.0 App Configuration

EasyCode is a custom configuration done by PTI Technical Support.

Troubleshooting StorLogix Mobile 2.0

Troubleshooting the StorLogix Mobile is mostly a verification of all the settings. Here is a quick list of things to check.

- Make sure LogixServer is running and online
- Make sure the site's StorLogix computer connects to the Internet.
- Verify the app is using a valid StorLogix log-in and password.
- Verify the app is using the correct EasyCode site key.
- Verify that StorLogix Sync Push is allowed in the computer's firewall.
- Restart the LogixServer and StorLogix Sync Push services.
- If the site uses EasyCode, verify EasyCode is operational.

Troubleshooting EasyCode

Troubleshooting EasyCode like the StorLogix Mobile is mostly verifying the settings. The troubleshooting can fall into two categories: EasyCode offline and setup/connection issues.

EasyCode Offline

- Verify the Falcon XT is online
- Verify the computer has access to the Internet
- Verify that the StorLogix Sync Push service is running

Setup / Connection Issues

- Verify the EasyCode app has the correct Site Code.
- Verify the EasyCode site key in StorLogix, **EasyCode → Register EasyCode Site Key**
- Verify the operator's log-in used by EasyCode
- Restart the StorLogix Sync Push service
- Restart the LogixServer

Software Troubleshooting

While most issues with the hardware are related to physical connections not setup/programming issues, users of StorLogix can also experience issues with the software and its communications with the Falcon XT. In this section, we discuss the tools and information a tech can use to troubleshoot the computer and software issues.

Working with the StorLogix Services

There are 5 services at the heart of the StorLogix software. Knowing how to start, stop, and manipulate these services can help in troubleshooting some of the issues with the software. Each of the services performs a specific task in the system. Refer to .

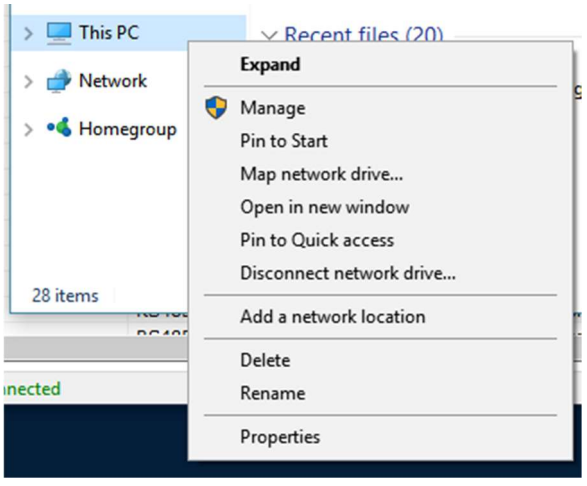
Service	Function
SQL Server (PTI) / MSSQL$PTI	The StorLogix database
LogixServer	Communications to the Falcon XT(s)
StorLogix Interface	Processes data from the account management software
StorLogix Sync	Communications between StorLogix App and the computer
StorLogix Sync Push	Communication between EasyCode and the computer

Table 8: StorLogix Services

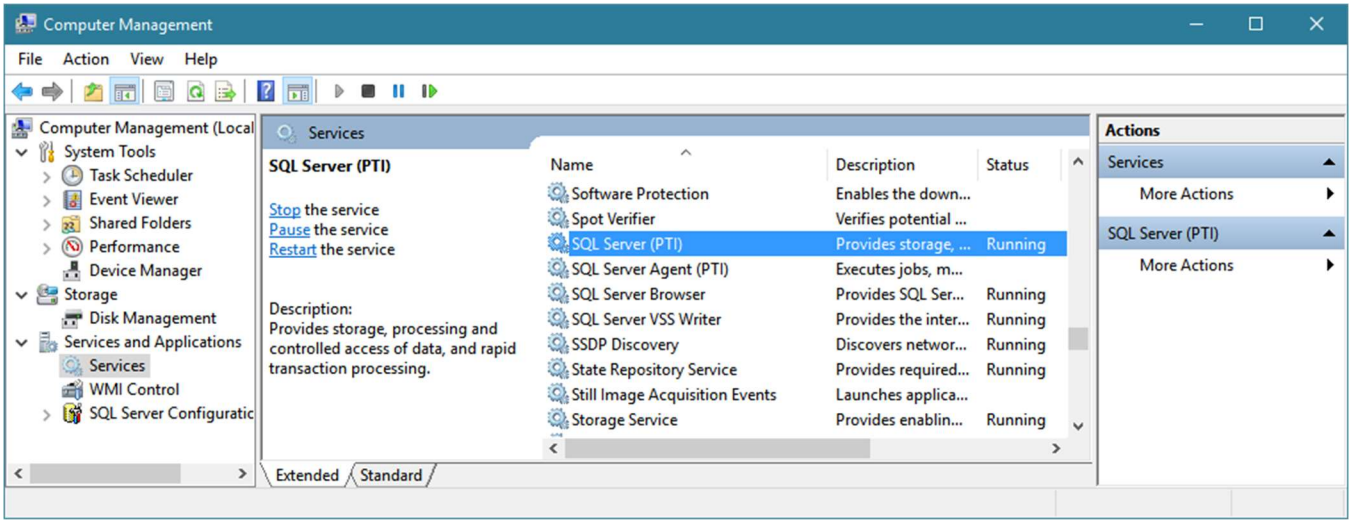
Access, Start, Stop, and Restart Services

