TX3 Series

TX3-CX-A8 Aperio™ Door Controller System

Installation and Operation Manual

TX3 Aperio Door Controller System Installation and Operation Manual Version 1.6

Mircom
25 Interchange Way
Vaughan, Ontario
L4K 5W3
905.660.4655
http://www.mircom.com

Table of Contents

List of Figures

1 Welcome

This manual provides information about the installation and operation of the TX3-CX-A8 Aperio™ Door Controller System, and must be read in its entirety before beginning any installation work.

Installation must be performed by a qualified technician and must adhere to the standards and special notices set by the local regulatory bodies.

Note: Mircom periodically updates panel firmware and Configurator Software to add features and correct any minor inconsistencies. For information about the latest firmware or software visit the Mircom website at **www.mircom.com**.

For warranty and special notices information see the Warranty and Special Notices chapter on page 106.

Warning: The Aperio Door Controller System must be grounded by a qualified electrician. An improperly grounded unit can result in equipment malfunction and electrical shock.

This chapter explains

- Introducing the TX3-CX-A8 Aperio Door Controller System
- Applications
- Configurable Features
- Installer Responsibilities
- Network Setup
- About This Manual
- Contact Us

1.1 Introducing the TX3-CX-A8 Aperio Door Controller System

The TX3-CX-A8 Aperio Door Controller System is part of the Mircom suite of products that provide building ready monitoring, control and integrated security solutions for use in the high-end multi-tenant residential market.

The Aperio Door Controller System addresses the need within today's high-end multi-tenant residential market for an easy-to-use tenant access system and an easy-to-use configuration utility.

This manual provides the technician with information about the installation and configuration of the Aperio Door Controller System and explains how to configure various components for a new system, including the modification of an existing system.

1.2 Applications

Mircom's Aperio Door Controller System consists of a controller, one or more Aperio hubs, one or more ASSA ABLOY™ wireless devices (door position switches, locksets and card readers), and the TX3 configuration software. The Aperio Door Controller System can set elevator usage if elevator controls are used.

A number of different ASSA ABLOY wireless devices are supported, all of which are configurable using the configurator software.

The Aperio Door Controller System can be used in a stand-alone or networked environment using an RS-485 network, an ethernet TCP/IP network, or an ethernet TCP/IP network with RS-485 subnetworks.

A network can consist of only TX3-CX-A8 panels or a combination of Touch Screens, Lobby Control Units, Elevator Restriction Units, and Card Access Units. Up to 63 units can be networked on any RS-485 network or subnetwork. Valid RS-485 network addresses range from 1 to 63. One of the networked units with a real time clock, such as Touch Screen, Lobby Control or Card Access must have their network address set to 1.

If an ethernet network is used, you can connect more than 63 units to your system. If you use an ethernet network with RS-485 subnetworks, each RS-485 subnetwork can have 63 devices connected to it.

1.2.1 Aperio Door Controller System

The Aperio Door Controller System consists of the following components.

- Aperio Door Controller

- Aperio hub
- Wireless device

The Aperio Door Controller communicates with one or more Aperio hubs on an RS-485 network. The wireless devices communicate wirelessly with Aperio hubs. When an access request is initiated at a device, the device sends the request wirelessly to its hub, and then the hub sends the request to the Aperio Door Controller. The Aperio Door Controller determines whether or not to grant access, and then sends the information to the hub which relays it back to the device.

Each TX3-CX-A8 Aperio Door Controller can by default support up to 8 devices (16 devices with firmware version 3.2.2. and higher) and a maximum of 15 Aperio hubs.

There are 2 kinds of hubs:

- 1 to 1: supports 1 wireless device
- 1 to 8: supports up to 8 wireless devices

The Aperio Door Controller System integrates with the TX3 Telephone Access, Touch Screen, Card Access, and Elevator Restriction systems by utilizing an RS-485 network for both Telephone Access and Aperio Door Controller Systems.

A PC provides configuration and on-line monitoring of the Aperio Door Controller System and the Telephone Access System status.

Note: The RS-485 network for the Aperio hubs is separate from the RS-485 network that connects the TX3 panels. Aperio hubs can only connect to the RS-485 connector on the MD-1113 Module board on the Aperio Door Controller board.

1.3 Configurable Features

The system is configured by connecting inputs and outputs to the Aperio Door Controller, and then using the configurator software to establish the correlations between these inputs and outputs.

Additional physical configuration is required using the DIP switches and jumpers on the panel and Aperio hubs.

- The DIP switches on the Aperio Door Controller specify the address of the panel on the RS-485 network shared with other TX3 panels. (See Setting the DIP Switches on Switch SW2 on page 57.)

- The DIP switches on the Aperio hubs specify the addresses of the hubs on the RS-485 network they share with the panel. (See Setting the Aperio hub address on page 33.)
- Jumper settings set the controller for firmware updates. (See Updating Firmware on page 62.)
- Devices are paired to Aperio hubs using the Aperio Programming Application from ASSA ABLOY. (See Pairing a Wireless Device to an Aperio Hub on page 38.)

1.3.1 Card Formats

- 26-bit Wiegand SIA
- 32-bit CSN
- 34-bit Awid
- 35-bit HID corporate 1000
- 35-bit Indala
- 36-bit HID Simplex
- 36-bit Keyscan C15001
- 37-bit Cansec
- 37-bit HID 10304
- 37-bit Mircom
- 39-bit Kantech XSF
- 50-bit RBH

1.3.2 PC Configurator Software

The TX3 Configurator Software, TX3-MSW, is a combined Telephone Access, Aperio Door Controller, Card Access Controller, Touch Screen, and Elevator Restriction Unit configurator that uses a common database. Once the controller is installed the system applies its default values. Use the configurator software to fully configure the system. See the following documentation:

- LT-995 Telephone Access, Card Access, Configurator and Touch Screen Configuration and Administration Manual
- LT-973 TX3 Software Guide

1.4 Installer Responsibilities

The installation and setup must be done by a qualified technician. The technician is responsible for installing all of the system components, connecting all of the input and output wiring, installing the Aperio hubs, installing the wireless devices for the appropriate door entry systems, and ensuring that the wiring adheres to the requirements of the system for proper operation using the TX3 Configurator software.

1.4.1 PC Requirements

See LT-995, the TX3 System Configuration and Administration Manual, for the latest requirements.

1.5 Network Setup

The Aperio Door Controller System can consist of either a stand-alone controller or networked controllers. Networked controllers can communicate over an RS-485 network, an ethernet TCP/IP network, or a combination of an ethernet network with RS-485 subnetworks. All controllers can communicate over RS-485. To communicate over an ethernet network you need at least one IP-enabled controller (called a Master Node).

The TX3 Configurator software can connect to any of these network configurations. How you connect to the network (that is, through TCP/IP, USB, a modem, or the COM port) determines what devices you can configure on the network using the TX3 Configurator. The different network configurations are explained in the rest of this section.

Figure 1 shows a basic Aperio Door Controller System with one Aperio Door Controller, one Aperio hub, and two locksets. Up to 15 Aperio hubs can be connected to an Aperio Door Controller and each controller can support up to 8 devices (16 devices with firmware version 3.2.2 and higher). The Aperio Door Controller and all Aperio hubs must be within 3000 feet of each other; the maximum distance between an Aperio hub and a device is 45 feet.

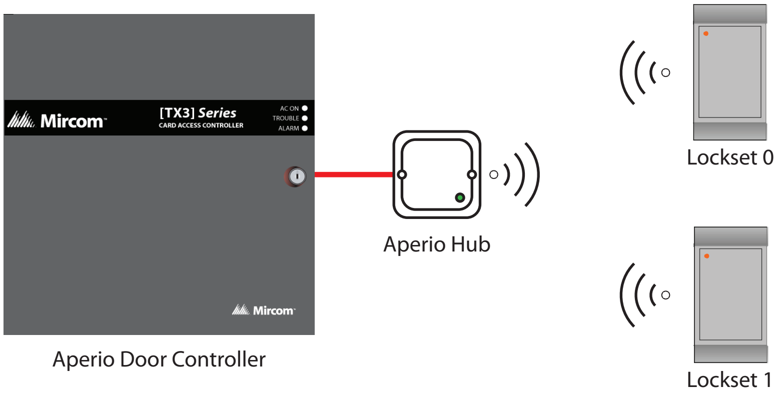


Figure 1. Basic Aperio Door Controller System

Figure 2 shows a network with two Aperio Door Controllers over an RS-485 network, each with one Aperio hub and two wireless devices. The Aperio Door Controller System can have up to 63 controllers networked together on an RS-485 network. If you connect to any of the controllers using a modem, USB, or COM port with the TX3 Configurator, you can configure any of the devices on the RS-485 network using the TX3 Configurator software.

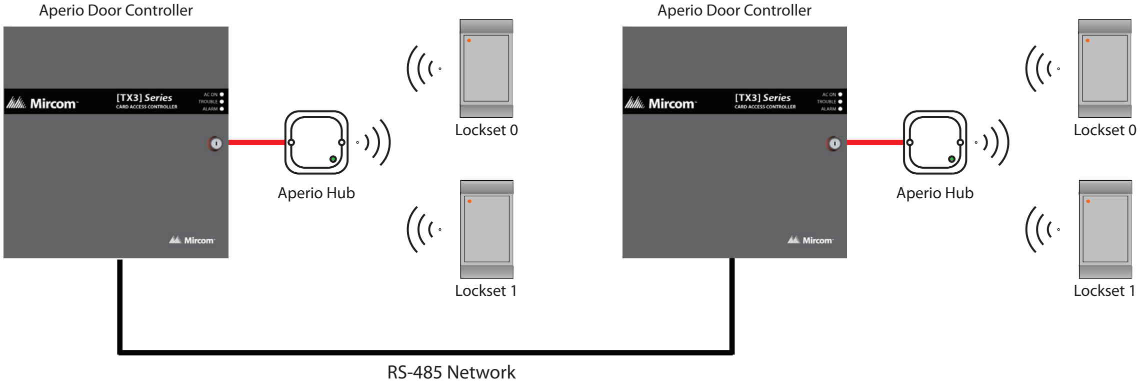


Figure 2. Aperio Door Controller System using an RS-485 network

Figure 3 shows a configuration with Aperio Door Controllers connected to an Ethernet TCP/IP network. This configuration removes the 63 device limitation that you have in an RS-485 network. The devices connected to an Ethernet TCP/IP network are called Master Nodes. If you connect to the TCP/IP network with the TX3 Configurator, you can connect to and configure any of the Master Nodes on the Ethernet TCP/IP network. If you connect directly to one of the Master Nodes using USB, a modem, or a COM port, you will be able to configure that Master Node but not any other Master Node.

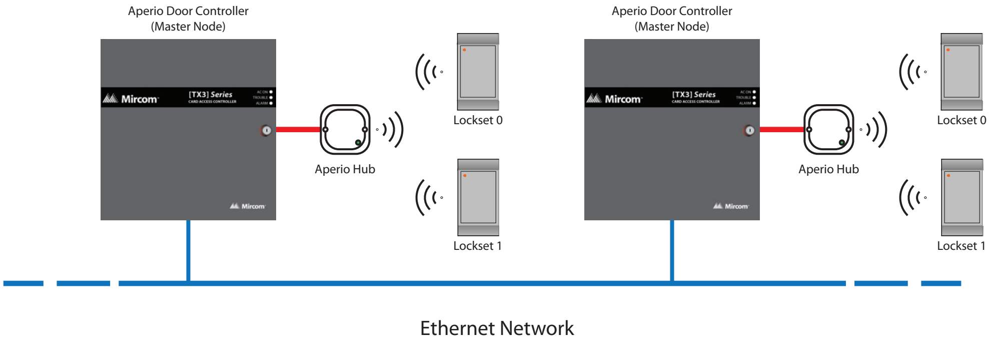


Figure 3. Aperio Door Controller System using an Ethernet TCP/IP network. Controllers connected to an Ethernet network are Master Nodes

Note: In order for an Aperio Door Controller to be a Master Node it must have the optional TX3-IP IP Module installed.

Figure 4 shows an Aperio Door Controller System using an Ethernet network with RS-485 subnetworks. Devices connecting to a Master Node’s RS-485 subnetwork are Slave Nodes to the Master Node. Each RS-485 subnetwork can have up to 63 controllers connected to it; you can still have more than 63 Master Nodes connected to the Ethernet network.

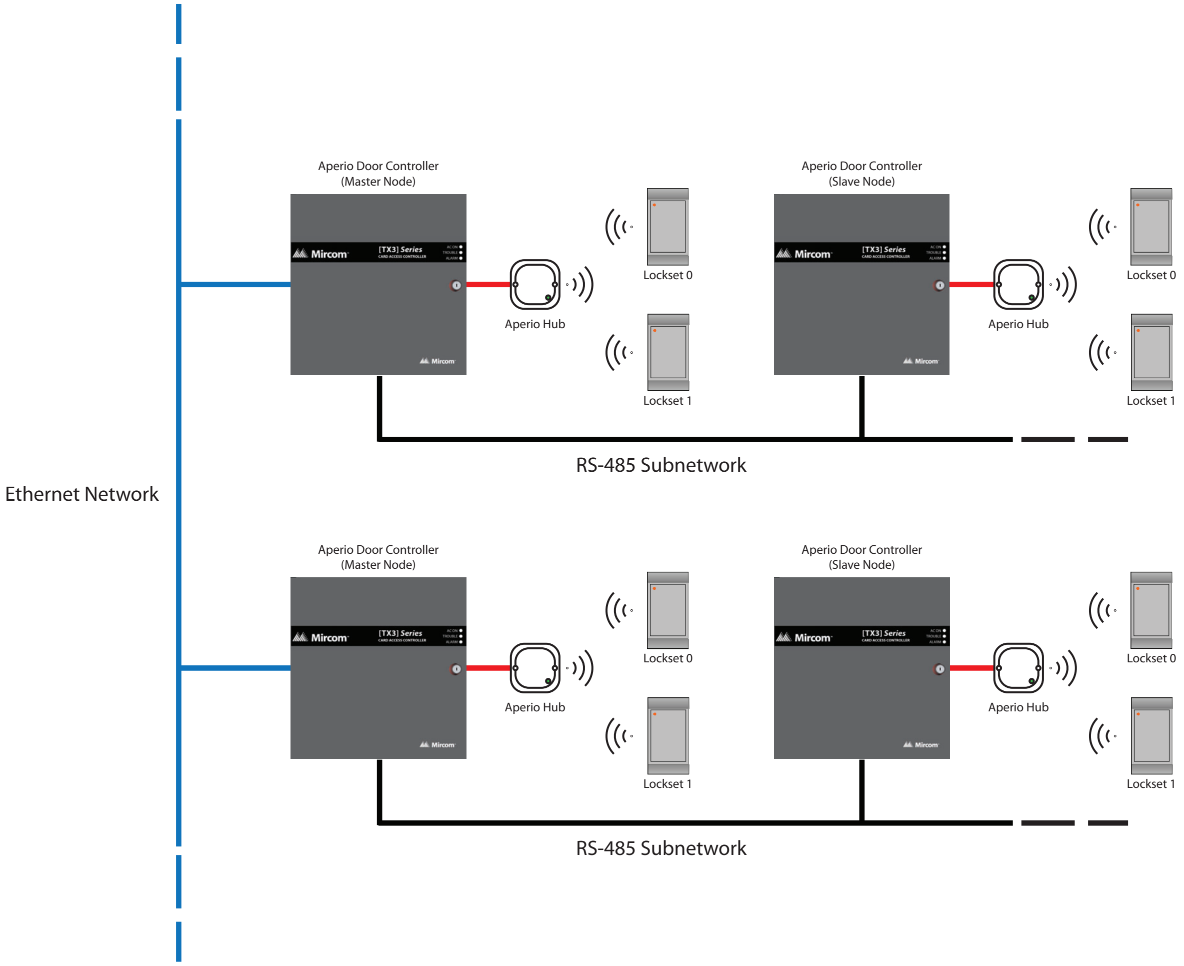


Figure 4. Aperio Door Controller System using an Ethernet network with RS-485 subnetworks

If you connect to the Ethernet network using the TX3 Configurator software, you can configure any of the nodes in the system. If you connect directly to a controller using USB, a modem, or the COM port, you will only be able to configure controllers that are on the same RS-485 subnetwork as that controller.

Note: There can only be **one** Master Node on an RS-485 subnetwork. That is, you cannot connect one RS-485 subnetwork to another RS-485 subnetwork.

1.6 About This Manual

This manual provides comprehensive information on the installation and configuration of the Aperio Door Controller System by the installation technician. Tasks are described in the order that they are likely to be performed.

Chapter 2 describes the installation of the controller.

Chapter 3 describes the configurable modes of operation.

This manual applies to the following model:

- TX3-CX-A8 Aperio Door Controller System Kit

1.6.1 Additional Documentation

For additional documentation, see the following Mircom literature:

- LT-969 TX3 Telephone Access System Installation and Operation Manual
- LT-968 TX3 Telephone Access System User's Guide
- LT-971 TX3-MDM Modem Module Installation
- LT-1161 TX3-IP IP Module Installation Instructions
- LT-5997 TX3-CX-1NP Installation
- TX3 Two Door Card Access System Kit Catalogue Number 6531
- TX3 Series Elevator Restriction Accessories Catalogue Number 6532
- LT-995 TX3 Configuration and Administration Manual
- LT-973 TX3 Configurator Quick Start
- LT-6027 TX3-USB-AD Kit Installation Instructions

1.6.2 Key Terms

The following terms are common and specific to this manual:

CAU. Card Access Unit

ERU. Elevator Restriction Unit

LCU. Lobby Control Unit

1.7 Contact Us

1.7.1 Canada and USA

Toll Free: 1-888-660-4655

Local: 905-660-4655

Fax: 905-660-4113

1.7.2 Website

http://www.mircom.com

2 Installation and Setup

This chapter describes the installation and setup of the controller, Aperio hubs, and wireless devices.

This chapter explains

- Grounding the Aperio Door Controller System
- Installing the Controller and Components
- Controller Board Description
- Connecting the Inputs
- Connecting the Outputs
- Installing and Configuring Aperio Hubs
- Installing and Pairing Wireless Devices
- Setting the DIP Switches on Switch SW2
- Setting Jumpers
- Turning on the Controller
- Updating Firmware
- Beginning Configuration

2.1 Grounding the Aperio Door Controller System

Grounding reduces the risk of electrical shock by providing an alternate escape route for the electrical current. The Aperio Door Controller System is equipped with a 16 gauge electrical wire attached to the panel chassis Ground Terminal.

Note: Do not disconnect this wire.

Attach the end of the supplied wire to a suitable grounding wire 16 gauge or thicker. Attach the other end to the cold water ground.

2.2 Installing the Controller and Components

The Aperio Door Controller surface mounts with four screws as shown in Figure 5. The back cover is 12 inches wide by 14 inches long. The top two mounting holes are 10 inches apart.

