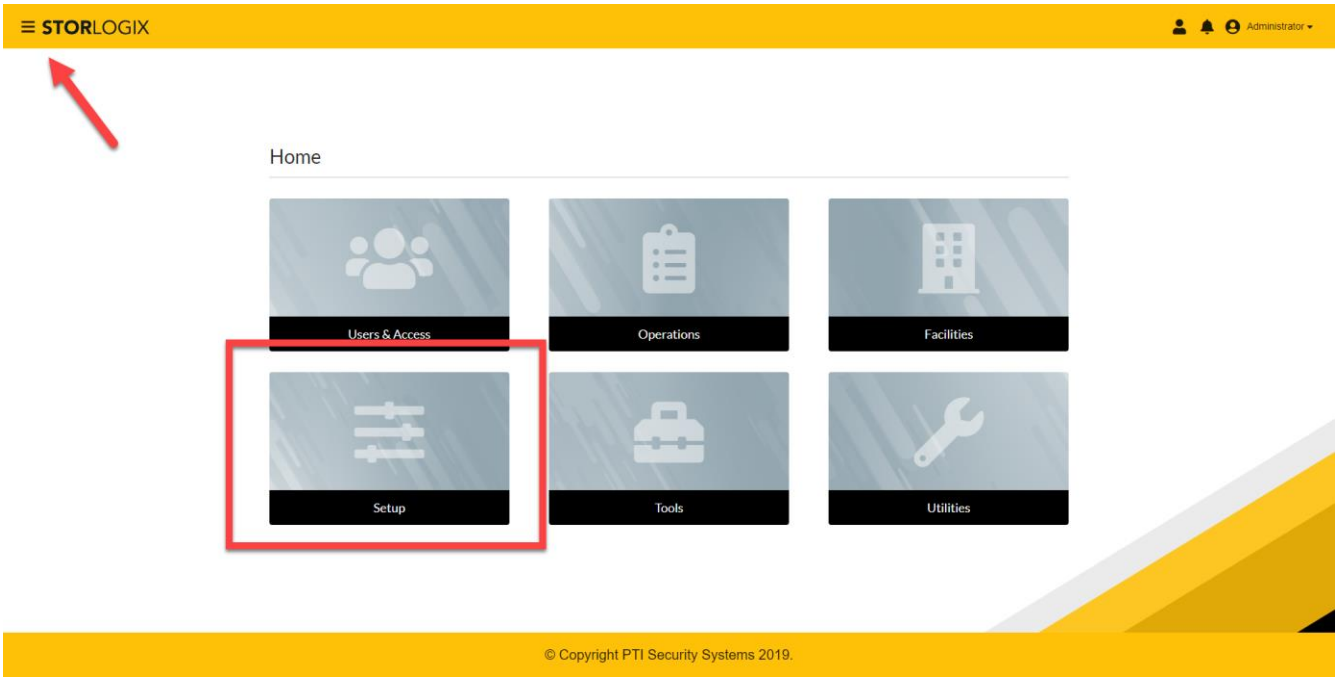
How to Set Up Falcon XT in StorLogix

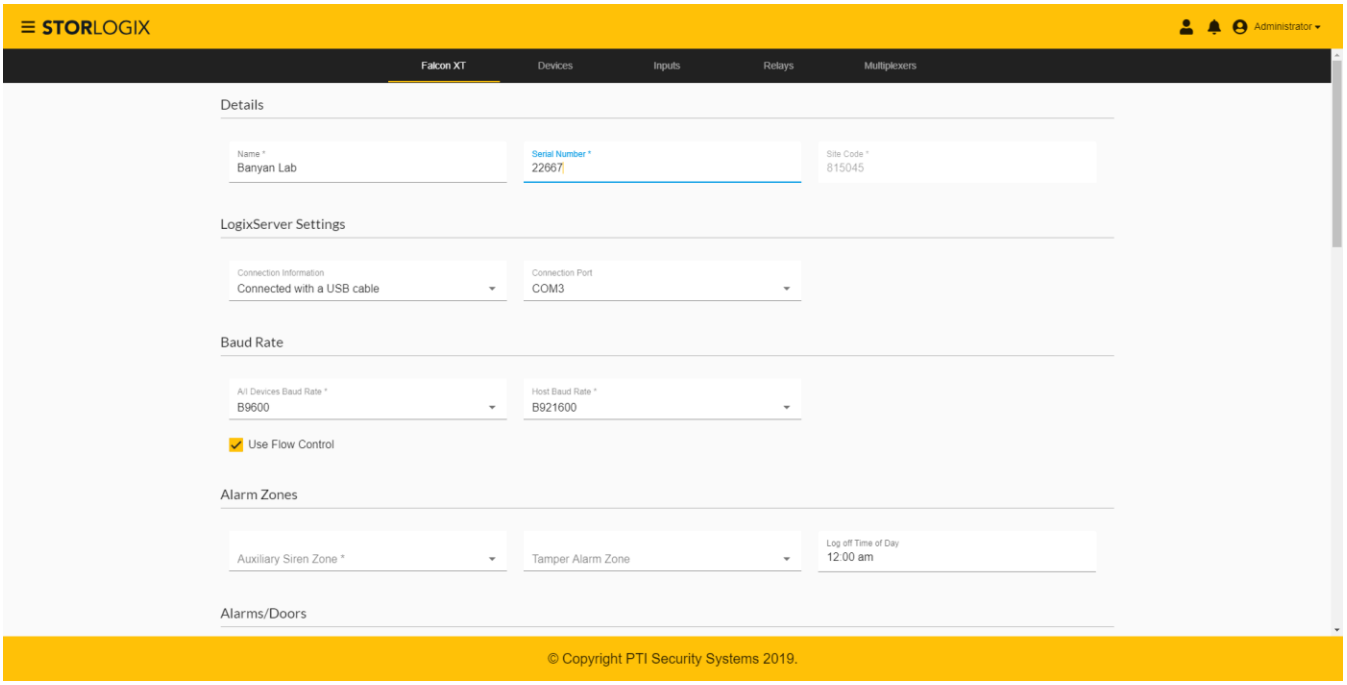
Setting up the Falcon XT

To set up the Falcon XT:

1. Click on your **Setup** in the home screen. (Alternatively, you can click on the three bars in the top left corner to display the Navigation Menu)