Windows provides several ways to access the services running on the computer. This section shows you one of those methods which should work on most versions of the Windows operating system. Depending on the version of Windows, the screens may look different than those shown here.

Open Windows's File Explorer. You can usually access the File Explorer through the Start menu. Right-click on the folder representing the computer. Depending on the version of Windows, the folder is named Computer, My Computer, or This PC. From the right-click menu, select **Manage**. The Computer Management utility opens.



Picture 98: Accessing Services

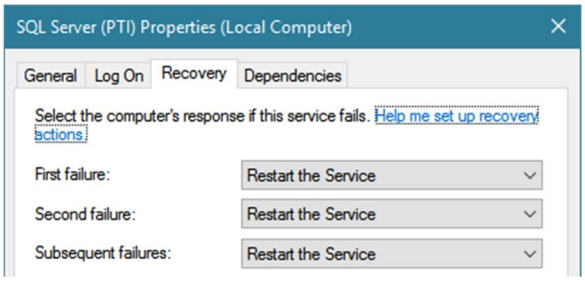


Picture 99: Services Windows

In the left panel, click the arrow beside **Services and Applications**, then select **Services**. The center panel fills with a list of all the services on the computer. Each entry shows the status of the service. You can select any of the services, and you get the options to **Stop**, **Pause**, or **Restart**. If the service is not running, you have the option to start the service.

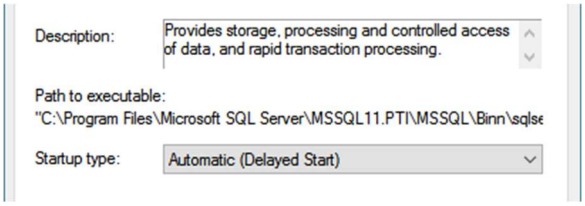
Sometimes, the services do not start after a reboot. Use the following two tweaks to help eliminate this issue.

1. Right-click the service in question and select **Properties**. On the **Recovery** tab, set the **First Failure**, **Second Failure**, and **Subsequent Failures** to **Restart the Service**. This tweak alone could resolve the startup issue. Test the system with this tweak before trying the second one.



Picture 100: Restart Options for Services

2. On the **General** tab of the service's **Properties** dialog, set the **Startup Type** to **Automatic (Delayed Start)**. After a reboot, the service could take up to 5 minutes to start. Keep this in mind should you use this tweak. The user needs to wait for about 5 minutes before launching any of the StorLogix programs.



Picture 101: Startup Options for Services

Troubleshooting Connection Issues in LogixServer

On some occasions, you have issues with the communication between the computer and the Falcon XT. The exact issue can vary depending on the connection type. Here you find some general troubleshooting steps you can take to resolve these communications issues.

Five Connection Types

1. **USB** – direct connection through a USB A to B connectors. Max 15' / 3m.
2. **RS-232** – direct connection through a serial cable to an RS-232 port on the computer. Max 50' / 15m. This connection requires a special cable from PTI.
3. **Dial-Up Modem** – uses a connection through an analog telephone line. This method is not recommended and should always be considered a last resort. This setup requires Matching Courier modems on both ends.
4. **Ethernet on LAN** – a local network connection to the Falcon XT. Max 328' / 100m.
5. **Ethernet on WAN** – uses a network connection across the internet through a broadband connection.