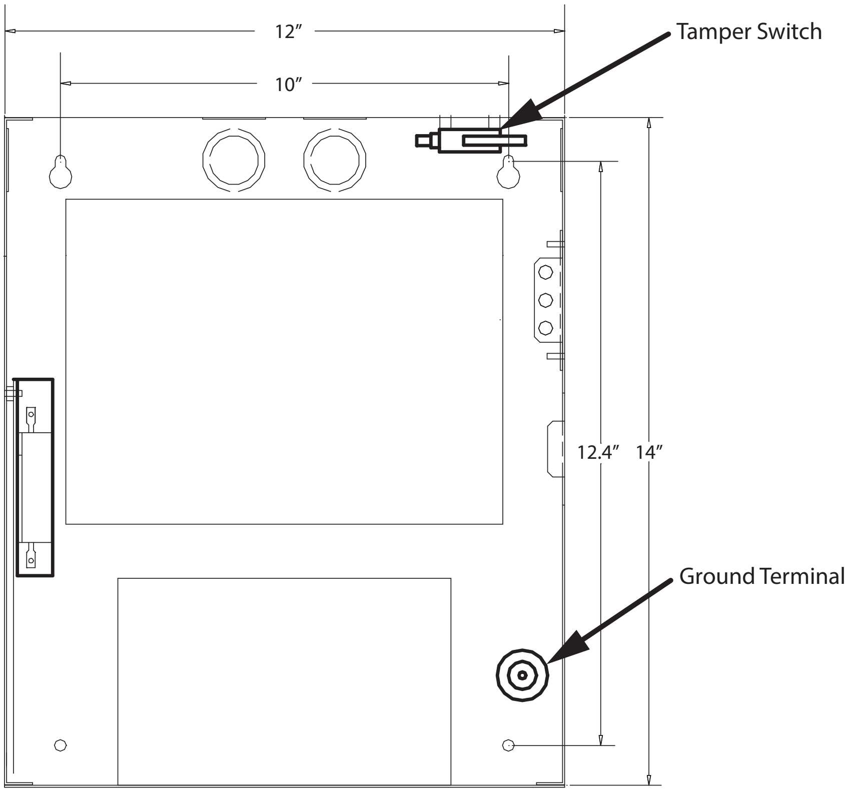


Figure 5. Controller Back Cover Dimensions and Optional Component Location

2.2.1 Additional Components

Install the following additional components as required:

- Tamper switch
- TX3-IP IP Module
- Battery

2.2.2 Installing the Aperio Door Controller

The Aperio Door Controller enclosure mounts directly on the wall to the wall stud using the mounting screws locations as shown in Figure 5.

To mount the Aperio Door Controller

1. Find a suitable location for the enclosure beside a wall stud.
2. Using the controller back cover as a template, mark the top two mounting hole locations 10" apart as shown in Figure 5.
3. Place the screws halfway into the wall in the position shown using a suitable screw.
4. Hang the box onto the two screws.
5. Screw the other two screws at the bottom of the panel.
6. Tighten all four screws into place.

2.2.3 Installing the Tamper Switch

The tamper switch is located at the top right corner of the back cover shown in Figure 5. Connect the tamper switch wire to one of the general purpose input and then correlate the opening of the cover to a specific output (action). For a complete description of correlations, see section 3.8, Correlations, on page 85.

2.2.4 Installing the IP Module

Install the optional TX3-IP IP Module in the location shown in Figure 6. Secure the IP Module into the location using the supplied four screws.

For additional documentation see the TX3-IP IP Module Installation Instructions LT-1161.

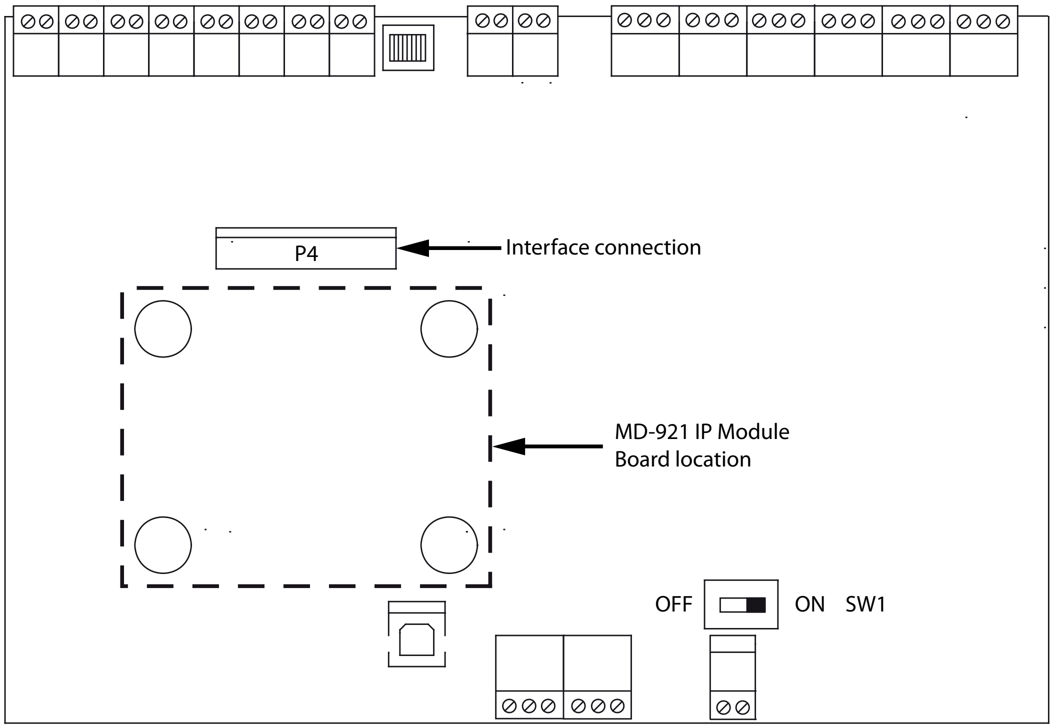


Figure 6. IP Module Board Location

2.3 Controller Board Description

The Aperio Door Controller controls access points according to how the inputs and outputs are defined and correlated with each other. Inputs and outputs are defined by how the access and control points are wired with the controller.

Before you begin you must establish how you want the outputs to behave as a function of the inputs. For a complete description of correlation and the modes of operation see section 3.8, Correlations, on page 85.

Keep a record of the wiring for configuration purposes.

2.3.1 Controller Panel LEDs

There are three status LEDs on the front of the Aperio Door Controller:

AC ON LED. `AC ON LED` illuminates steady green when AC power is present.

Trouble LED. `Trouble LED` flashes amber at a slow rate when there is a common trouble condition in the system. Trouble consists of:

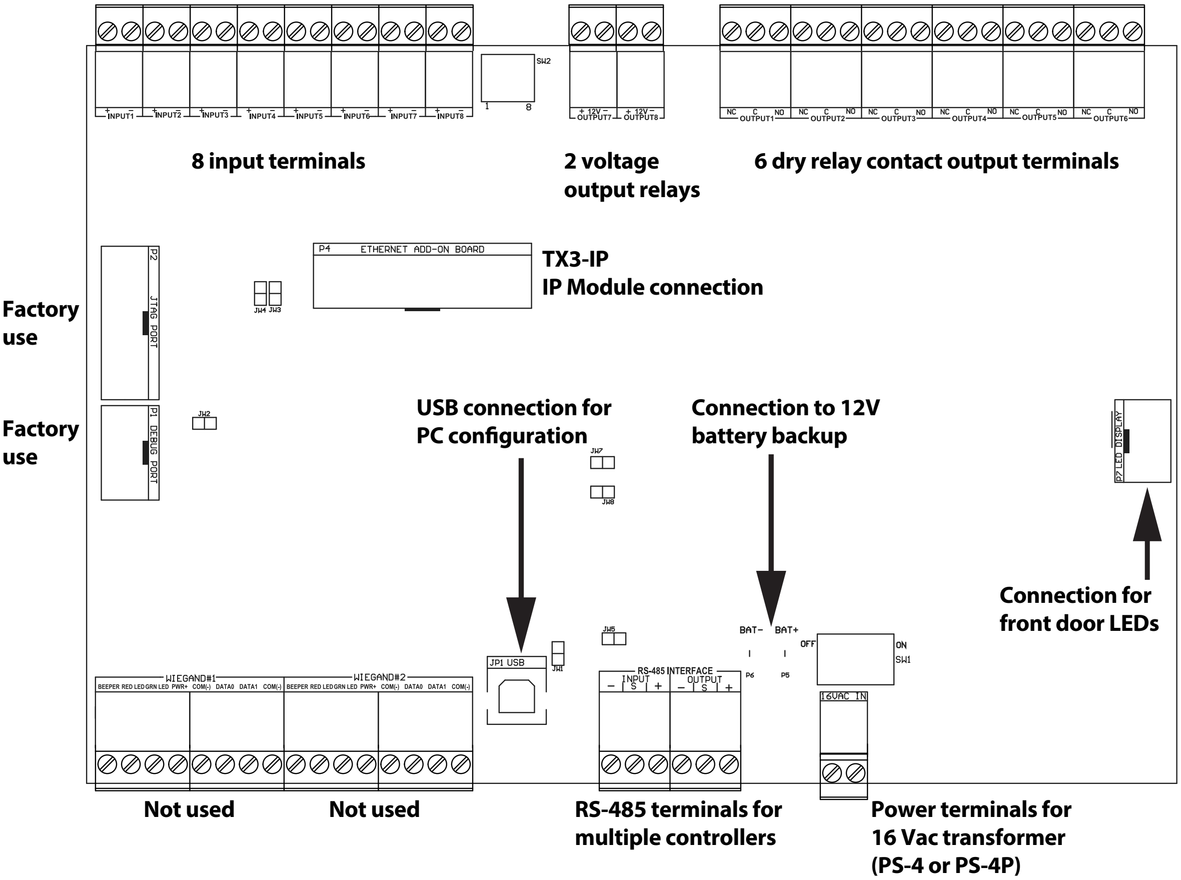
- any supervised input
- AC power/low battery
- door held open warning

Alarm LED. `Alarm LED` flashes red at a fast flash rate when there is a forced entry or the door held open alarm timer expires.

2.3.2 Controller Board Components

The Aperio Door Controller consists of the following terminals:

- 8 inputs
- 8 outputs (6 relay contact outputs and 2 outputs providing 12 Vdc)
- power supply
- RS-485 connector
- USB, IP Module, and Modem board connectors



8 input terminals

2 voltage output relays

6 dry relay contact output terminals

Factory use

TX3-IP IP Module connection

Factory use

USB connection for PC configuration

Connection to 12V battery backup

Connection for front door LEDs

Not used

Not used

RS-485 terminals for multiple controllers

Power terminals for 16 Vac transformer (PS-4 or PS-4P)

Figure 7. Controller Board Connection Locations

2.3.3 Power Supply

The power supply connection is situated at the bottom right of the main controller board and receives 16 VAC, 40 VA. Use 18 AWG wiring. An external PS-4 or PS-4P plug-in transformer connects to the power terminals. Refer to Figure 5 and Figure 8.

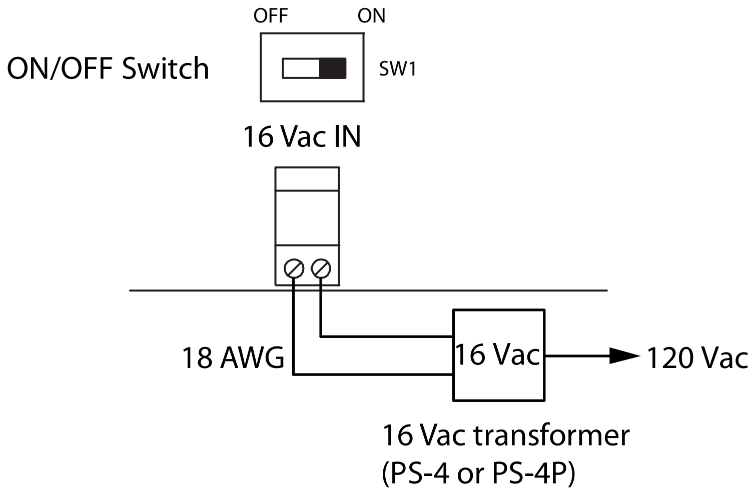


Figure 8. Power Supply

2.3.4 ON/OFF Switch and Battery Back-up

Battery back-up is provided with a 12V 6.5AH battery which fits inside and at the bottom of the unit. Connect the battery to the connectors located to the left of the ON/OFF switch SW1 as shown in Figure 9.

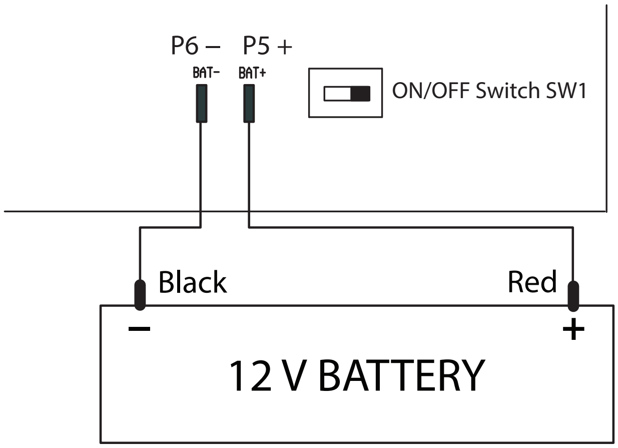


Figure 9. Controller Board Battery Wiring

Note: Battery backup is optional.

2.3.5 The Controller Board RS-485 Terminal

Note: The RS-485 network described in this section is for networking TX3 controllers only. Information on how to connect Aperio hubs to the MD-1113 Module board's RS-485 network terminal can be found in section 2.6, Installing and Configuring Aperio Hubs, on page 30.

An RS-485 terminal lets you easily connect multiple Telephone and Card Access Controllers across a network. The RS-485 connection is situated at the bottom middle of the main controller board and consists of two separate terminals, each for an input and output.

Connect the RS-485 input terminal to the RS-485 output terminal of another controller. See figure 10 for RS-485 wiring between panels.

On boards with the model number MD-10xx, you can close JW5 on the first and last panels instead of using end-of-line 120 Ω resistors.

If there are problems with RS-485 communication, close both JW7 and JW8 on either the first or last controller connected by RS-485.

Note: Use twisted shielded pair.

Recommended cables:

- RS485 cables
  - Belden 3109A RS-485, (4 pr) 22 AWG (7x30) or equivalent
  - Belden 9842 RS-485, (2 pr) 24 AWG (7x32) or equivalent
  - Belden 9841 RS-485, (1 pr) 24 AWG (7x32) or equivalent
- CAT5 Cables
  - Belden 72001E ETHERNET Cat 5e 2 Pair, 24 AWG or equivalent
  - Belden 70006E Cat 5e, 100Mb/s, Quad, AWG 22 (1) or equivalent

Maximum total length:

- 4000 feet (1244 m) for 22 AWG
- 2500 feet (762.5 m) for 24 AWG

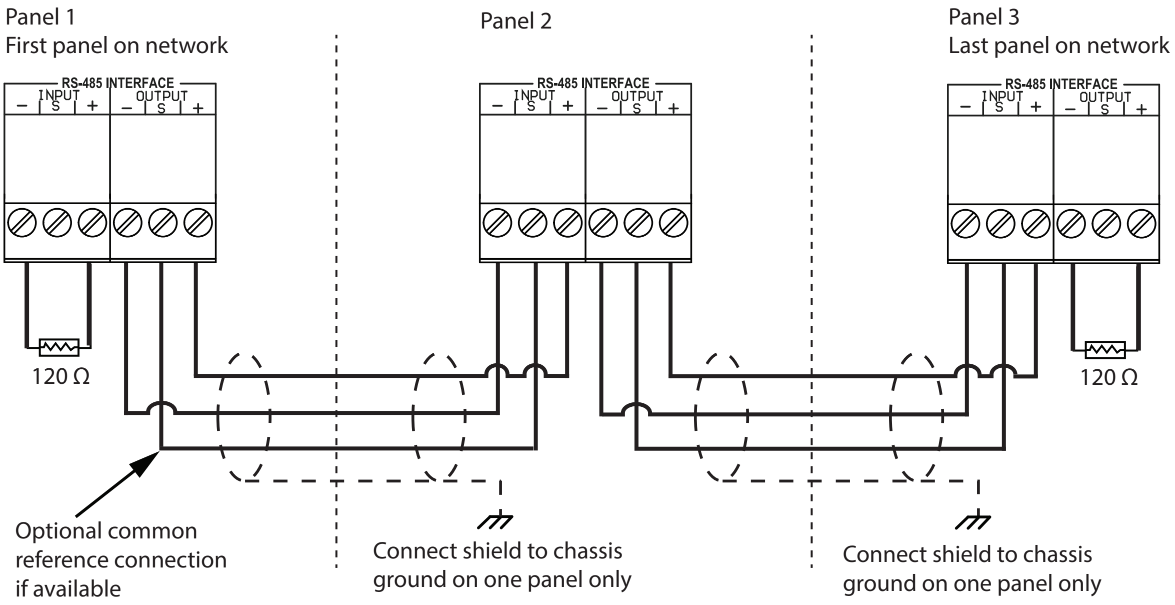

Panel 1
First panel on network
Panel 2
Panel 3
Last panel on network
RS-485 INTERFACE
INPUT
OUTPUT
– S +
120 Ω
Optional common reference connection if available
Connect shield to chassis ground on one panel only
Connect shield to chassis ground on one panel only

Figure 10. Inter-Panel RS-485 Wiring

2.3.6 USB Port

The USB port provides a connection to a PC, for configuring the Aperio Door Controller and downloading any new firmware.

2.4 Connecting the Inputs

Each Aperio Door Controller has eight general purpose inputs to accommodate the different types of configurable functions associated with the inputs. For additional details and a complete description of the different types of configurable functions see section 3.6, Aperio Door Controller Inputs, on page 81.

After the installation and setup is complete, the functional state of all inputs and circuit supervision types must be configured using the TX3 Configurator software. During configuration you can also establish correlations between inputs and outputs.

Each input is configured according to:

- active state
- supervision requirement

- alarm delay

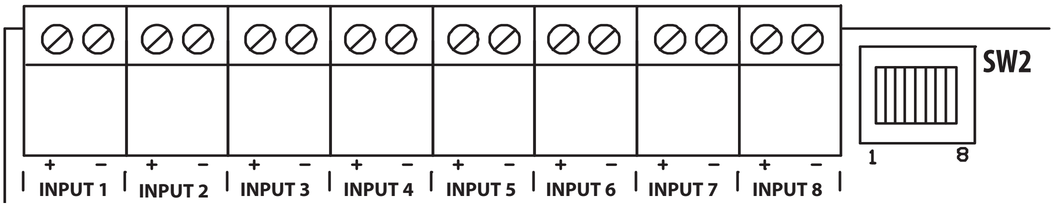


Figure 11. Controller Board Input Terminals

2.4.1 Inputs 1 to 8

Inputs 1 to 8 are programmable general purpose inputs. A general purpose input is mainly used for establishing a correlation with a specific output. When a general purpose input becomes active it is considered as an event that correlates to either turn on or off a general purpose output, or to turn on or off the high security mode. Other correlated events include different functions such as forced entry and door held open. Figure 12 shows an example with switches connected to three of the general purpose input terminals.