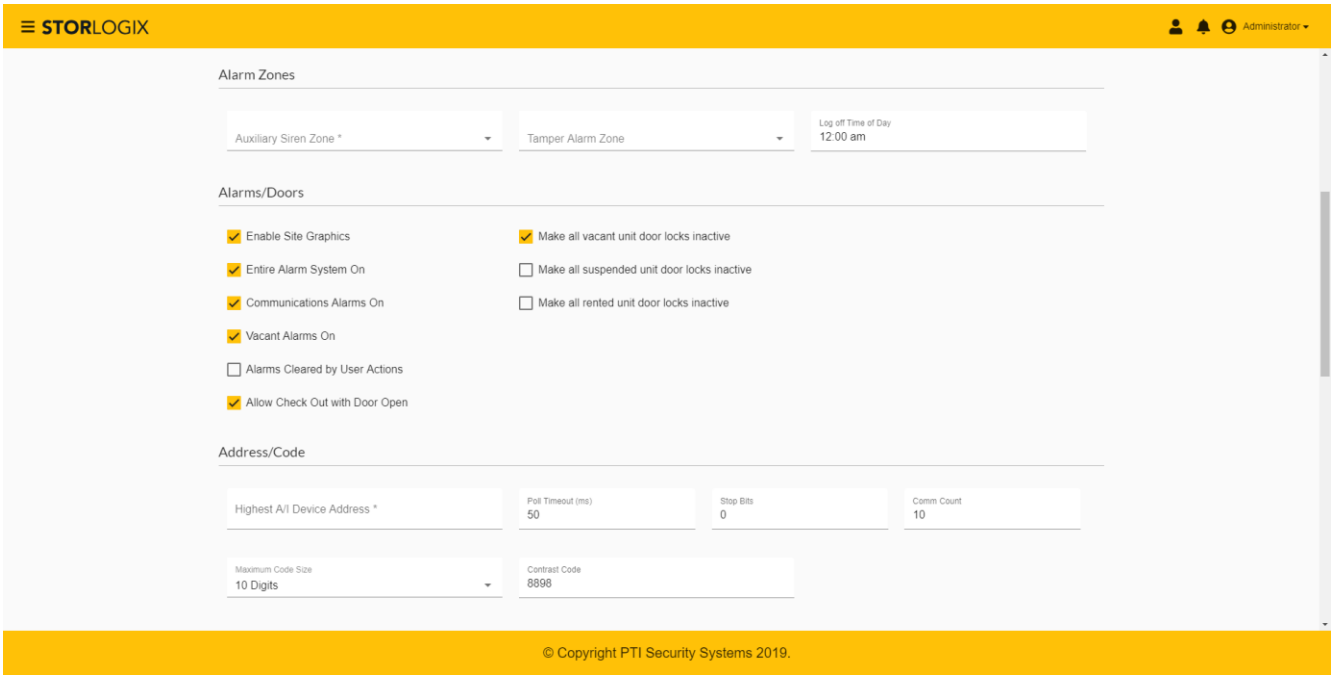
2. You will be directed to a page like the screenshot below.
    a. On the **Details** section, enter your site name and serial number (serial number is located inside the Falcon XT, above the ethernet jack).
    b. The **Logix Server Settings** should auto-fill
    c. The **Baud Rate** should auto-fill by default
    d. **Use Flow Control** should always be check marked. Never remove this checkmark unless instructed to do so by a Technical Support representative.



3. Alarm Zones
    a. **Auxiliary Siren Zone**: This is the Alarm Zone that is set off to allow sirens connected to the Multiplexer Relays to sound. Generally, this is the Default Alarm Zone.
    b. **Tamper Alarm Zone**: This is the Alarm Zone that is set off when tamper alarms in the system are triggered. Generally, this is set to the Default Alarm Zone.
    c. **Log Off Time of Day**: This setting allows the system to automatically log all users off the site at a certain time to clear anyone off-site who did not log off at an exit keypad as they left the site. If this is set to None, then the system never logs these individuals off-site. Caution: We do not recommend that this function be used on sites with 24-hour access because a user could potentially come on-site immediately prior to the Log Off time and be logged off even though they are actually on-site, turning off any lights and setting off alarms.

4. Alarm/Doors
    a. **Enable Site Graphics**: Must be checked if the site is using Site Graphics
    b. **Entire Alarm System On**: Must be checked for the alarm system to work. Removing the checkmark from this field will disable the alarm system.
    c. **Communications Alarms On**: should be check marked. This allows alarms to sound if a keypad, multiplexer, or other AI Device loses communications to the Controller. If the site wiring is installed correctly, then the only time a communication alarm would sound is if an AI Device is damaged in some way.
    d. **Vacant Alarms On**: should be check marked. This allows vacant units with door switches to report door activity. This is highly recommended as it helps prevent unauthorized access to Vacant Units which is often a source of crime on self-storage sites (such as vagrants living in units, illegal drug labs, and theft by hiding in empty units to access other units after hours). It is also a good idea to have this turned on to allow potential customers to hear and see the security alarms when a vacant unit is shown to them. This helps to market your security. To turn Vacant Alarms off, remove the checkmark from this field.
    e. **Allow Check Out With Door Open**: is only used if a Device is set to Check In/Out in the AI Device Properties. If a Device is set to Check In/Out and a user tries to leave the site without closing their door, the keypad will deny them exit and display a message reminding them that they left their door open.