General Troubleshooting Steps

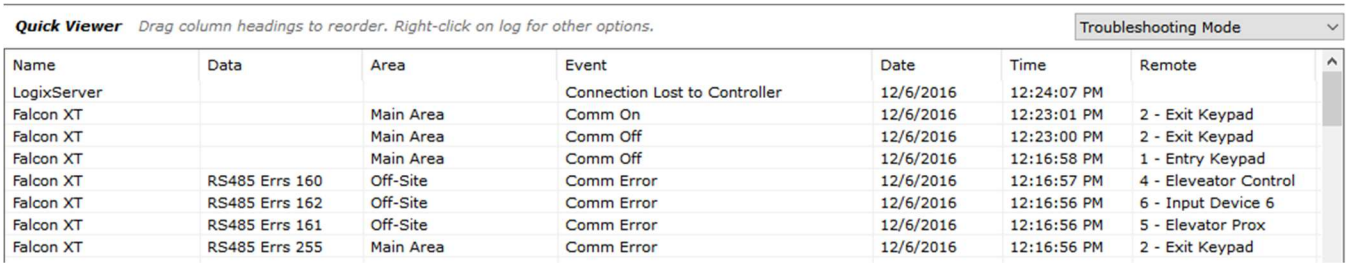
- Make sure to select the proper connection type in LogixServer.
- Verify that the Falcon XT is getting 24 VAC from the power transformer. If the voltage falls below this minimum, the XT cannot communicate with the computer. The issue can happen when the XT is being powered only through the battery.
- Restart the LogixServer service. Sometimes, the service gets locked up, and restarting can get it out of the "stuck" state. See (page 96).
- Reset the Falcon XT by pressing the reset button (SW1) in the upper-left corner of the Falcon XT circuit board. The reset button resets the communications as well as power cycling the devices using the output power on P13 (Remote Devices).
- Replace any cables involved in the communications connection to the Falcon XT (USB, serial, network cables).
- Trying a different connection type, e.g., switch from USB to Ethernet.
- "On LAN" connection, make sure the computer or network firewall is not blocking the connection to the Falcon XT.
- On WAN connection, verify the port forwarding on ports 8897, 7955, and 7950 to the Falcon XT at the remote site.

StorLogix Troubleshooting Tools

Besides the Heath Check mentioned previously, the StorLogix program has several tools that can help you diagnose/correct issues in the program. The two chief components are the Troubleshooting Mode event filter and the Database Troubleshooter.

Troubleshooting Mode Event Filter

In the event filter dropdown list, there is a **Troubleshooting Mode** filter. This filter displays events that do not show in other filters, not even the **All Events** filter.



Quick Viewer *Drag column headings to reorder. Right-click on log for other options.* Troubleshooting Mode

Name	Data	Area	Event	Date	Time	Remote
LogixServer			Connection Lost to Controller	12/6/2016	12:24:07 PM	
Falcon XT		Main Area	Comm On	12/6/2016	12:23:01 PM	2 - Exit Keypad
Falcon XT		Main Area	Comm Off	12/6/2016	12:23:00 PM	2 - Exit Keypad
Falcon XT		Main Area	Comm Off	12/6/2016	12:16:58 PM	1 - Entry Keypad
Falcon XT	RS485 Errs 160	Off-Site	Comm Error	12/6/2016	12:16:57 PM	4 - Eleveator Control
Falcon XT	RS485 Errs 162	Off-Site	Comm Error	12/6/2016	12:16:56 PM	6 - Input Device 6
Falcon XT	RS485 Errs 161	Off-Site	Comm Error	12/6/2016	12:16:56 PM	5 - Elevator Prox
Falcon XT	RS485 Errs 255	Main Area	Comm Error	12/6/2016	12:16:56 PM	2 - Exit Keypad