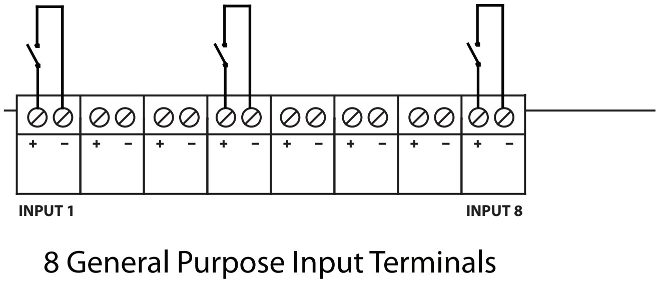


Figure 12. Input Terminal Sample Connections

2.4.2 Active State

An active state is when the input circuit is considered active and is configured as one of the following:

- Open
- Close (default)

There are some restrictions in configuring the active state depending on what kind of supervision is required.

If the input is not supervised, the input is either ‘open’ or ‘closed’. If the input is supervised for ‘open’, the active state cannot be ‘open’.

If the input is supervised for both ‘open’ and ‘short’, the active state cannot be ‘open’.

2.4.3 Supervision Requirement

Each input is configured for a specific type of supervision depending on your particular installation requirements as follows:

- None
- Open circuit
- Short circuit
- Open and short circuit

2.4.3.1 None

When inputs are configured with no supervision, the active state is either 'Open' or 'Close' as programmed.

2.4.3.2 Open circuit

When configured as supervised for an open circuit, the active state is 'closed' (short). Open supervision uses a single 47K ohm resistor.

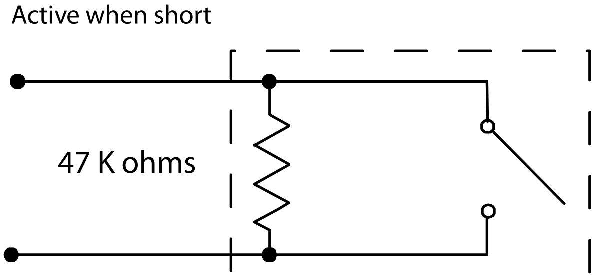


Figure 13. Input - Supervised for Open

Note: The active state cannot be an open state.

2.4.3.3 Short circuit

When configured as supervised for a short circuit, the active state is open. A single 47K ohm resistor is required for short supervision.

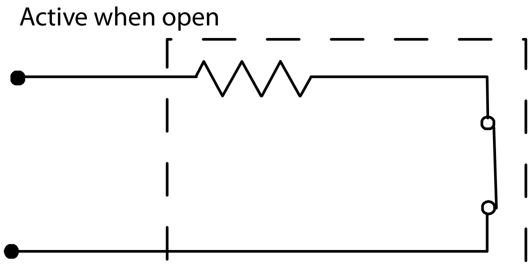


Figure 14. Input - Supervised for Short

Note: The active state cannot be a short state.

2.4.3.4 Supervise for open and short

When configured as supervise for both ‘open’ and ‘short’, the active state cannot be open, therefore the active state is closed.

Two 22K ohm resistors are required for supervision.

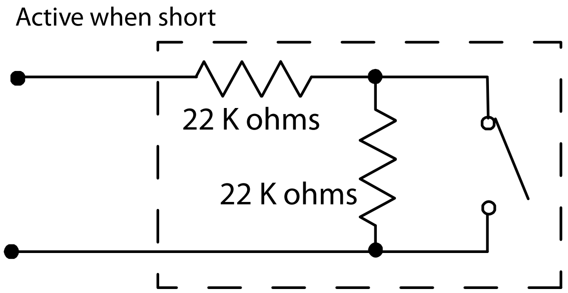


Figure 15. Input - Supervised for Open and Short

Note: The active state cannot be an open state.

2.4.4 Alarm Delay

Alarm delay is a TX3 Configurator defined parameter that specifies the amount of time before an input raises an alarm condition. For more information see section 3.6, Aperio Door Controller Inputs, on page 81.

2.5 Connecting the Outputs

There are 8 general purpose outputs located on the top right hand corner of the Aperio Door Controller as shown in Figure 7.

Each output is wired for a specific function or for an active state. Determine the functional requirements for the device and connect the outputs accordingly. For additional details and a complete description of the different types of configurable functions, see section 3.7, Aperio Door Controller Outputs, on page 83.

After the installation and setup is complete, the functional state of all outputs must be configured using the TX3 Configurator software.

2.5.1 Active State

Outputs require active states. Each output is configured for the active state to indicate one of the following:

- Energized
- De-energized

2.5.2 Outputs 1 to 6

Outputs 1 to 6 are relay contact programmable outputs with the following characteristics. Figure 16 shows a sample connection.

- normally open (NO)
- normally closed (NC) available
- 125 VAC / 2 A
- 30 VDC / 1 A

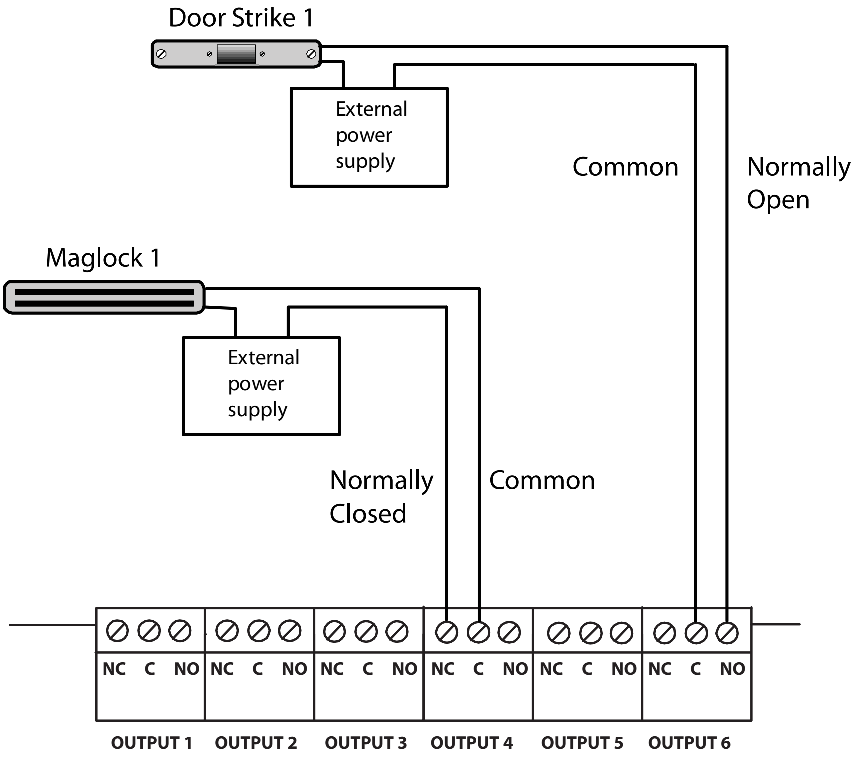


Figure 16. Controller Output Terminal Sample Connections

2.5.3 Outputs 7 and 8

Outputs 7 and 8 are programmable and provide a combined output of 1 A. Each individual output is capable of providing:

- 12 VDC
- 500 mA of current (700 mA maximum)

Note: Outputs 7 and 8 are capable of providing a maximum output of 700 mA each, for a combined output of 1 A. For example, if output 7 provides 700 mA, then output 8 provides 300 mA.

You can power Aperio hubs from outputs 7 and 8. See Powering the Aperio hubs on page 36 for information on connecting power to Aperio hubs.

By default, Outputs 7 and 8 are set to `De-energized` in the Configurator. If you are using Outputs 7 and 8 to power hubs, do not change this setting.

Note: If you use one or both of Outputs 7 and 8 to power your Aperio hubs, do not use these outputs in your correlations (see section 3.8, Correlations, on page 85).

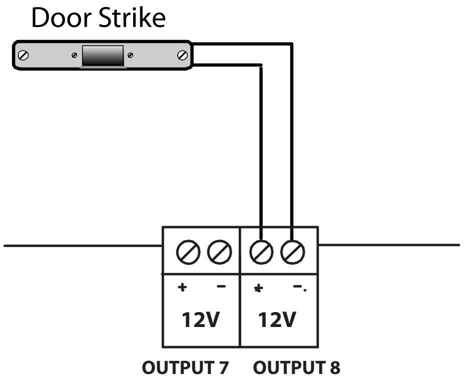


Figure 17. Outputs 7 and 8 Sample Connections

Figure 17 shows a door strike activated and powered by output 8.

2.6 Installing and Configuring Aperio Hubs

Each TX3-CX-A8 Aperio Door Controller can by default support up to 8 devices (16 devices with firmware version 3.2.2 and higher) and a maximum of 15 Aperio hubs. Each Aperio hub can support up to 8 devices.

This section covers the following topics.

- Choosing Installation Locations
- Configuring the Aperio Hubs
- Installing and Pairing Wireless Devices
- Wireless Device Status LEDs

2.6.1 Choosing Installation Locations

When choosing locations to install your TX3-CX-A8 Aperio Door Controllers, Aperio hubs, and wireless devices, the following conditions **MUST** be met (see Figure 18).

A. The length of the RS-485 bus connecting the Aperio Door Controller and the Aperio hubs must be less than 3000 feet.

B. The distance between any two Aperio hubs must be at least 1 foot.

C. The distance between an Aperio hub and any of its associated devices must be between 10 feet and 45 feet in ideal conditions (that is, little to no wireless interference); under less than ideal conditions, the maximum distance should be reduced to 15 feet.

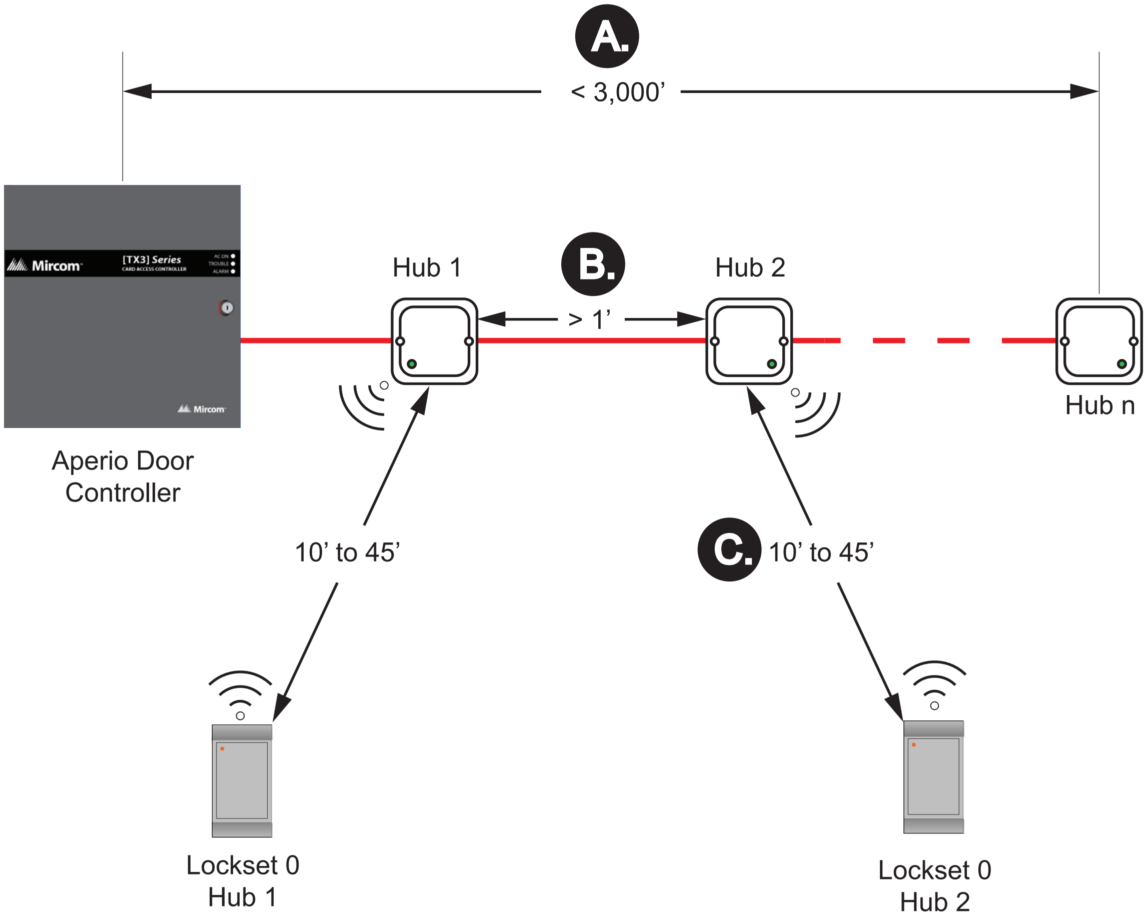


Figure 18. Distance limitations when installing the TX3-CX-A8 Aperio Door Controller System

In addition to these requirements, the following best practices should be taken into consideration.

- The LED on the Aperio hub should point to the wireless devices it is going to be paired with.
- The Aperio hub should be placed on the same side as the key hole or card reader of the wireless device. Thinner walls and shorter distances between the hub and the device may permit placement on opposite sides.
- Metallic sheet or mesh in the ceiling or walls weakens the wireless signal between the hub and wireless devices.

- The Aperio hubs and wireless devices should be installed at least 1 foot away from mirrors and large metallic surfaces (for example, cable ladders).
- The Aperio hubs and wireless devices should be kept at least 13 feet away from WiFi/WLAN routers, radio transmitters, and other sources of electromagnetic interference (for example, microwave ovens, electric motors, and other high power electrical equipment).
- It is recommended that you verify the radio link quality using the Aperio Programming Application (APA).

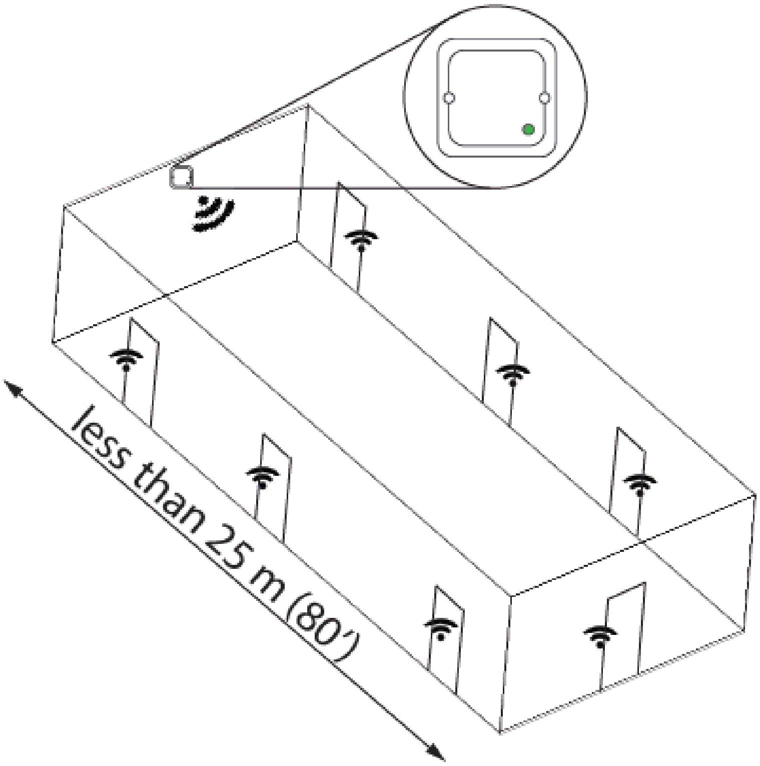


Figure 19. The hub should be on the same side of the wall as the devices, and facing them

2.6.2 Configuring the Aperio Hubs

Before installing the Aperio hubs, you must configure the hubs to communicate with the Aperio Door Controller. This section contains instructions on how to perform the following tasks.

1. Setting the Aperio hub address
2. Connecting the TX3-CX-A8 to the Aperio hubs
3. Powering the Aperio hubs

To perform these actions, you need to access DIP switch S101 and connector J100 on the back of the Aperio hubs (see Figure 20). S101 configures the RS-485 network settings for the Aperio hub. J100 connects the Aperio hub to the RS-485 network and to power.

Figure 20 shows the terminals on a 1 to 8 hub. The 1 to 1 hub looks different, but the terminal labels are the same.

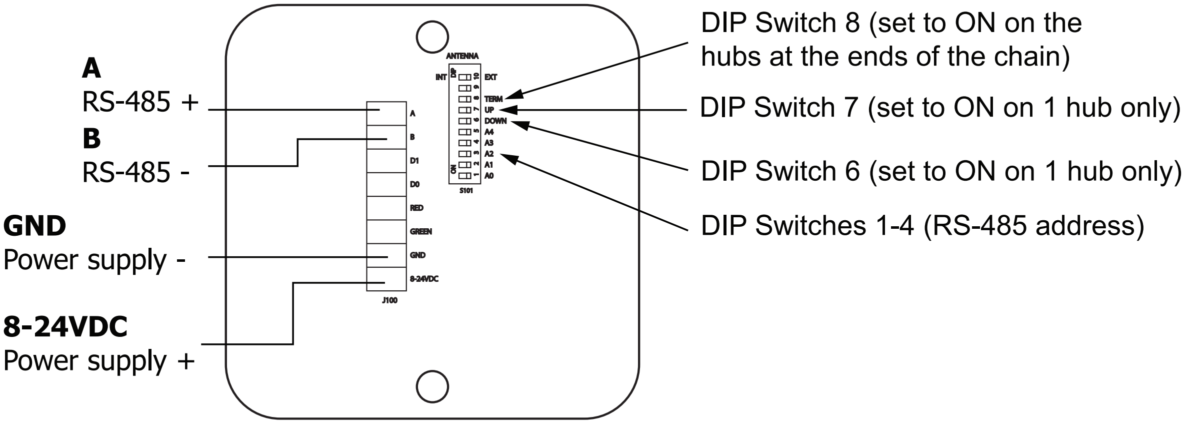

A
RS-485 +
B
RS-485 -
GND
Power supply -
8-24VDC
Power supply +
ANTENNA
INT
DIP
ON
1
2
3
4
5
6
7
8
9
10
EXT
TERM
UP
DOWN
A4
A3
A2
A1
A0
S101
A
B
D1
D0
RED
GREEN
GND
8-24VDC
J100
DIP Switch 8 (set to ON on the hubs at the ends of the chain)
DIP Switch 7 (set to ON on 1 hub only)
DIP Switch 6 (set to ON on 1 hub only)
DIP Switches 1-4 (RS-485 address)

Figure 20.   Terminals on a 1 to 8 Aperio hub

2.6.2.1 Setting the Aperio hub address

Each Aperio hub must have a unique RS-485 network address. Use DIP switches 1-4 on S101 (see Figure 20) to set the RS-485 network address for each of your Aperio hubs. Valid addresses range from 1 to 15.