5. **Address/Code** Most often should be left default.
    a. **Highest A/I Device Address** should always be set equal to or greater than the highest AI Device Address number on the system. If you are unsure, always set this number to 127. If the number is set lower than the address on a device, the device will no longer communicate with the Falcon XT and will not function.
    b. **Poll Timeout** The Falcon XT constantly polls the AI Devices to see if they have any information (such as requests for access or door activity). This occurs many times each second. The Poll Timeout is the amount of time that the Falcon XT will wait for an answer from the device before recognizing that there is a communication error and moving on to poll the next device. The Falcon XT will then come back and poll this device again after each successive device, until it finds communications, or until it reaches the **Comm Count**, in which case it will report a Communications Off Event. Random Radio Frequency Interference can periodically interfere with these signals, so the system should be set with some leeway in Polling. This number should be set between 10 and 50 on most systems.
    c. **Maximum Code Size**: is used with magnetic swipe cards and proximity cards. These cards generally have a ten-digit code, but some Accounting Software programs for Self-Storage only allow 7, 8, or 9 digit codes. If your accounting software has this limit, set the Maximum Code Size equal to its limitation
    d. **Contrast Code**: is only used with older models of Falcon Series Keypads, manufactured prior to 2002. These devices did not have a backlit LCD display and so the contrast had to be adjusted to allow it to be read easily in local light conditions. This is rarely used and should only be encountered on retrofits. It is very important to note that the number set as the contrast code CANNOT be issued as an access code to a user.


STORLOGIX
Administrator
Alarm Zones
Auxiliary Siren Zone *
Tamper Alarm Zone
Log off Time of Day
12:00 am
Alarms/Doors
Enable Site Graphics
Entire Alarm System On
Communications Alarms On
Vacant Alarms On
Alarms Cleared by User Actions
Allow Check Out with Door Open
Make all vacant unit door locks inactive
Make all suspended unit door locks inactive
Make all rented unit door locks inactive
Address/Code
Highest A/I Device Address *
Poll Timeout (ms)
50
Stop Bits
0
Comm Count
10
Maximum Code Size
10 Digits
Contrast Code
8898
© Copyright PTI Security Systems 2019.

6. On the same page, scroll down
    a. **Reporting** check boxes should be marked by default
    b. **Anti-Passback** has a dropdown with different settings
        i. Allow Anti-Passback: This allows any valid user to enter or exit the site without a previous exit or entry.
        ii. Timed Anti-Passback: This prevents users from sharing a card by passing back across a gate to the next person.
        iii. Logical Anti-Passback: Used in high security sites that have multiple access-controlled areas. Prevents users from entering an area unless they first entered the area before it.
        iv. Timed Logical Anti-Passback: Combines the previous two, requiring logical anti-passback for entrance within a certain set time.
    c. **Late Exit** is used to control customer exit from the site after their allowed Time Schedule Hours in their *Access Level*. Warning: Use care when setting late exit as users can get stuck on site.
        i. No Late Exit: Limits users to access and exit only during their permitted hours. If a user enters the site before their hours are closed, but stay until their hours close, they will be locked on site.
        ii. Timed Late Exit: Set a grace period that the user can exit the site after hours. Many sites use this to allow clients a 30-60-minute grace period. After the grace period, late users will be stuck on site.
        iii. Counted Late Exit: This allows a limited number of late exits. Allows a user to visit a site after hours. If a user reaches the limit, the user will be locked on site for any future violations.
        iv. Timed – Counted Late Exit: Combines the previous two, allowing a certain number of exits during a set grace period. After, they will be locked on site, even if they haven't reached the count time. After the count time is reached, they will be locked on the site even if they are still within the grace period.
        v. Free Late Exit: Allows exit after hours at any time. A Late Exit violation event will still show on the event log.

    d. **Aux A** and **Aux B** settings should never be changed by the customer without the guidance of Technical Support.

7. Click **Submit** to finish