Picture 102: EventLog Troubleshooting Mode

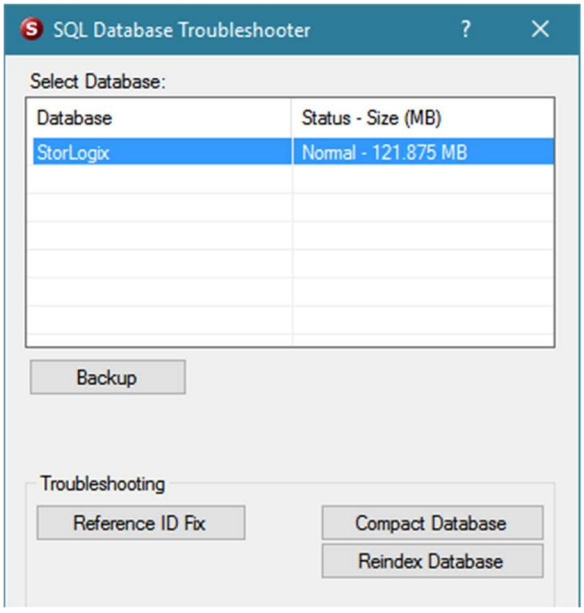
Troubleshooting Mode is the quickest way to look for communications issues and other errors. If you are unsure what a message means, you can contact technical support for assistance. Besides seeing the error message, the log shows every event that happens in the system. For example, with access granted, it reports what relay(s) fired in conjunction with the valid code entry. Troubleshooting Mode is an easy way to verify step by step what is happening when an event occurs in the system. Unlike the other filters, you cannot block any events from showing in the Troubleshooting Mode log.

SQL Database Troubleshooter

The **SQL Database Troubleshooter** gives you tools to correct issues with the SQL database. To open the Troubleshooter, select the menu **Tools → Database Troubleshooter**.

The **Backup** button allows you to create an SQL backup of the selected database.

Clicking on the **Reference ID Fix** goes through the database and correct any duplicate ID assignments.



Picture 103: Database Troubleshooter

Re-index Database will "defrag" the database and is useful when the program is starting to get sluggish. This utility puts things back in their proper order.

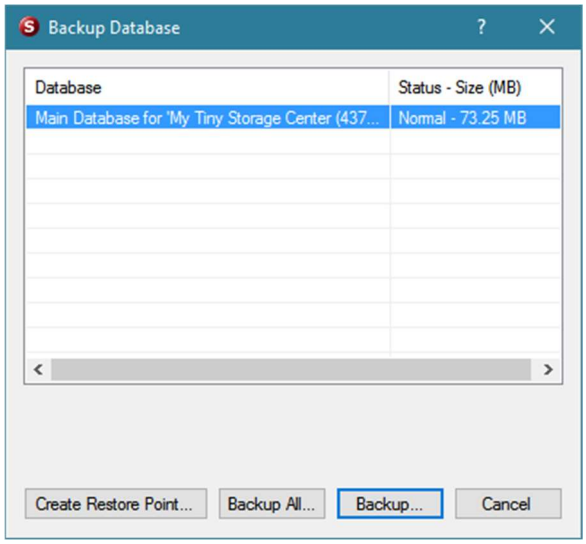
Another tool for help in a sluggish system is the **Compact Database** button, which eliminates records that are no longer needed or are waiting for deletion from the system.

While these tools can help some issues, there are times when more significant steps are needed. See (page 104).

Backup

Although the program does periodically prompt the operator to do a backup, there are times when you want to manually backup the system. Any time you are about to make changes to the software or after making changes, it is usually a good idea to create a backup just in case something goes wrong, and you need to revert to the previous setup.

Access the backup dialog through the menus **File → Backup**.

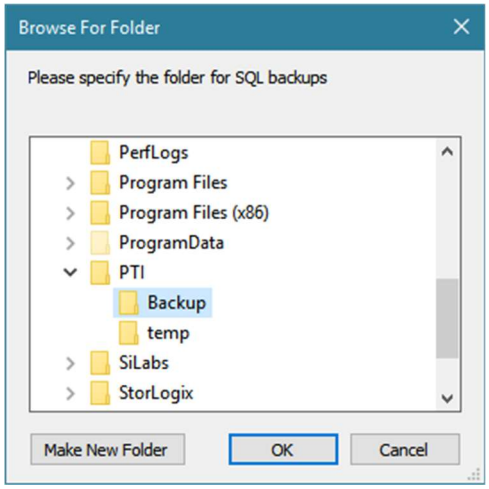


Picture 104: Backup Box

To create a backup, select the database in the **Database** list, and click on the **Backup** button.

Use the **Create Restore Point** to create a complete backup of registry entries and files that you add to the system. Do not use this feature unless you are using badges or have added custom sound files to your system.

Backup All was a holdover from previous versions of StorLogix when the software used separate databases for the log.



Picture 105: Backup Save Box

The **Cancel** button closes the backup dialog without backing up.

When you click on **Create Restore Point**, **Backup All**, or **Backup**, a **Browse for folder** dialog opens. Select the folder where you want the backup to go.