Refer to Table 1 for information on how to set each DIP switch for a particular network address.

Table 1:   S101 DIP switch settings for Aperio hub RS-485 network addressing

Address	Switch 1 (A0)	Switch 2 (A1)	Switch 3 (A2)	Switch 4 (A3)
1	ON	OFF	OFF	OFF
2	OFF	ON	OFF	OFF
3	ON	ON	OFF	OFF
4	OFF	OFF	ON	OFF
5	ON	OFF	ON	OFF
6	OFF	ON	ON	OFF
7	ON	ON	ON	OFF
8	OFF	OFF	OFF	ON

Table 1: S101 DIP switch settings for Aperio hub RS-485 network addressing (Continued)

Address	Switch 1 (A0)	Switch 2 (A1)	Switch 3 (A2)	Switch 4 (A3)
9	ON	OFF	OFF	ON
10	OFF	ON	OFF	ON
11	ON	ON	OFF	ON
12	OFF	OFF	ON	ON
13	ON	OFF	ON	ON
14	OFF	ON	ON	ON
15	ON	ON	ON	ON

2.6.2.2 Connecting the TX3-CX-A8 to the Aperio hubs

The TX3-CX-A8 communicates with the Aperio hubs through an RS-485 network. The RS-485 signals are transmitted through terminals A and B of the J100 connector on the Aperio hubs (see Figure 20) and through the + and - terminals of the RS-485 connector on the MD-1113 Module board of the TX3-CX-A8.

Figures 21 and 22 show two examples of networks with three Aperio hubs. In Figure 21, there is an Aperio hub on one end of the network and the MD-1113 is on the other end of the network. Note that in this configuration, the Aperio hub at the end of the bus is terminated (DIP switch 8 is on) and that jumpers JW1 and JW2 on the MD-1113 are open.

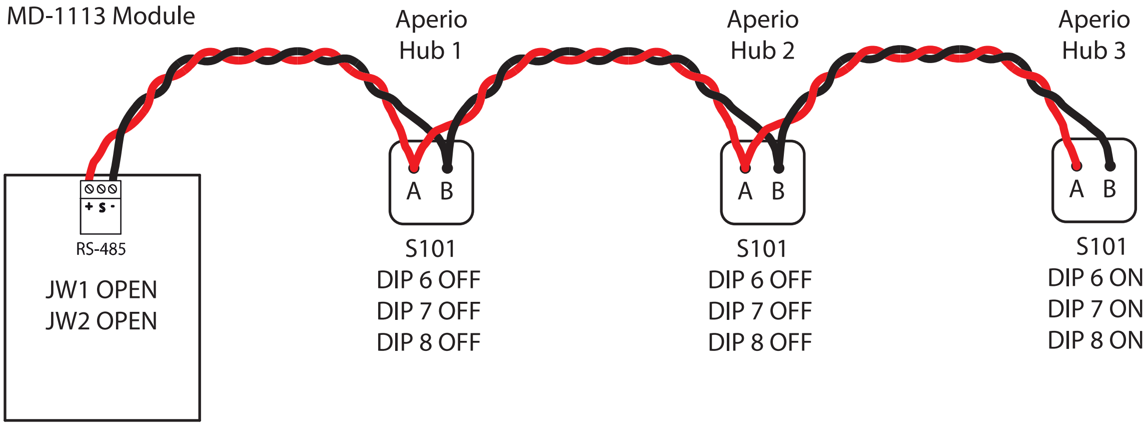


Figure 21. A network with one end terminated by the MD-1113 and the other end terminated by an Aperio hub

In Figure 22, Aperio hubs are on both ends of the network. Note that the Aperio hubs on the ends are terminated (DIP switch 8 is on) and that jumpers JW1 and JW2 on the MD-1113 Module board are open.

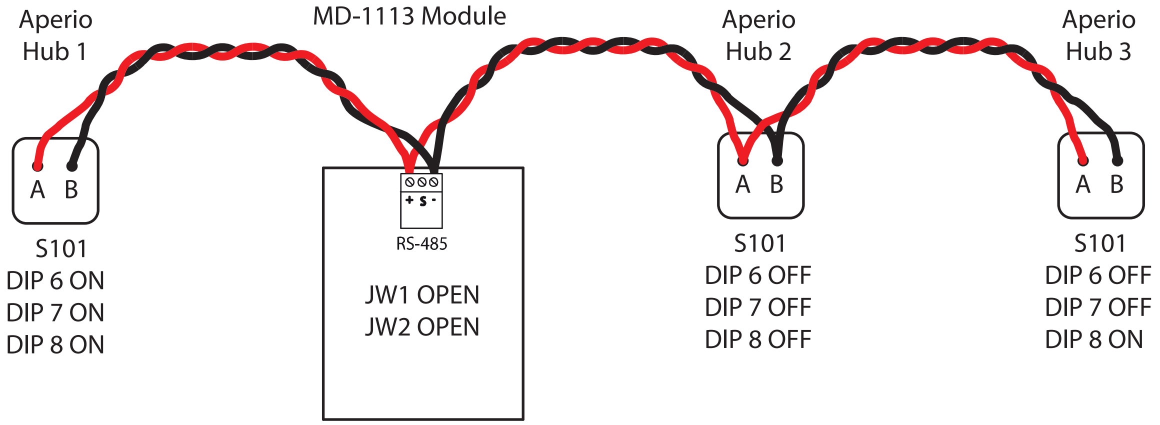


Figure 22. A network with both ends terminated by Aperio hubs

The following guidelines must be followed when networking the Aperio hubs with the TX3-CX-A8.

A. Each Aperio hub must have a unique RS-485 network address. Set the address using DIP switches A0-A3 on S101. See “Setting the Aperio hub address” on page 33.

B. The RS-485 bus for the Aperio hubs must connect to the RS-485 connector on MD-1113 Module board.

C. The Aperio hubs must be connected in a daisy chain configuration (see Figures 21 and 22).

D. When connecting an Aperio hub to the MD-1113 Module board:

- connect the A terminal on the J100 connector of the hub to the positive (+) terminal of the RS-485 connector on the MD-1113;
- connect the B terminal on the J100 connector of the hub to the negative (-) terminal of the RS-485 connector on MD-1113.

E. When connecting two Aperio hubs together:

- connect the A terminal on the first hub to the A terminal on the second hub;
- connect the B terminal on the first hub to the B terminal on the second hub.

F. Aperio hubs located on the ends of the RS-485 network must be terminated. To terminate an Aperio hub, set DIP switch 8 (TERM) on S101 to ON (see Figures 21 and 22).

G. One of the Aperio hubs must have DIP switches 6 (DOWN) and 7 (UP) set to ON (see Figures 21 and 22).

H. Jumpers JW1 and JW2 on the MD-1113 are open. This is the factory default setting.

2.6.2.3 Powering the Aperio hubs

The power requirements for the Aperio hubs are as follows.

- 8-24 VDC
- 250 mA

To power the Aperio hub, connect the positive voltage output of your power supply to the `8-24VDC` terminal on the J100 connector and the ground of your power supply to the `GND` port of the J100 connector (see Figure 20).

See section 2.5.3 on page 29 for information about powering the Aperio hubs from outputs 7 and 8.

Note: If you use one or both of Outputs 7 and 8 to power your Aperio hubs, do not use these outputs in your correlations (see section 3.8, Correlations, on page 85).

2.6.2.4 Installing the Aperio hub

This section describes how to install the Aperio hub on the following standard assemblies:

- Switch box assembly
- Square box assembly
- Octagon box assembly
- Handy box assembly

In addition to the Aperio hub, you will need a mounting plate and a plaster ring (for square box assemblies). See Figure 23.

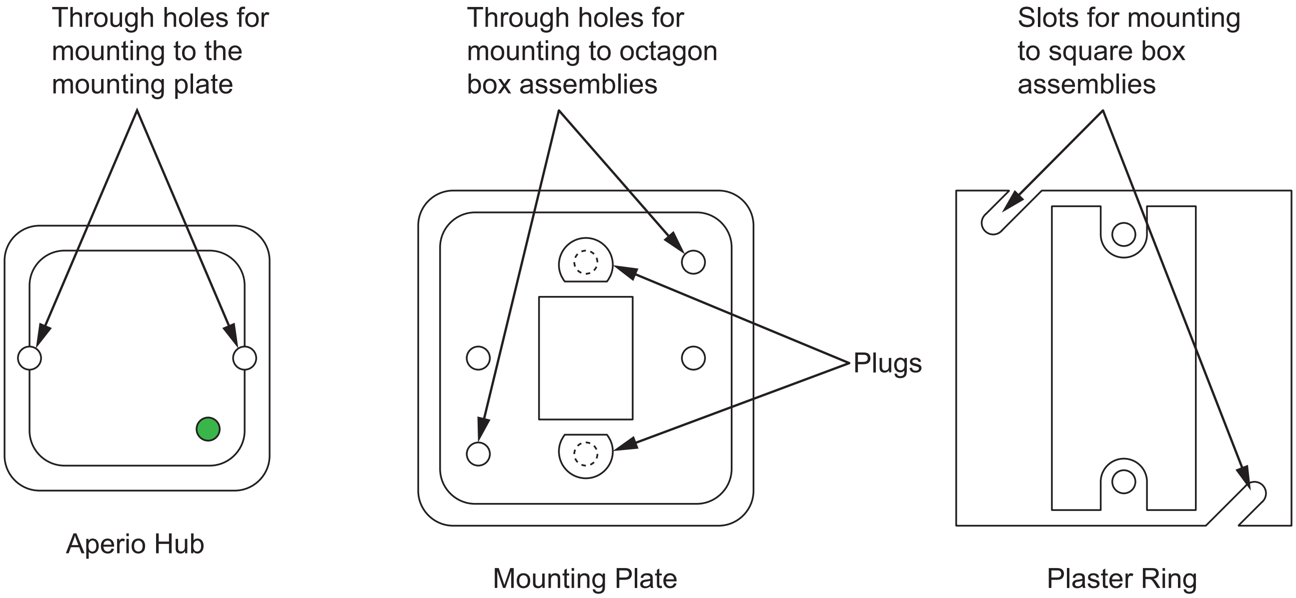

Through holes for mounting to the mounting plate
Through holes for mounting to octagon box assemblies
Slots for mounting to square box assemblies
Plugs
Aperio Hub
Mounting Plate
Plaster Ring

Figure 23. The Aperio hub along with the mounting plate and plaster ring used for installing the Aperio hub on standard box assemblies

Note: Configure the Aperio hub, including all DIP switch settings, network connections, and power connections, before installing it.

To install the Aperio hub

1. Remove the plugs from the mounting plate (see Figure 23).
2. Secure the mounting plate to the box assembly with two screws.

Note: If you are installing onto a square box assembly, first secure the plaster ring to the assembly using two screws (see Figure 23), and then secure the mounting plate to the plaster ring.

3. Place the plugs over the through holes of the mounting plate.
4. Secure the Aperio hub to the mounting plate using two screws.

2.6.2.5 Aperio hub status LEDs

Each Aperio hub has a single LED that indicates the status of the hub. Refer to Table 2 for the different LED indications and their associated device status.

Table 2: Aperio hub LED status indications

LED Indication	Description	Aperio Hub Status
🟩	Green	Online.
🟥🟩	Green with one red flash	Aperio lock is offline.
🟥🟩🟥🟩	Green with two red flashes	Aperio Door Controller is offline.
🟥🟩🟥🟩🟥🟩	Green with three red flashes	Aperio lock and Aperio Door Controller are offline.
🟨 🟨 🟨 🟨 🟨 🟨 🟨 🟨 🟨 🟨 🟨	Fast flashing yellow	UHF communication.
🟨	Yellow	Pairing active.

2.7 Installing and Pairing Wireless Devices

After installing the Aperio Door Controllers and Aperio hubs, you can install the wireless devices, and then associate each device with an Aperio hub. The process of associating a wireless device with its Aperio hub is called pairing.

2.7.1 Installing a Wireless Device

Refer to the Installation Instructions for your wireless device.

2.7.2 Pairing a Wireless Device to an Aperio Hub

Each device must be paired with a hub using the Aperio Programming Application. Pairing establishes a secure radio communication link between the wireless device and the Aperio hub. If pairing is not properly performed, the device will either not be able to communicate with the hub or the radio communication link between the device and hub will be insecure, jeopardizing the security or your devices.

This section covers the basic procedure for pairing a wireless device with an Aperio hub. The first step is to create a new installation database for your site using the site's Encryption Key file. The second step is to scan for the Aperio hubs in your installation and then pair each device to a hub.

To pair a device with an Aperio hub, you need the following:

- A Tritech TriBEE USB Radio dongle.
- A computer with the drivers for the Tritech TriBEE USB Radio dongle and the Aperio Programming Application installed.
- The Encryption Key file for your installation.
- At least one access card.

If you do not have all of these items, contact Mircom Technical Support. See Contact Us on page 16 for the contact information.

To create a new installation database

1. Insert the Tritech TriBEE USB Radio dongle in your computer, and then start the Aperio Programming Application.
2. If you are prompted to select an installation or to enter an installation name, click `Cancel`.
3. Click `File > New`.
4. In the `Installation name` text box, enter the name for your installation.
5. Click the `Select key file` button (...) in the `Key file` area.
6. In the `Select key file` window, browse to the location of the Encryption Key file for your installation, select it, and then click `Open`.
7. Click `Create new`.
8. In the `Enter Password` window, enter a valid password for the installation database, confirm the password, and then click `OK`.
9. Click `Cancel` to close the communication hub selection window.
10. Close the Aperio Programming Application.

The next time you start the Aperio Programming Application, the new installation will appear in the list of installations. The installation database contains the information stored in the Encryption Key file and is used to establish a secure radio communication link between the wireless devices and the Aperio hubs. At this point the Encryption Key file is no longer needed and should be deleted.

Note: The Encryption Key file should be treated with the same care as the Master Key in a traditional door security system. Someone with access to the Encryption Key file can gain unauthorized access to any door in the system. Once the installation database for your site has been created, the Encryption Key file should be erased from the hard drive. A copy of the Encryption Key file should be stored in a secure location.

Once you have created the installation database for your site, you can start pairing wireless devices to Aperio hubs. Each device can be paired to only one hub, but each hub can have up to eight devices paired to it.

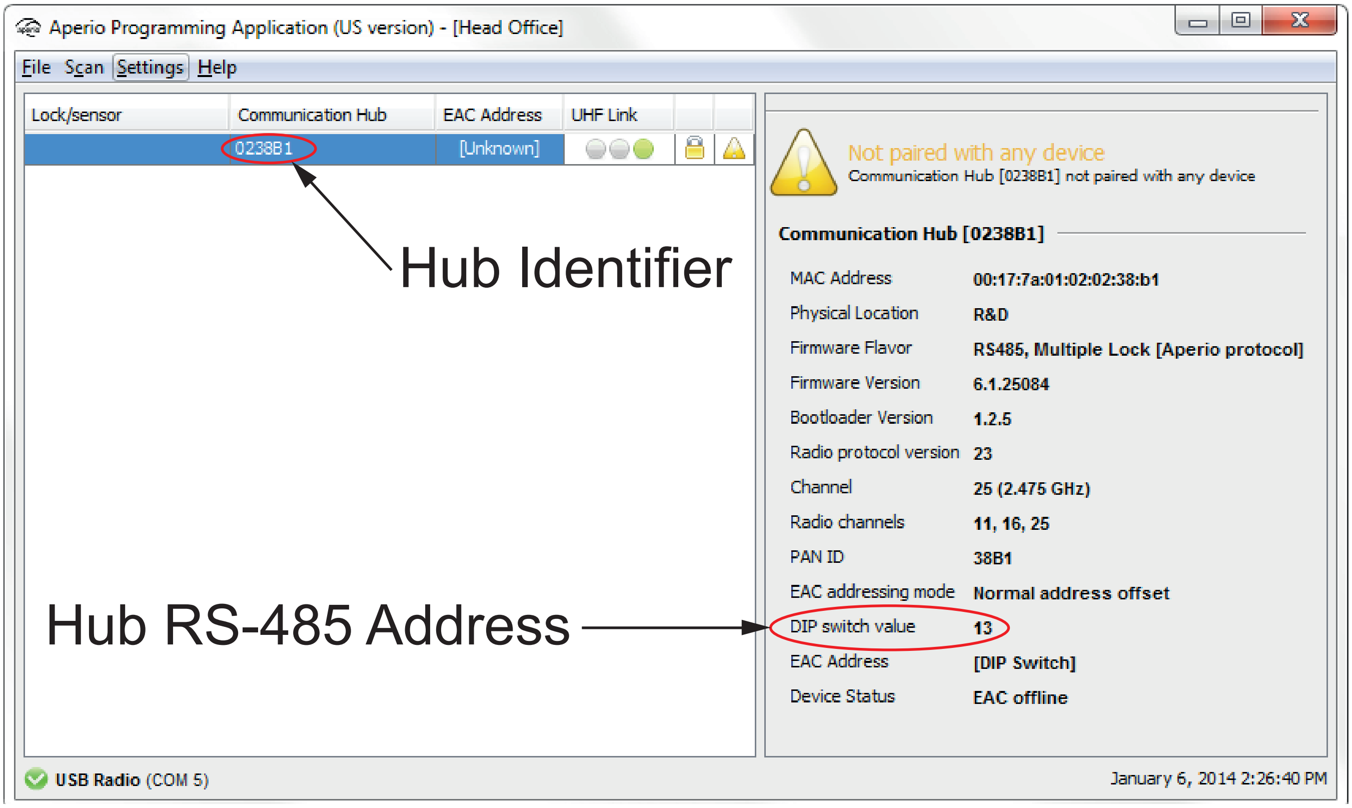
To pair a wireless device with a hub

1. Start the Aperio Programming Application.
2. Select your installation, and then click `Open`.
3. Enter the password for your installation, and then click `OK`.
4. In the communication hub selection window, select the hub(s) that you want to pair your device(s) to, and then click `Show details`.

Notes:

- The values in the in the `Communication Hub` column are the last four digits of the Aperio hub's MAC address. The MAC address for each hub is printed on a label attached to the side of the Aperio hub.
- If your hub is not listed in the communication hub selection window, click `Rescan`.

The Aperio Programming Applications details page appears with information about your hubs. The `DIP switch value` setting tells you the RS-485 address for your hub



Lock/sensor	Communication Hub	EAC Address	UHF Link
	0238B1	[Unknown]	

Not paired with any device
Communication Hub [0238B1] not paired with any device

Communication Hub [0238B1]

MAC Address	00:17:7a:01:02:02:38:b1
Physical Location	R&D
Firmware Flavor	RS485, Multiple Lock [Aperio protocol]
Firmware Version	6.1.25084
Bootloader Version	1.2.5
Radio protocol version	23
Channel	25 (2.475 GHz)
Radio channels	11, 16, 25
PAN ID	38B1
EAC addressing mode	Normal address offset
DIP switch value	13
EAC Address	[DIP Switch]
Device Status	EAC offline

USB Radio (COM 5)
January 6, 2014 2:26:40 PM

Figure 24. The communications hub details page in the Aperio Programming Application

5. Right-click the hub you want to pair the device to, and then select `Communication hub > Pair with lock or sensor`.

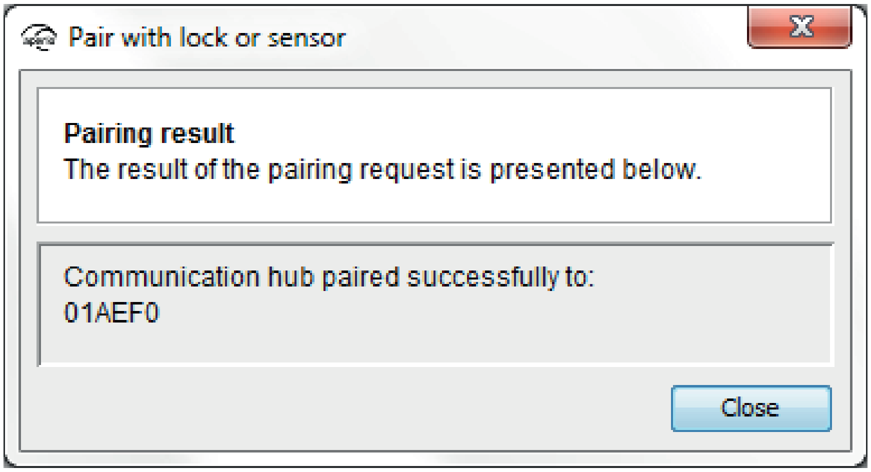
   The `Pair with lock or sensor` window appears.

6. Swipe an access card at the device.

   The red LED on the device blinks three times. Proceed to the next step when the LED stops blinking.

7. Click `Done` in the `Pair with lock or sensor` window.

The Aperio Programming Application pairs the device with the hub. If the pairing is successful, the following window appears.



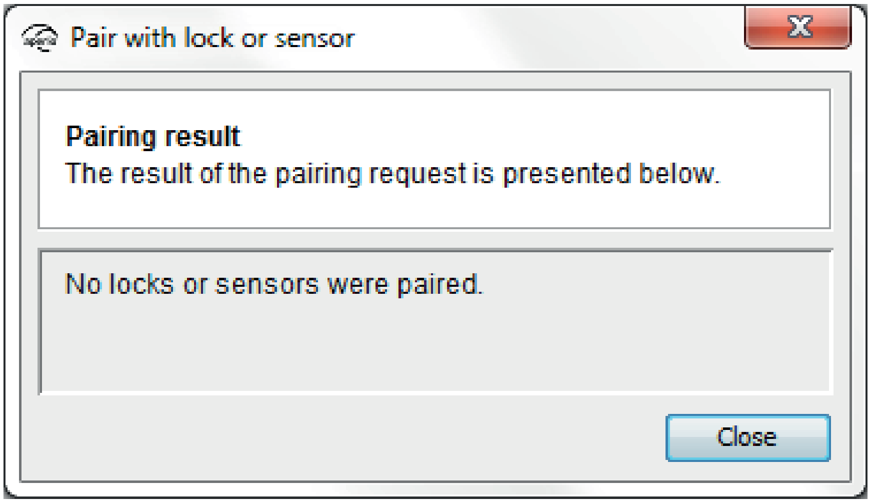
Pairing result
The result of the pairing request is presented below.

Communication hub paired successfully to:
01AEF0

Figure 25. Communication hub paired successfully

The values shown in the window are the last six digits of the device’s MAC address.

If the pairing is unsuccessful, the following window appears.



Pairing result
The result of the pairing request is presented below.

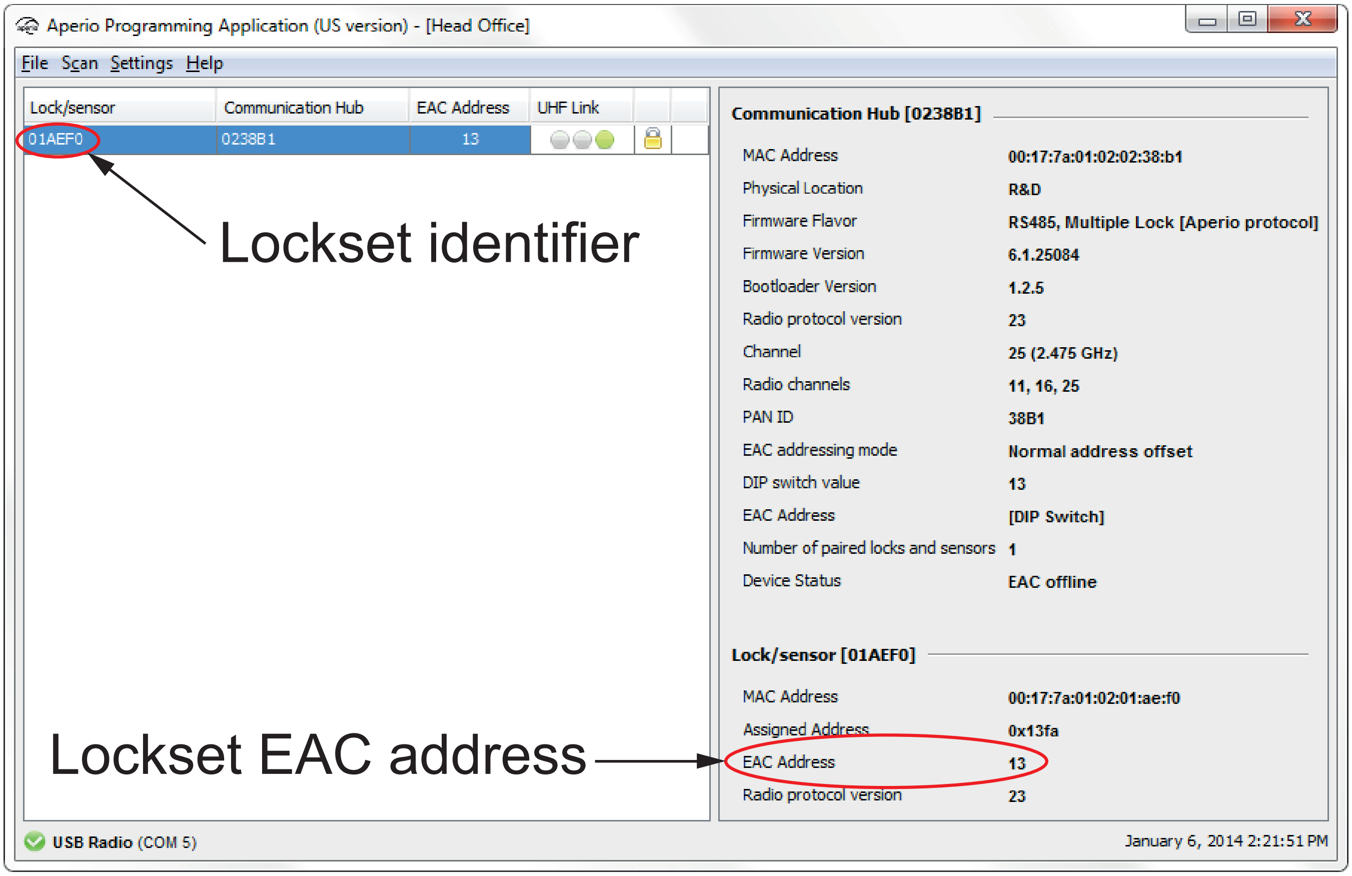
No locks or sensors were paired.

Figure 26. No locks or sensors were paired

To try pairing the device again, click `Close` and then repeat steps 5 to 7 until the pairing is successful.

8. Click `Close`, and then select the device that you just paired in the Aperio Programming Application Window.

The Aperio Programming Application displays the device details below the hub details.



Lock/sensor	Communication Hub	EAC Address	UHF Link
01AEF0	0238B1	13	○○● 🔒

Lockset identifier

Communication Hub [0238B1]

MAC Address	00:17:7a:01:02:02:38:b1
Physical Location	R&D
Firmware Flavor	RS485, Multiple Lock [Aperio protocol]
Firmware Version	6.1.25084
Bootloader Version	1.2.5
Radio protocol version	23
Channel	25 (2.475 GHz)
Radio channels	11, 16, 25
PAN ID	38B1
EAC addressing mode	Normal address offset
DIP switch value	13
EAC Address	[DIP Switch]
Number of paired locks and sensors	1
Device Status	EAC offline

Lock/sensor [01AEF0]

MAC Address	00:17:7a:01:02:01:ae:f0
Assigned Address	0x13fa
EAC Address	13
Radio protocol version	23

Lockset EAC address

USB Radio (COM 5) January 6, 2014 2:21:51 PM

Figure 27. Device details information

In particular, the device details information includes the EAC address for the device. The EAC address is a unique number that is assigned to each device and ranges from 1 to 127. This number is used to find the hub address and device address for each device in your job.

9. Use tables 3 and 4 in the following pages to determine the hub address and the device address for your device, and then label your device with its EAC address, hub address, and device address.

For example, in Figure 27 the EAC address for the device is 13. Using Table 3, we find that EAC address 13 translates to a **Hub address** of **13** and a **Device address** of **0**.

Note: It is critical that you label your device with the correct EAC address, hub address, and device address. If you do not do this, you will not be able to properly configure your device in the TX3 Configurator application.

10. Repeat steps 5 to 9 for all of the devices that you want to pair with your Aperio hubs.

When you have finished pairing all the locks in your installation, close the Aperio Programming Application.

Table 3: EAC address to Hub and Device address conversion table: 1 to 63

EAC Address	Hub Address	Device Address	EAC Address	Hub Address	Device Address	EAC Address	Hub Address	Device Address	EAC Address	Hub Address	Device Address
1	1	0	17	1	1	33	1	2	49	1	3
2	2	0	18	2	1	34	2	2	50	2	3
3	3	0	19	3	1	35	3	2	51	3	3
4	4	0	20	4	1	36	4	2	52	4	3
5	5	0	21	5	1	37	5	2	53	5	3
6	6	0	22	6	1	38	6	2	54	6	3
7	7	0	23	7	1	39	7	2	55	7	3
8	8	0	24	8	1	40	8	2	56	8	3
9	9	0	25	9	1	41	9	2	57	9	3
10	10	0	26	10	1	42	10	2	58	10	3
11	11	0	27	11	1	43	11	2	59	11	3
12	12	0	28	12	1	44	12	2	60	12	3
13	13	0	29	13	1	45	13	2	61	13	3
14	14	0	30	14	1	46	14	2	62	14	3
15	15	0	31	15	1	47	15	2	63	15	3

Table 4: EAC address to Hub and Device address conversion table: 65 to 127

EAC Address	Hub Address	Device Address	EAC Address	Hub Address	Device Address	EAC Address	Hub Address	Device Address	EAC Address	Hub Address	Device Address
65	1	4	81	1	5	97	1	6	113	1	7
66	2	4	82	2	5	98	2	6	114	2	7
67	3	4	83	3	5	99	3	6	115	3	7
68	4	4	84	4	5	100	4	6	116	4	7
69	5	4	85	5	5	101	5	6	117	5	7
70	6	4	86	6	5	102	6	6	118	6	7
71	7	4	87	7	5	103	7	6	119	7	7
72	8	4	88	8	5	104	8	6	120	8	7
73	9	4	89	9	5	105	9	6	121	9	7
74	10	4	90	10	5	106	10	6	122	10	7
75	11	4	91	11	5	107	11	6	123	11	7
76	12	4	92	12	5	108	12	6	124	12	7
77	13	4	93	13	5	109	13	6	125	13	7
78	14	4	94	14	5	110	14	6	126	14	7
79	15	4	95	15	5	111	15	6	127	15	7

2.7.3 Security Modes for Devices and Aperio Hubs

There are two security modes that the wireless devices and the Aperio hubs can use to communicate with each other: Manufacturer Mode and Customer Mode. Manufacturer Mode is an insecure radio communication that uses a default encryption key. Customer Mode is a secure radio communication that uses the customer Encryption Key file. After you have paired your wireless devices to their hubs, you must determine the security mode for each device and hub. If any of your hubs or devices are in Manufacturer Mode, switch them to Customer Mode.

Note: Leaving an installation in Manufacturer Mode compromises the security of your installation because anyone with the Aperio Programming Application and a Tritech TriBEE USB dongle could gain full access to your installation. It is highly recommended that you change your security mode to Customer Mode.

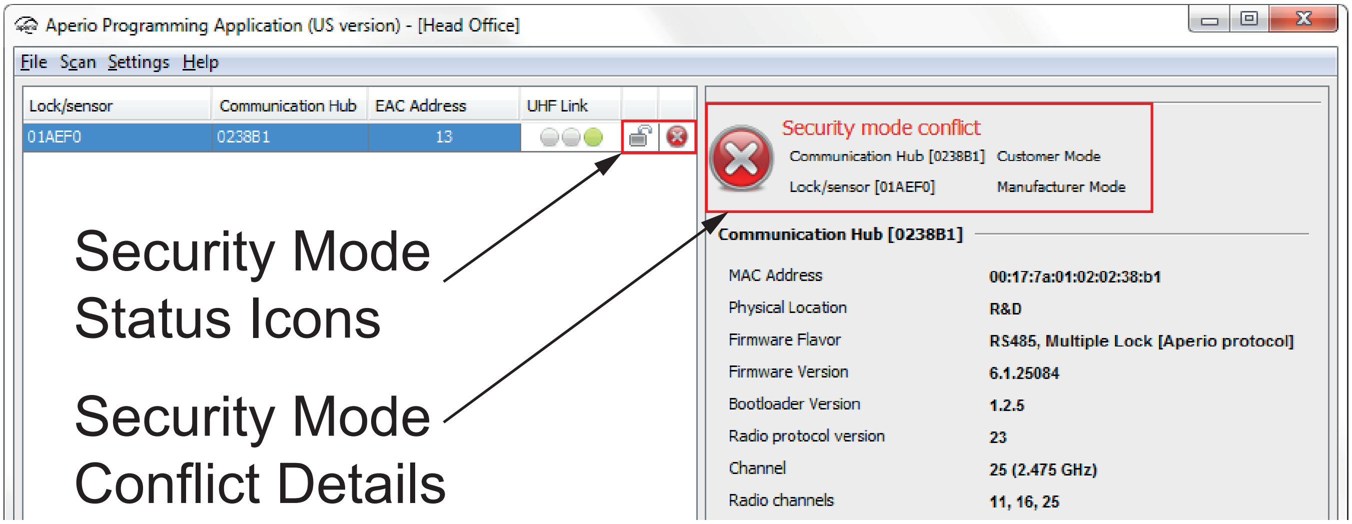
2.7.3.1 Determining the Security Modes for a Device-Hub Pair

Pairing a wireless device with an Aperio hub does not ensure secure communication between them. Secure communication is only established when both device and hub are communicating in Customer Mode. After you have paired a device with a hub, use the Aperio Programming Application to determine what security mode the device and hub are using.

To determine the security mode of a device-hub pair

1. Start the Aperio Programming Application.
2. Select your installation, and then click `Open`.
3. Enter the password for your installation, and then click `OK`.
4. In the communication hub selection window, select the hubs in your installation, and then click `Show details`.
5. Select a device-hub pair.

   The icons next to the UHF link icons indicate the security mode of the device-hub pair (see Figure 28). If there is a conflict in security mode settings between the device and the hub, information about the conflict is given in the details pane.


Aperio Programming Application (US version) - [Head Office]
File
Scan
Settings
Help
Security Mode Status Icons
Security Mode Conflict Details

Lock/sensor	Communication Hub	EAC Address	UHF Link		
01AEF0	0238B1	13	○○●	🔓	⊗

Security mode conflict

Communication Hub [0238B1]	Customer Mode
Lock/sensor [01AEF0]	Manufacturer Mode

Communication Hub [0238B1]

MAC Address	00:17:7a:01:02:02:38:b1
Physical Location	R&D
Firmware Flavor	RS485, Multiple Lock [Aperio protocol]
Firmware Version	6.1.25084
Bootloader Version	1.2.5
Radio protocol version	23
Channel	25 (2.475 GHz)
Radio channels	11, 16, 25

Figure 28. Security mode status and details for a device-hub pair

For a list of the most common security mode icons, the security status indicated by the icons, and the recommended action to take, refer to Table 5.

Table 5: Security Mode status icons for a device-hub pair

Security Mode Icons	Security and Communication Statuses	Recommended Action
🔒	Secure. Both device and hub are communicating in Customer Mode.	None.
🔓	Insecure. Both device and hub are communicating in Manufacturer Mode.	Change the security mode for **both** the device **and** the hub to Customer Mode.
🔓 ⊗	Insecure and no communication. The device is communicating in Manufacturer Mode.	Change the device's security mode to Customer Mode.
🔒 ⊗	Insecure and no communication. The hub is communicating in Manufacturer Mode.	Change the hub's security mode to Customer Mode.

2.7.3.2 Setting an Aperio Hub to Customer Mode

In order to ensure a secure site, all Aperio hubs must be communicating in Customer Mode. If an Aperio hub is not communicating in Customer Mode, use the Aperio Programming Application to set it to Customer Mode.

To set an Aperio hub to Customer Mode

1. Select the Aperio hub in the Aperio Programming Application.
2. Right-click on the Aperio hub, and then select `Communication Hub > Switch to Customer Mode`.
3. Click `OK`.