You can use the **Make New Folder** button to create a new folder for the backup.

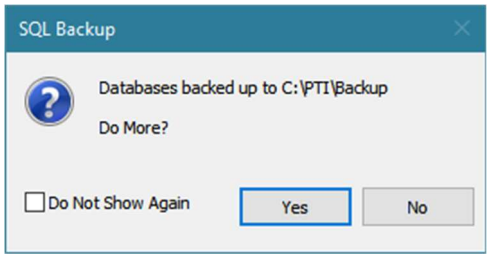
Select a folder and click **OK** to create the backup in that folder.

Click the **Cancel** button to return to the main backup screen and stop the backup process.

The default backup location is *C:\PTI\Backup,* as defined in StorLogix's preferences.

You sometimes find backups created in the SQL instance folder, *C:\Program Files\Microsoft SQL Server\MSSQL11.PTI\MSSQL\Backup*. A best practice is to create the backup on the local hard drive then move it to removable media of some kind like a flash drive. Attempting to backup directly to removable media can result in errors, corruption, or incomplete backups.

After you select a folder and click the **OK** button, StorLogix creates the backup in the selected folder. A message window pops up, informing you that the backup has completed.



Picture 106: Backup Save Box

Click the **Yes** button to create another backup. You return to the beginning backup screen.

Clicking the **No** button exits the backup screen and return you to the StorLogix program.

The checkbox for **Do Not Show Again** prevents the message from showing again and automatically uses the **Yes** or **No** selection you made.

Restore

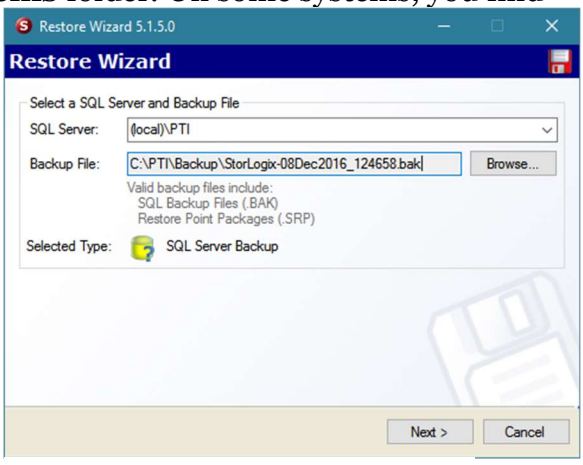
The Restore process takes information from a backup and restores the data from the database to the time the backup creation. Before restoring a backup, close StorLogix, LogixServer Dashboard, and StorLogix Interface if they are open. Open the Windows start menu and find the **Restore Site Data** under the **PTI Security Systems** folder. On some systems, you find it in a subfolder named **StorLogix**.

Use the **Browse** button to locate the backup or restore point you want to use.

The two most common places to look for backups are *C:\PTI\Backup* and *C:\Program Files\Microsoft SQL Server\MSSQL11.PTI\MSSQL\Backup*.

The **SQL Server** is the connection to the PTI database. In most cases, leave this at *(local)\PTI*.

Click the **Next** button to advance to the second step.

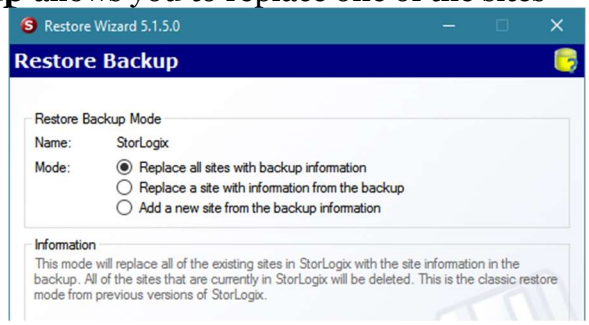


Picture 107: Box 1 Restore

The **Cancel** button closes the wizard without restoring the backup or restores point.

On the second screen, select how you want to use the backup.

Replace a site with information from the backup allows you to replace one of the sites defined in the database with the data in the backup.



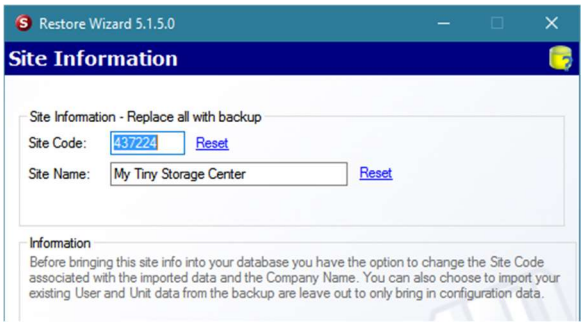
Picture 108: Box 2 Restore

Replace a site with information from the backup allows you to replace one of the sites defined in the database with the data in the backup.