2.7.3.3 Setting a Wireless Device to Customer Mode

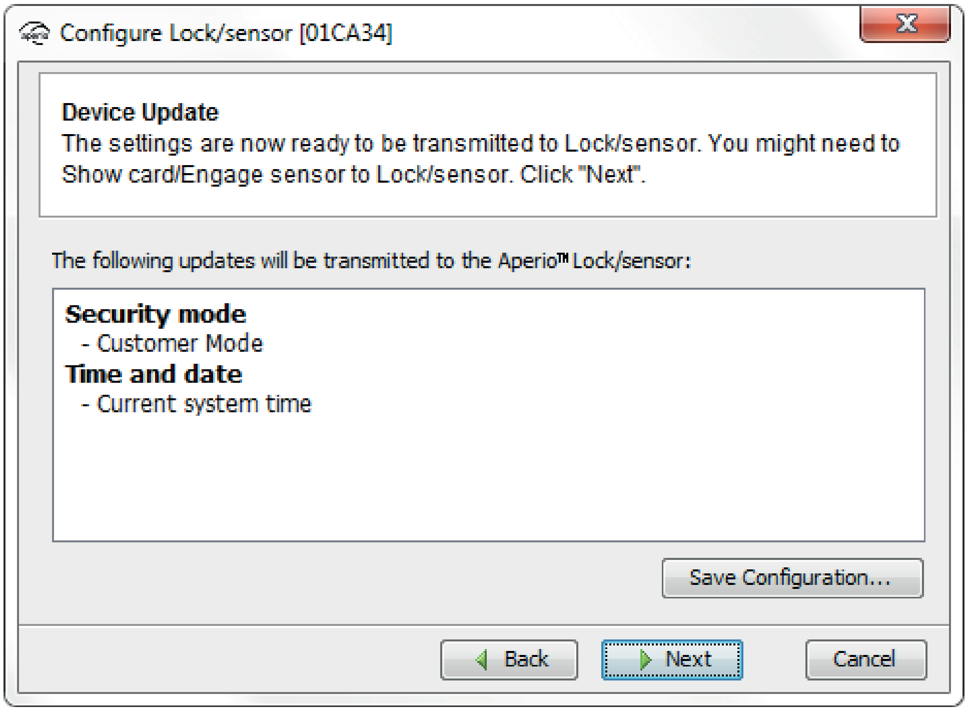
In order to ensure a secure site, all devices must be communicating in Customer Mode. If a device is not communicating in Customer Mode, use the Aperio Programming Application to set it to Customer Mode.

Note: If you need to make multiple configuration settings (for example, security mode and override credentials) to your wireless devices, it is recommended that you make all of the settings on one device and then save the configuration. You can then apply the configuration to all of the other devices. See section 2.7.6, Saving and Applying a Configuration, on page 56 for information on saving a configuration.

To set a wireless device to Customer Mode

1. Select the device in the Aperio Programming Application.
2. Right-click on the wireless device, and then select either `Configure` or `Lock/sensor > Configure`.
3. Click `Next` until you reach the `Security Mode Setting` page.
4. Click `Change`.
5. Select `Switch to Customer mode in device`, and then click `OK`.
6. Click `Next` until you reach the `Device Update` page.

   This page summarizes all the configuration changes you have made. Your page should look similar to the following figure (that is, it should show that the Security Mode will be set to Customer Mode).



Device Update

The settings are now ready to be transmitted to Lock/sensor. You might need to Show card/Engage sensor to Lock/sensor. Click "Next".

The following updates will be transmitted to the Aperio™ Lock/sensor:

Security mode
- Customer Mode

Time and date
- Current system time

Figure 29. Configuration summary

7. Click `Next`.

8. Swipe an access card at the device.

9. Click `Close` to return to the Aperio Programming Application window.

2.7.4 Enabling Remote Open

Wireless devices can be configured to support remote unlocking from either the TX3 Configurator monitor or during an auto-unlock schedule. When you set the unlock mode to ON in the TX3 Configurator monitor, the Aperio wireless device unlocks and stays unlocked until you set the unlock mode to OFF. When an auto-unlock schedule is configured, the wireless device unlocks at the beginning of the auto-unlock schedule and then returns to locked mode at the end of the schedule.

To configure a wireless device to support remote unlocking, you must first enable the advanced options for the Aperio Programming Application and then you must configure each device to support the Remote Open option.

2.7.4.1 Enabling Advanced Options in the Aperio Programming Application

To enable advanced options in the Aperio Programming Application

1. Click `Settings > User Settings`.

2. Select `Show advanced settings`.

3. Click `OK` to close the Message window.

4. Click `OK` to close the User Settings window.

5. Restart the Aperio Programming Application and then log in to your installation.

You now have access to the advanced configuration options.

2.7.4.2 Configuring an Aperio Hub to Support Remote Open

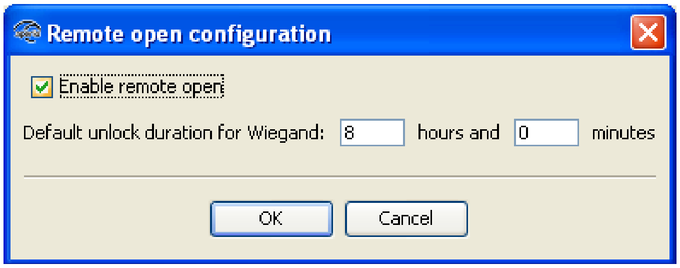
To configure an Aperio hub to support Remote Open

1. Right-click on the Aperio hub, and then select either `Configure` or `Communication Hub > Configure`.

2. Click `Next` until you reach the `Electronic Access Controller Settings` page.

3. In the `Remote Open` section, click `Change`.

4. Select `Enable remote open`, and then click `OK`.



Remote open configuration

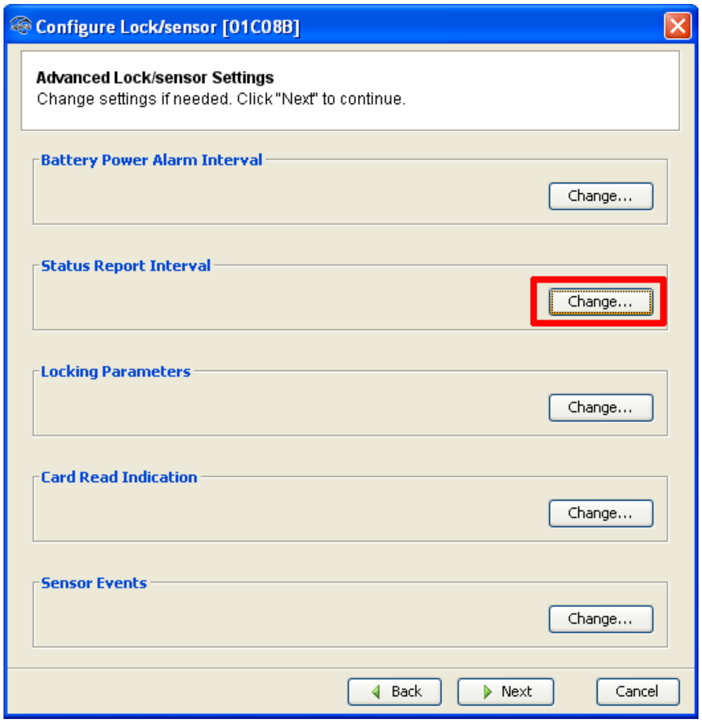
☑ Enable remote open

Default unlock duration for Wiegand: 8 hours and 0 minutes

Figure 30. Remote open configuration

5. Click Next until you reach the `Advanced Lock/sensor Settings` page.

6. Click `Change` beside `Status Report Interval`.

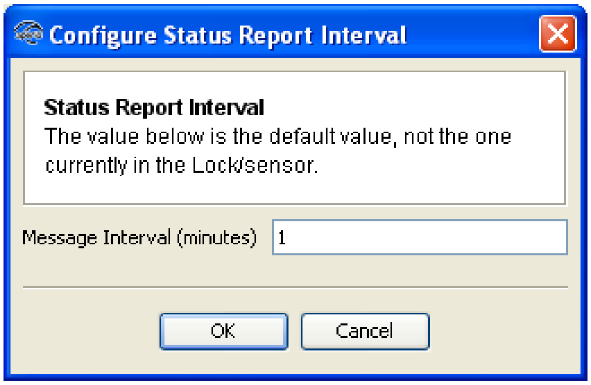


Configure Lock/sensor [01C08B]

Advanced Lock/sensor Settings
Change settings if needed. Click "Next" to continue.

Figure 31. Status Report Interval

7. Change the Message Interval to 1 minute.



Configure Status Report Interval

Status Report Interval
The value below is the default value, not the one currently in the Lock/sensor.

Message Interval (minutes) 1

Figure 32. Configure Status Report Interval

8. Click `OK`.

Note: The Status Report Interval (or Message Interval) is the interval that the lockset sends its status to the hub. The hub waits for the lockset to report its status before it makes any changes to the lockset. To use Remote Open, change the Status Report Interval to a low number, such as 1 or 2 minutes. Otherwise, if you try to open the lock remotely, it may not unlock for 60 minutes (the default Status Report Interval).

9. Click `Next` until you reach the `Device Update` page.

   This page summarizes all the configuration changes you have made. In particular, you should verify that the Remote Open option is set to activate).

10. Click `Next`.

11. If you are prompted to show a card or to engage a sensor, swipe an access card at the device that is paired with the hub.

12. Click `Close` to return to the Aperio Programming Application window.

2.7.5 Override Credentials

A wireless device must communicate with the Aperio Door Controller to determine whether or not to allow access. If the device cannot communicate with either Aperio Door Controller, no one is allowed access.

To avoid this, you can configure an override credentials table for each device. When a device cannot communicate with the Aperio Door Controller, the device checks the credential on the card and then searches for the credential in its override credentials table. If the credential is found, the device grants access. Override credentials are stored in the device and have to be configured for each device individually.

There are two steps to adding override credentials to a device. First, you need to find the credential's information from device's audit trail. After that, you use this information to set the override credentials at the device.

Note: When configuring a wireless device, you must swipe a card at the device to send the configuration settings. Cards with override credentials **cannot** be used to send **any** configuration changes to devices. When you are prompted to swipe a card at a device, make sure that the card is **not** an override credential.

2.7.5.1 Reading Credential Information

In order to enter an override credential, you must know the type of credential, the credential (in hexadecimal format), and the number of bits in the credential. This information is stored in the wireless device's audit log when you swipe the credential (that is, the card) at the device.

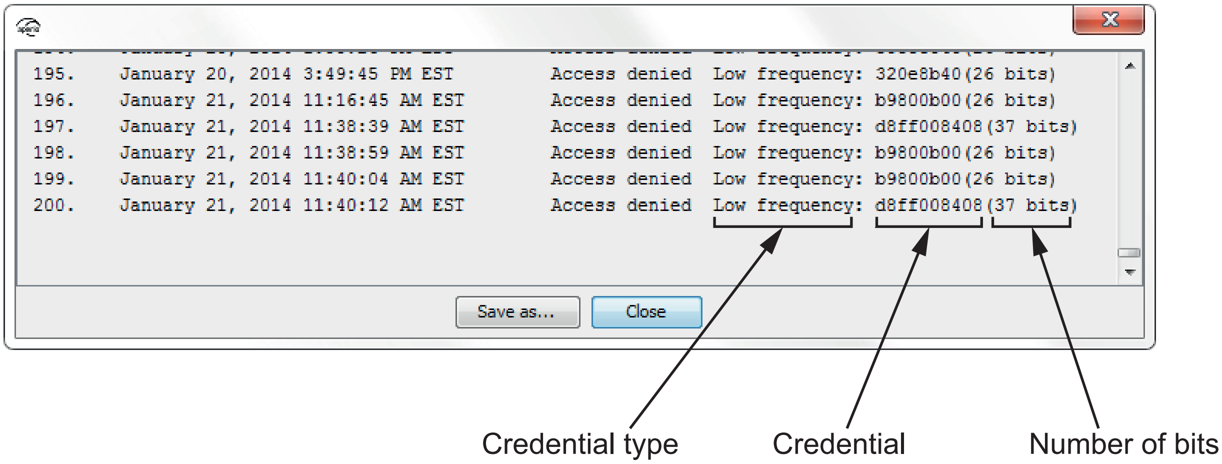
To read credential information

1. Swipe all of the cards that you want to assign override credentials to at a paired device.

Note: All override credentials must be added at the same time. If you need to add more than one override credential, swipe **all** of the credentials (cards) that you need to add at the device.

2. In the Aperio Programming Application, right-click on the wireless device where you swiped the credentials, and then select `Lock/Sensor > Get Audit Trail`.
3. Swipe a card at the wireless device.

The audit trail for the device opens in a separate window. The window shows you the credential type, the credential (in hexadecimal), and the number of bits for the credential for all the cards swiped at the device (see Figure 33). Scroll to the bottom of the audit trail to find the information for the credentials you swiped in step 1.



```
195.    January 20, 2014 3:49:45 PM EST        Access denied  Low frequency: 320e8b40(26 bits)
196.    January 21, 2014 11:16:45 AM EST       Access denied  Low frequency: b9800b00(26 bits)
197.    January 21, 2014 11:38:39 AM EST       Access denied  Low frequency: d8ff008408(37 bits)
198.    January 21, 2014 11:38:59 AM EST       Access denied  Low frequency: b9800b00(26 bits)
199.    January 21, 2014 11:40:04 AM EST       Access denied  Low frequency: b9800b00(26 bits)
200.    January 21, 2014 11:40:12 AM EST       Access denied  Low frequency: d8ff008408(37 bits)
```

Figure 33. The Audit Trail window for a wireless device

4. Record the credential type, credential, and number of bits for all of the cards you want add to the override credentials table. Alternatively, you can save the audit trail to a text file (click `Save as` in the audit trail window).

5. Click `Close` to return to the Aperio Programming Application.

2.7.5.2 Setting Override Credentials

A card with override credentials can gain access at a wireless device even when the device cannot communicate with the Aperio Door Controller. Override credentials are stored at the device and have to be programmed into each device individually.

Notes: The following should be kept in mind when setting override credentials:

- If you need to make multiple configuration settings (for example, security mode and override credentials) to your wireless devices, it is recommended that you make all of the settings on one device and then save the configuration. You can then apply configuration to all of your other devices. See section 2.7.6, Saving and Applying a Configuration, on page 56 for information on using configurations.
- Override credentials cannot be used to make configuration changes (for example, pairing a device with a hub).
- If you do not have the credential information for your cards

(credential type, credential, and the number of bits), see section 2.7.5.1, Reading Credential Information.

To set override credentials on a wireless device

1. Right-click on the wireless device, and then select either `Configure` or `Lock/sensor > Configure`.

2. Click `Next` until you reach the `Override Credential` page.

3. Select the credential type from the drop-down list. Note the following:

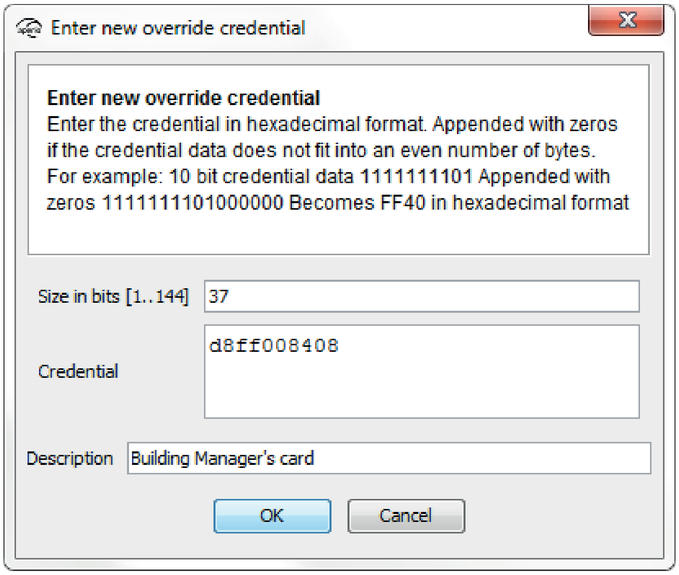
   - If your credential type is **Low frequency**, select `HID Prox and EM Prox` from the list.
   - If your credential type is **iClass**, select `iClass` from the list.

4. Click `Add`.

5. In the `Enter new override credential` window, enter the following information:

   - **Size in bits**: the number of bits of the credential
   - **Credential**: the credential value (in hexadecimal)
   - **Description**: (optional) a description for the override credential

   Your window should look similar to the following figure.



Enter new override credential

Enter new override credential
Enter the credential in hexadecimal format. Appended with zeros if the credential data does not fit into an even number of bytes.
For example: 10 bit credential data 1111111101 Appended with zeros 1111111101000000 Becomes FF40 in hexadecimal format

Size in bits [1..144]: 37

Credential: d8ff008408

Description: Building Manager's card

Figure 34. Enter new override credential

6. Click `OK`.

7. Repeat steps 3 to 6 for all of your override credentials.

Note: **All** override credentials **must** be added at the same time. If you try to add an override credential at a later time, you will lose all of the override credentials currently stored in the device.

8. Click `Next` until you reach the `Device Update` page.

   This page summarizes all the configuration changes you have made. In particular, you should verify that the override credentials you added are all there and that there are no errors.

9. Click `Next`.

10. Swipe a card at the device.

11. Click `Close` to return to the Aperio Programming Application.

2.7.5.3 Deleting Override Credentials

Every time you add override credentials to a device, the old override credentials are replaced with the new ones. However, you cannot use an empty override credentials list to delete all of the override credentials at a device. To delete all of the override credentials from a device, you must specifically tell the device to remove all of its override credentials.

To delete all the override credentials at a device

1. Right-click on the wireless device, and then select either `Configure` or `Lock/sensor > Configure`.

2. Click `Next` until you reach the `Override Credential` page.

3. Select the `Remove all credentials in lock` check box at the bottom of the page.

4. Click `Next` until you reach the `Device Update` page.

   This page summarizes all the configuration changes you have made. In particular, you should verify that **Remove all override credentials** is listed in the changes.

5. Click `Next`.

6. Swipe a card at the device.

7. Click `Close` to return to the Aperio Programming Application.

2.7.6 Saving and Applying a Configuration

After making configuration settings to a device, you can save the configuration and then apply the same configuration settings to other devices. This is useful if you have to make the same configuration settings (for example, security mode and override credentials) to a number of devices.

2.7.6.1 Saving a Configuration

To save a configuration

1. Right-click on the wireless device, and then select either `Configure` or `Lock/sensor > Configure`.
2. Click `Next` to access the configuration windows, and then set all of the configuration options for your devices.

   Some of the configuration options and how to set them are described in this manual (for example, section 2.7.3.3, Setting a Wireless Device to Customer Mode, and section 2.7.5.2, Setting Override Credentials).
3. When you reach the `Device Update` page, verify that all of the configuration settings are correct.
4. Click `Save Configuration`.
5. In the `Save Configuration` window, enter a name for the configuration, and then click `OK`.
6. Click `Next` to send the configuration to the device.
7. Swipe a card at the device.
8. Click `Close` to return to the Aperio Programming Application.

2.7.6.2 Applying a Configuration to a device

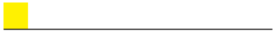
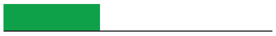
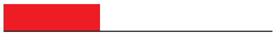
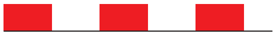
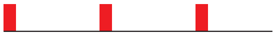
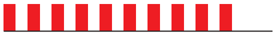
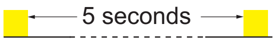
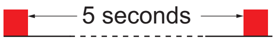
To apply a configuration to a device

1. Right-click on the wireless device, and then select either `Apply configuration` or `Lock/sensor > Apply configuration`.
2. Select the configuration you want to apply from the list of saved configurations.
3. Click `Confirm`.
4. Swipe a card at the device.
5. Click `Close` to return to the Aperio Programming Application.

2.7.7 Wireless Device Status LEDs

Each device has three LEDs (yellow, red, and green) that indicate the status of the device. Refer to Table 6 for the different LED indications and their associated device status.

Table 6: Wireless device LED status indications under normal operation

LED Indication	Description	Device Status
	One yellow flash (0.25 s)	Reading card.
	One green flash (1.0 s)	Access granted (Aperio Door Controller is either online or offline).
	One red flash (1.0 s)	Access denied (Aperio Door Controller is online).
	Three red flashes (0.5 s)	Access denied (Aperio Door Controller is offline).
	One red flash (0.125 s) every second	Lock mechanism blocked when closing.
	Ten red flashes (0.125 s)	Maintenance required. If repeating, lock cannot close.
	One yellow flash (0.25 s) every 5 seconds	Battery needs replacement.
	One red flash (0.25 s) every 5 seconds	Battery has reached end of life and the lock is disabled.

2.8 Setting the DIP Switches on Switch SW2

The DIP switches on SW2 are used to set the address for the Aperio Door Controller on the TX3 RS-485 network. Valid addresses are 1 to 63. DIP switches 1 to 6 are used for binary addressing with DIP switch 1 being the least significant bit. DIP switch SW2 is found at the top central portion of the Aperio Door Controller board (see Figure 35).

See Table 7 for the DIP switch settings for RS-485 network addressing.

Note: DIP Switch 7 is not used and should remain at the factory set value (OFF).

Notes: DIP Switch 8 determines how an IP address is assigned to the IP Module (if installed).

- **DIP Switch 8 OFF:** The IP address is assigned using a DHCP server. This is the factory default setting.
- **DIP Switch 8 ON:** The IP address is assigned using the Configurator software.

Table 7: SW2 DIP Switch Settings for RS-485 Network Addressing

ADDRESS	SWITCH 1	SWITCH 2	SWITCH 3	SWITCH 4	SWITCH 5	SWITCH 6
1	ON	OFF	OFF	OFF	OFF	OFF
2	OFF	ON	OFF	OFF	OFF	OFF
3	ON	ON	OFF	OFF	OFF	OFF
4	OFF	OFF	ON	OFF	OFF	OFF
5	ON	OFF	ON	OFF	OFF	OFF
6	OFF	ON	ON	OFF	OFF	OFF
7	ON	ON	ON	OFF	OFF	OFF
8	OFF	OFF	OFF	ON	OFF	OFF
9	ON	OFF	OFF	ON	OFF	OFF
10	OFF	ON	OFF	ON	OFF	OFF
11	ON	ON	OFF	ON	OFF	OFF
12	OFF	OFF	ON	ON	OFF	OFF
13	ON	OFF	ON	ON	OFF	OFF
14	OFF	ON	ON	ON	OFF	OFF
15	ON	ON	ON	ON	OFF	OFF
16	OFF	OFF	OFF	OFF	ON	OFF
17	ON	OFF	OFF	OFF	ON	OFF
18	OFF	ON	OFF	OFF	ON	OFF
19	ON	ON	OFF	OFF	ON	OFF
20	OFF	OFF	ON	OFF	ON	OFF
21	ON	OFF	ON	OFF	ON	OFF

Table 7: SW2 DIP Switch Settings for RS-485 Network Addressing (Continued)

ADDRESS	SWITCH 1	SWITCH 2	SWITCH 3	SWITCH 4	SWITCH 5	SWITCH 6
22	OFF	ON	ON	OFF	ON	OFF
23	ON	ON	ON	OFF	ON	OFF
24	OFF	OFF	OFF	ON	ON	OFF
25	ON	OFF	OFF	ON	ON	OFF
26	OFF	ON	OFF	ON	ON	OFF
27	ON	ON	OFF	ON	ON	OFF
28	OFF	OFF	ON	ON	ON	OFF
29	ON	OFF	ON	ON	ON	OFF
30	OFF	ON	ON	ON	ON	OFF
31	ON	ON	ON	ON	ON	OFF
32	OFF	OFF	OFF	OFF	OFF	ON
33	ON	OFF	OFF	OFF	OFF	ON
34	OFF	ON	OFF	OFF	OFF	ON
35	ON	ON	OFF	OFF	OFF	ON
36	OFF	OFF	ON	OFF	OFF	ON
37	ON	OFF	ON	OFF	OFF	ON
38	OFF	ON	ON	OFF	OFF	ON
39	ON	ON	ON	OFF	OFF	ON
40	OFF	OFF	OFF	ON	OFF	ON
41	ON	OFF	OFF	ON	OFF	ON
42	OFF	ON	OFF	ON	OFF	ON
43	ON	ON	OFF	ON	OFF	ON
44	OFF	OFF	ON	ON	OFF	ON
45	ON	OFF	ON	ON	OFF	ON
46	OFF	ON	ON	ON	OFF	ON
47	ON	ON	ON	ON	OFF	ON
48	OFF	OFF	OFF	OFF	ON	ON
49	ON	OFF	OFF	OFF	ON	ON
50	OFF	ON	OFF	OFF	ON	ON

Table 7: SW2 DIP Switch Settings for RS-485 Network Addressing (Continued)

ADDRESS	SWITCH 1	SWITCH 2	SWITCH 3	SWITCH 4	SWITCH 5	SWITCH 6
51	ON	ON	OFF	OFF	ON	ON
52	OFF	OFF	ON	OFF	ON	ON
53	ON	OFF	ON	OFF	ON	ON
54	OFF	ON	ON	OFF	ON	ON
55	ON	ON	ON	OFF	ON	ON
56	OFF	OFF	OFF	ON	ON	ON
57	ON	OFF	OFF	ON	ON	ON
58	OFF	ON	OFF	ON	ON	ON
59	ON	ON	OFF	ON	ON	ON
60	OFF	OFF	ON	ON	ON	ON
61	ON	OFF	ON	ON	ON	ON
62	OFF	ON	ON	ON	ON	ON
63	ON	ON	ON	ON	ON	ON

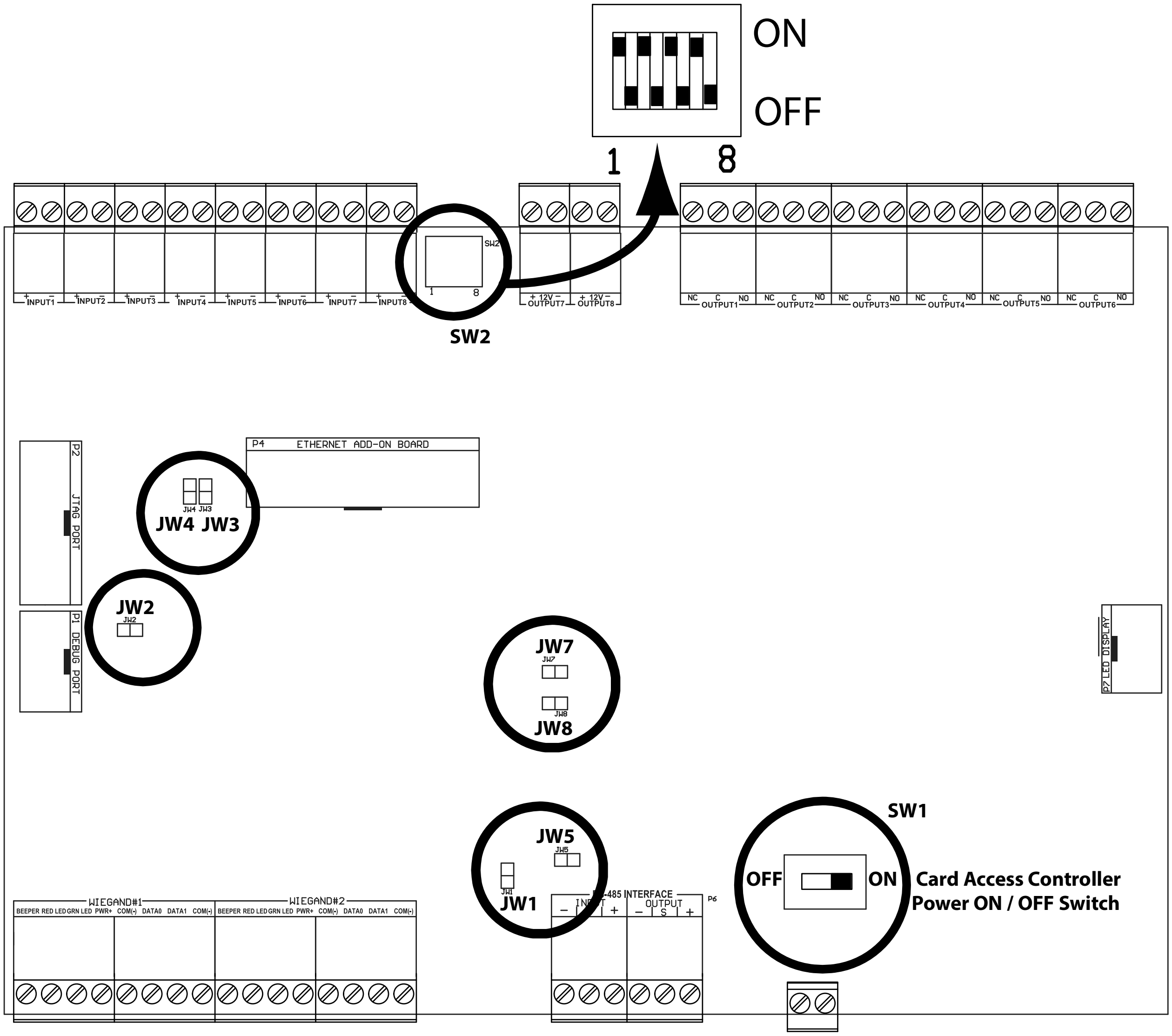


Figure 35. Location of Jumpers JW1 to JW8 and Switches SW1 and SW2

2.9 Setting Jumpers

There are seven pre-set jumpers on the controller board as follows (refer to Figure 35):

JW1. `JW1` is used for updating firmware and by default is always open.

JW2. `JW2` is used for updating firmware and by default is open. See Updating Firmware on page 62.

JW3 and JW4. JW3 and JW4 are not used and are open by default.

JW5. JW5 is open by default. On boards with the model number MD-10xx, you can close JW5 on the first and last controllers instead of using end-of-line 120 Ω resistors for RS-485.

JW7 and JW8. If there are problems with RS-485 communication, close both JW7 and JW8 on either the first or last controller connected by RS-485. By default, JW7 and JW8 are open.

2.10 Turning on the Controller

Before you turn on the controller, ensure that the all connections adhere with the correct operation of the devices.

Once the controller is turned on, you must begin the configuration. Basic configuration settings for the Aperio Door Controller are covered in Chapter 3 Configuration. For detailed information on how to configure the controller and other TX3 devices, see LT-995 Configuration and Administration Guide.

2.10.1 Default Configuration Values

Once the controller is on, it operates according to its preset default configuration values. When the configurator software first starts, it uses the default values and adopts these values as its initial settings.

The default configuration values are adopted only when the following situations occur:

- turning the system on for the first time
- memory corruption
- program upgrade

2.11 Updating Firmware

You can update the firmware on your panel with the TX3 Configurator software by using one of the following methods.

- Firmware Upgrade Wizard
- Network Firmware Upgrade

The Firmware Upgrade Wizard can be used to update only one panel at a time. It will work on any panel.

The Network Firmware Upgrade procedure can update more than one panel at the same time. In order to use the Network Firmware Upgrade, all of the panels must already have firmware that supports this feature installed on them.

Refer to LT-995, TX3 Configuration and Administrator Manual, for instructions on how to perform both of types of firmware upgrade. LT-995 can be found on the TX3 Configurator Software installation CD, USB flash drive, or on the Mircom website.

2.11.1 Firmware Version Control

The firmware version number is accessible from the configurator software and changes whenever there is a major, minor or revision update.

The following convention is used whenever there is a major, minor or revision change:

Initial release. Version 1.00.0

Major change. Version 2.00.0

Minor change. Version 2.01.0

Revision changes. Version 2.01.1

2.12 Beginning Configuration

The Aperio Door Controller is now configurable using the following connections.

- USB connection
- Ethernet connection
- COM port connection
- Modem connection

For a complete description of the configuration and on how to establish a connection to the Aperio Door Controller using a USB, ethernet, COM port or modem connection, see the following documentation:

- LT-995 Configuration and Administration Guide
- TX3 Configurator Quick Start LT-973

Verify the following:

- Ensure that the controller and all connected devices and components are fully operational.

- Ensure the controller DIP Switches (SW2) are set with a unique network address.
- Ensure the TX3 Configurator software is set with the correct controller network address.
- Ensure that your PC and the TX3 Configurator are set with the correct date and time.

To start the configuration

1. Connect the PC to the controller using the USB port.
2. Launch the TX3 Configurator and click `Connect.` Once connected the connection icon appears in the Configurator tool bar.
3. Configure the Aperio Door Controller System using the instructions in Chapter 3 Configuration, the TX3 Configurator Software Program TX3-MSW, or the LT-995 Configuration and Administration Guide.

3 Configuration

This chapter describes how to create a job with an Aperio Door Controller using the TX3 Configurator software. All the configurable features and their modes of operation and detailed information on how to configure the system using the TX3 Configurator software are covered.

This chapter explains

- Configuring Aperio Door Controller panels with the TX3 Configurator
- Adding and Deleting Access Points
- Access Point Schedule Options
- Access Point Timer Options
- Advanced Options
- Aperio Door Controller Inputs
- Aperio Door Controller Outputs
- Correlations
- Access Levels and Elevator Control
- Cards
- Schedules
- Holidays
- Sending Your Configuration
- System Status

3.1 Configuring Aperio Door Controller panels with the TX3 Configurator

TX3 Configurator software is used to configure your Aperio Door Controller panel (as well as any other TX3 panels in your TX3 system). Before you can configure an Aperio Door Controller panel, you must create a job that has an Aperio Door Controller added to it.

Note: To perform the tasks described in this chapter, you must have a computer with the latest version of the TX3 Configurator software. Details on how to install the software and drivers can be found in LT-995, the TX3 Series Configuration and Administration Manual.

3.1.1 Creating a New Job

This section describes two methods for creating a new job with the TX3 Configurator software. The first method creates a new job using a template. This method is recommended for an installation with a single panel that is not connected to any other TX3 devices. The second method creates a new job by reading all of the panels on the network. This method is recommended for an installation where the Aperio Door Controller panel is connected to other TX3 panels using either an RS-485 network, a TCP/IP network, or a TCP/IP network with RS-485 subnetworks (see section 1.5, Network Setup, on page 12 for more information on TX3 networks).

3.1.1.1 Creating a New Job Using a Template

Use a template to create a new job that with a single a stand-alone Aperio Door Controller panel.

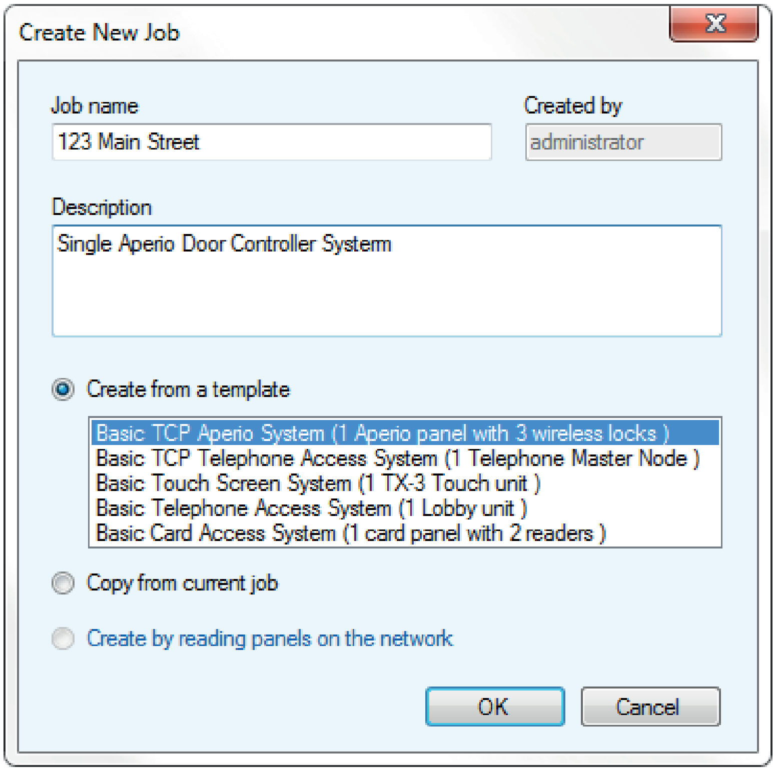
To create a new job using a template

1. Start the TX3 Configurator.
2. Enter your username and password, and then click `Login`.

   By default, the username is `administrator` and there is no password.
3. Click `File > New Job`.
4. Enter a name for the job in the `Job name` text box.
5. (Optional) Enter a description for the job in the `Description` text box.
6. Select `Create from a template`.

7. Select the `Basic TCP Aperio System (1 Aperio panel with 3 wireless locks)` option.

   Your Create New Job window should look similar to Figure 36.