Add a new site from the backup information that allows you to add a site to the setup using the information in the backup.

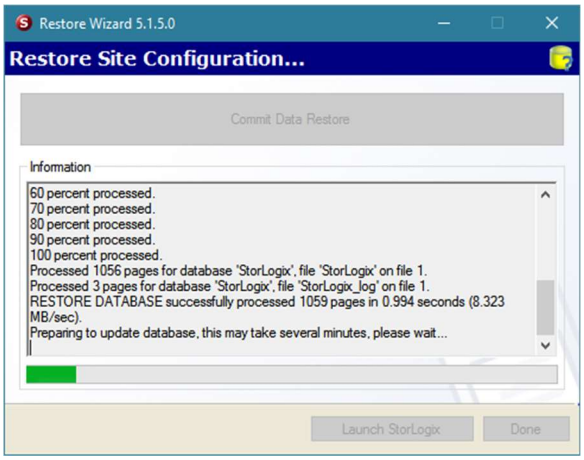
Use the **Back** button to return to the previous screen. Clicking the **Next** button takes you to the third step. **Cancel** closes the wizard without changing any data.

On the third step, the Site Code and the Site Name should populate automatically from the backup information. You can change these settings, but in most cases, you will not.



Picture 109: Box 3 Restore

Use the **Back** button to return to the previous screen. Clicking the **Next** button takes you to the fourth step. **Cancel** closes the wizard without changing any data.



Picture 110: Box 3 Restore

The fourth step is the actual restore process. The progress bar at the bottom shows the progress of the restoration. Once it finishes, the buttons become activated, and the progress bar fills.

Click the **Launch StorLogix** button to open StorLogix and close the wizard.

To close the wizard without launching Storlogix, click the **Done** button.

Appendix A – Door Boss Latch Integration Guide

DOOR BOSS

LATCH INTEGRATION GUIDE

INTEGRATED HASPS


Chateau C-ARL-1-S


Chateau C-ARL-1


Chateau C-ARL-PLUS-1


Chateau C-GR-2-S


C-ARL-PLUS-1-Mini


Chateau C-DL-1


Chateau C-ARL - F - ZC


Chateau C-ARL-F-CH


Chateau C-ARL-A- Mini


Defense - SS – DBCI - 1


Defense - SS – RL 1


Defense - SS – RL 2


Defense – SS - 487



Janus Mini Latch

HASPS NOT INTEGRATED


Janus 60287 Latch
Currently does not integrate


DBCI Apex Latch
Currently does not integrate
No plans to integrate

NOTE: This document is to be used by the sales team and installers, ***and is intended for internal use only.*** **NOT FOR CUSTOMER USE.**

Appendix B – Final Test

1. How do you configure the Intercom connection on a keypad?

2. How far back from the unit hasp do you install a DoorBoss?

3. Can StorLogix be installed on a MAC?

4. What does “short-wiring” a device accomplish?

5. How does the Core Graphics computer connect to the Falcon XT?

6. What is the default baud rate for a PTI device?

7. On the Falcon XT, D24(SYS1) blinking three times means?

8. Using the Relay Boards Dip Switches, what is the highest address for the equipment?

9. Can you install a PTI wireless Headend, Transceiver, or Repeater inside an “I” Beam?

10. What gauge wire do PTI devices use to connect to the Falcon XT?

11. True or False: Hard Resetting, the Falcon XT, will not destroy all its data.

12. Can you see the data coming over from the CMA before StorLogix processes it?

13. What are three TCP ports forwarded at the remote site router to connect a Falcon XT and StorLogix over the Internet?

14. What re-engages a DoorBoss if a site does not have an Exit Keypad?

15. Are Holidays predefined in StorLogix?

16. What five items are needed to connect Storlogix to StorLogix Mobile 2.0?

17. What is the First thing you should do when troubleshooting a StorLogix issue?

18. What do LEDs D4 and D5 indicate on a VP keypad?

19. What is the max number of DoorBoss information columns in the Overlock software?

20. What are the five services, in Windows, installed with StorLogix?