Create New Job

Job name: 123 Main Street

Created by: administrator

Description: Single Aperio Door Controller Systerm

● Create from a template

- Basic TCP Aperio System (1 Aperio panel with 3 wireless locks)
- Basic TCP Telephone Access System (1 Telephone Master Node)
- Basic Touch Screen System (1 TX-3 Touch unit)
- Basic Telephone Access System (1 Lobby unit)
- Basic Card Access System (1 card panel with 2 readers)

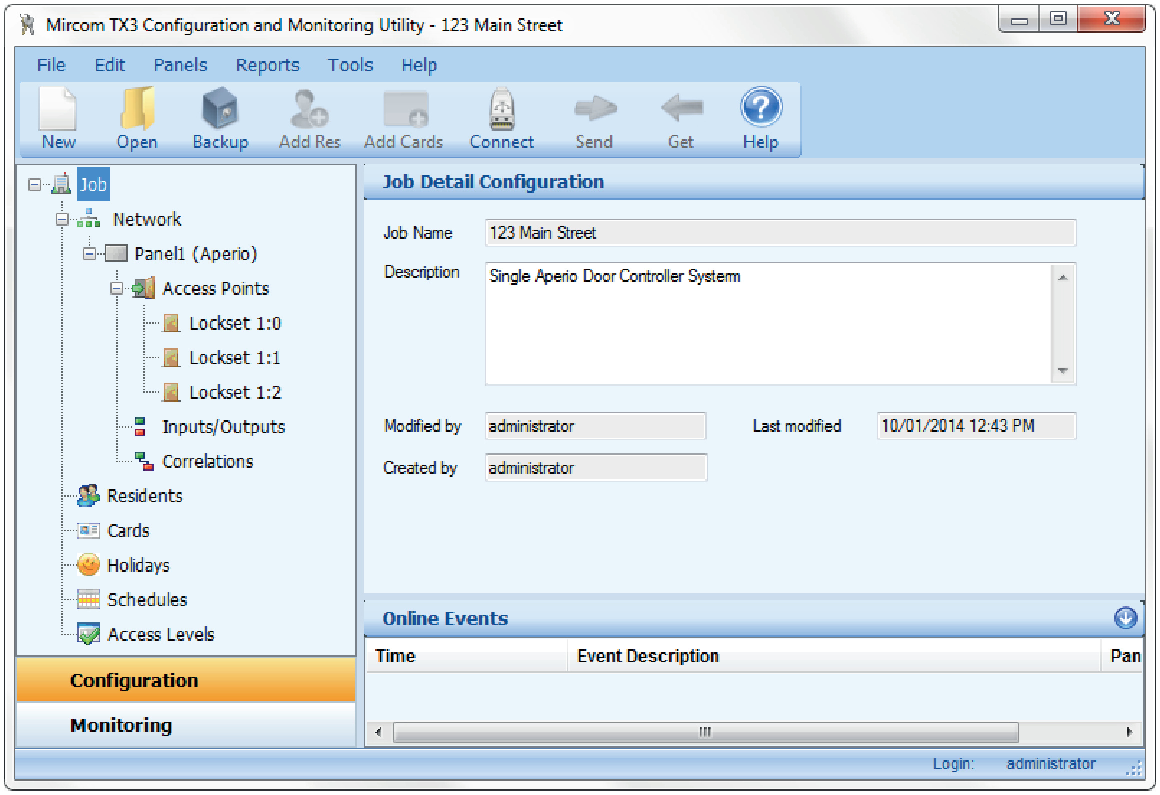
○ Copy from current job

○ Create by reading panels on the network

Figure 36. The Create New Job window

8. Click `OK`.

Your TX3 Configurator window should look similar to Figure 37. Notice that the template adds three access points (wireless devices) to the Aperio Door Controller panel. (To see the access points, expand the panel entry, and then expand `Access Points`.) See section 3.2, Adding and Deleting Access Points, for instructions on how to add more access points or delete extra access points if this configuration does not match your installation.



Job Detail Configuration

Job Name: 123 Main Street

Description: Single Aperio Door Controller System

Modified by: administrator

Last modified: 10/01/2014 12:43 PM

Created by: administrator

Login: administrator

Figure 37. The Job Detail Configuration window

3.1.1.2 Creating a New Job by Reading the Panels on the Network

If your Aperio Door Controller is connected with other TX3 panels, the TX3 Configurator can connect to your TX3 system, read all of the panels in the system, and then create a new job with all of your panels in it. In order to do this, all of the following conditions must be true.

- All of the panels must be powered on.
- Each panel on an RS-485 network or subnetwork must have a unique address.
- There can only be one Master Node connected to an RS-485 subnetwork.

Information on setting the RS-485 address for an Aperio Door Controller panel can be found in section 2.8, Setting the DIP Switches on Switch SW2, on page 57. Information about the different TX3 network configurations can be found in section 1.5, Network Setup, on page 12. To configure other TX3 panels (such as the Touch Screen or the Lobby Control Unit), refer to the appropriate installation and operation manual.

To create a new job by reading the panels on the network

1. Connect your computer to the TX3 system using one of the following methods, depending on the type of network your TX3 system is using:

   RS-485 only: Power down one of the panels on the RS-485 network, and then connect to the panel using a USB cable from your computer to the panel's USB connector. Once connected, power on the panel.

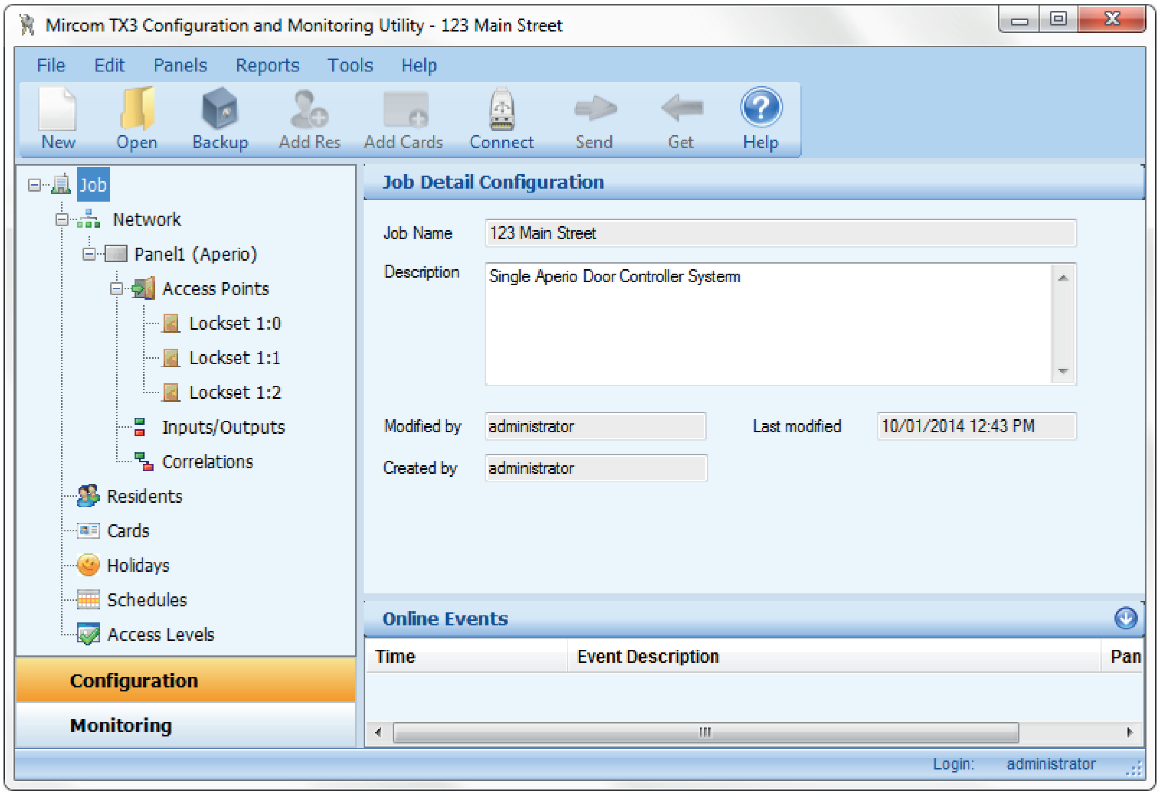
   TCP/IP or combination TCP/IP and RS-485: Use an ethernet cable to connect your computer to the TCP/IP network that the TX3 system is on.

2. Start the TX3 Configurator.

3. Enter your username and password, and then click `Login`.

   By default, the username is `administrator` and there is no password.

   Your TX3 Configurator window should look similar to Figure 38, with a job tree in the left pane. If there is no job tree in the left pane, you will need to create a new job. Follow the instructions in section 3.1.1.1, Creating a New Job Using a Template, to create the new job, and then continue to the next step.



Job Detail Configuration

Job Name: 123 Main Street

Description: Single Aperio Door Controller System

Modified by: administrator

Last modified: 10/01/2014 12:43 PM

Created by: administrator

Figure 38. The Job Detail Configuration window

4. Click `Network` in the job tree.

5. In the Network Configuration window, select the type of connection you made in step 1 from the `PC connection` list (that is, select either `USB` or `TCP/IP`).

6. From the menu bar, click `Panels > Connect`.

7. Click `File > New Job`.

8. Enter a name for the job in the `Job name` text box.

9. (Optional) Enter a description for the job in the `Description` text box.

10. Select `Create by reading panels on the network`.

11. Click `OK`.

    The TX3 Configurator connects to each of the panels to create the job. This may take a few minutes, especially if you have a large number of panels in your TX3 system.

12. From the menu bar, click `Panels > Disconnect`.

The job tree in your TX3 Configurator should be populated with all of the panels in your TX3 system. Disconnecting from the system is necessary in order to be able to configure your Aperio Door Controller panels. You cannot configure your TX3 system while you are connected to it.

3.1.2 Configuring an Aperio Door Controller Panel

Use the TX3 Configurator to set options for your Aperio Door Controller panel. Configuration options include setting the RS-485 address for the Aperio Door Controller panel as well as the types of cards that the panel can read.

To configure a panel

1. Select an Aperio Door Controller panel in your job tree.

2. Provide information for the following:

   Panel label. Provide a name for the Panel.

   Panel model. The application automatically retrieves the selected panel model information. This field is read only.

   Address. The drop down list displays the remaining available panel addresses. From this list select the panel address. This field is disabled if a connection is active. Ensure that this address matches the panel address.

   Master Node. If you are connected to your TX3 system through TCP/IP, this option lets you either configure the panel as a Master Node (select **This is a master** from the list) or specify the Master Node for your panel (select the Master Node from the list).

   Test Connection. This option tests the connection between your computer and a Master Node. You can only test the connection to a Master Node panel. You must be connected to the TX3 system in order to use `Test Connection`.

   IP address. The IP address of your panel if it is a Master Node on a TCP/IP network. This field only appears if you are connected to your TX3 system through TCP/IP.

Note: You cannot change a Master Node's IP address by editing the `IP address` field. To change a Master Node's IP address, use the IP Change Tool. See LT-995, the TX3 Configurator Configuration and Administration Manual, for details on how to use the IP Change Tool.

3. Provide information for each of the following:

   Card format. Select the card reader format for panel. See section 1.3.1 on page 11 for the list of supported formats. Select only the formats that are being used. In addition, do not select more than one format with the same bit length. For example, select either 36-bit HID Simplex or 36-bit Keyscan, but do not select both.

   Card discovery mode. Enable this option, then send the Job to the panel to put the panel into card discovery mode. While the panel is in card discovery mode and you present a card to the reader, the panel will display the card's raw data in the Online Events pane. To disable the feature, uncheck `Card discovery mode`, then send the job to the panel again.

   Custom Formats. See LT-995 on the USB flash or **http://www.mircom.com** for instructions on creating custom card formats.

   Report real time events to PC. Enable or disable real time event sending to the PC. If enabled, only the real time logs are sent to the PC.

Facility code. Enter the building's facility code with a value from 0 to 4294967294. Enabling the facility code mode lets you grant access to cards based on facility code.

Date and Time button. Select this option to set the date and time of the panel, set daylight savings time, and to set the panel adjustment time.

Note: Configuration settings must be sent to the panel in order for them to be applied in your TX3 system. After you have completed all of your configuration settings, connect to your TX3 system and send the job (see section 3.13, Sending Your Configuration, on page 98).

3.2 Adding and Deleting Access Points

Aperio Door Controllers can be configured with up to 8 wireless devices (access points). When you add a new Aperio Door Controller panel to your job, you have to add one access point for each wireless device that the panel controls. For example, if you installed an Aperio Door Controller with 2 Aperio hubs and paired 3 devices to each of the hubs, you will need to add 6 access points to your panel in the TX3 Configurator.

Note: The terms "access point", "wireless device", and "device" all refer to Aperio wireless locksets and sensors. To avoid confusion, the terms "wireless device" and "device" are used to refer to the Aperio wireless lockset and sensor hardware (for example, "swipe a card at the wireless device") and the term "access point" is used to refer to the software representation of an Aperio wireless device in the TX3 Configurator software (for example, "configure the timers for an access point" or "right-click on the access point").

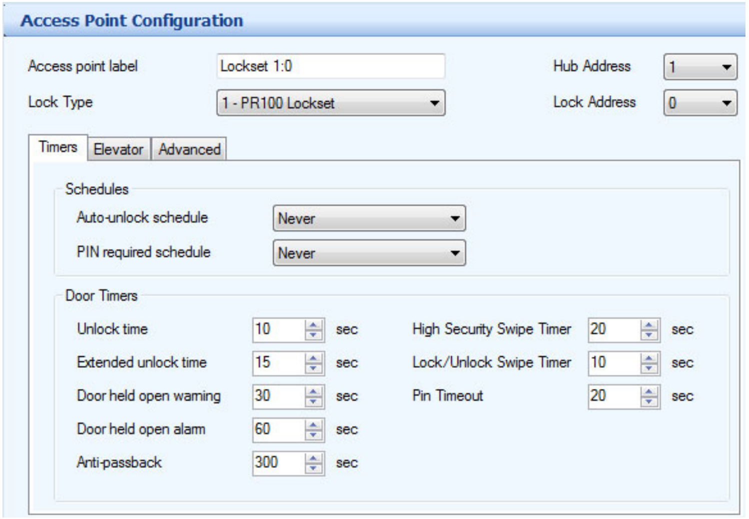
3.2.1 Adding and Configuring an Access Point

For each wireless device in your Aperio Door Controller system, you must add an access point that represents the wireless device in the TX3 Configurator job tree. In order for the Aperio Door Controller to control the wireless device, the access point must be properly configured with the wireless device's settings. Specifically, you must provide the Hub Address for the device (the Hub Address is the RS-485 address for the Aperio hub that the device is paired with), the Lock Address for the device, and the model of the device.

To add and configure an access point

1. Right-click on the Aperio Door Controller panel, and then select `Add Access Point`.

   A new access point is added and the Access Point Configuration window opens. The Configurator automatically assigns values for the Hub Address and the Lock Address. In the following steps you will change these values to match the Hub and Lock Addresses programmed into your wireless device.



Access Point Configuration

Access point label: Lockset 1:0
Hub Address: 1
Lock Type: 1 - PR100 Lockset
Lock Address: 0

Schedules
Auto-unlock schedule: Never
PIN required schedule: Never

Door Timers
Unlock time: 10 sec
Extended unlock time: 15 sec
Door held open warning: 30 sec
Door held open alarm: 60 sec
Anti-passback: 300 sec
High Security Swipe Timer: 20 sec
Lock/Unlock Swipe Timer: 10 sec
Pin Timeout: 20 sec

Figure 39. The Access Point Configuration window

2. Select the Hub Address of the device from the list.

   The Hub Address is the RS-485 address setting for the Aperio hub that the wireless device is paired to. You can select a value from 1 to 15.

Notes:

- If the Hub Address and Lock Address combination you want to select have already been assigned to another device, you will get an error. If you know that your values are correct, find the other access point and then change its Hub and Lock Address settings.
- If you followed the instructions in section 2.7.2, Pairing a Wireless Device to an Aperio Hub, there should be a label on the device with the Hub Address and Lock Address. If you did not label your device, you must use the Aperio Programming Application to find these values. See section 2.7.2, Pairing a Wireless Device to an Aperio Hub, on page 38 for more information on pairing and finding these addresses.

3. Select the Lock Address of the access point from the list.

   You can select from a value from 0 to 7 for your Lock Address.

4. Select the model of your wireless device from the Lock Type list.

5. Enter a label for the access point in the `Access point label` text box.

Continue with your configuration settings. After you have completed all of your configuration settings, connect to your TX3 system and send the job (see section 3.13, Sending Your Configuration, on page 98).

3.2.2 Deleting an Access Point

Wireless devices that have been unpaired from an Aperio Door Controller panel should have their access points deleted from the job.

To delete an access point

1. Find the access point you want to delete in the job tree.

   If you do not see the access point in your job tree, expand the Aperio Door Controller panel entry, and then expand the panel's `Access Point` entry.

2. Right-click on the access point you want to delete, and then select `Delete Access Point`.

3. Click `OK`.

Continue with your configuration settings. After you have completed all of your configuration settings, connect to your TX3 system and send the job (see section 3.13, Sending Your Configuration, on page 98).

3.3 Access Point Schedule Options

Access points can be configured to go into certain modes according to a schedule. These modes are:

- Auto-unlock
- PIN required

These modes are described in sections 3.3.1to 3.3.2. Section 3.3.3 explains how to enable a mode by selecting a schedule for it.

When a schedule becomes valid, the access point begins to operate under the mode. For example, if you select a schedule called “Office Hours” for the Auto-unlock mode, the access point automatically unlocks during the days and times set in the “Office Hours” schedule. Once the schedule ends, the access point goes into locked mode.

You must define the schedule for your mode before you can configure the access point for that schedule. By default, two schedules are programmed into the TX3 Configurator: Always and Never. If you want to set a custom schedule for an access point mode, see section 3.11, Schedules, on page 96.

3.3.1 Auto-unlock

During an auto-unlock schedule, the wireless device automatically unlocks and stays unlocked until the end of the schedule.

Note: In order for the Aperio Door Controller to unlock a wireless device remotely, the Remote Open option must be set for the wireless device. See section 2.7.4, Enabling Remote Open, on page 49 for information on how to do this.

3.3.2 PIN required

During the PIN required schedule, users will have to swipe a valid card at the device and then enter their PIN code in order to gain access. The PIN code is 1 to 4 digits long and must be set in the options for the card (see section 3.10, Cards, for information on configuring cards). 0 is not a valid PIN code.

Note: This feature requires a wireless device with a keypad.

3.3.3 Setting an Access Point Schedule

Access points can operate in `Auto-unlock` and `PIN required` modes according to a schedule for each mode. In order to set a schedule for a mode, the schedule must already be defined (see section 3.11, Schedules, on page 96).

To set the schedule for an access point mode

1. Find the access point in the job tree.

   If you do not see the access point in your job tree, expand the Aperio Door Controller panel entry, and then expand the panel's `Access Point` entry.

2. Click on the access point.
3. Select the **Timers** tab.
4. To set an auto-unlock schedule, select a schedule from the `Auto-unlock schedule` list.
5. To set a PIN required schedule, select a schedule from the `PIN required schedule` list.

Continue with your configuration settings. After you have completed all of your configuration settings, connect to your TX3 system and send the job (see section 3.13, Sending Your Configuration, on page 98).

3.4 Access Point Timer Options

You can set timers for criteria related to your access point, such as how long to unlock the access point and how long to wait for the anti-passback restriction to expire. The timers for each access point are accessed by selecting the access point and then selecting the `Timers` tab. The following timers are associated with the Aperio Door Controller System operation:

- Unlock Time
- Extended Unlock Time
- Door Held Open Warning
- Door Held Open Alarm
- Anti-passback
- High Security Swipe Timer
- Lock/Unlock Swipe Timer
- Pin Timeout

Each of these timers are explained in more detail in sections 3.4.1 to 3.4.8. Section 3.4.9 explains how to set these timers for an access point.

3.4.1 Unlock Time

The door unlock timer starts when the door unlocks. When the timer expires the door locks. The unlock timer is programmable from 0 to 300 seconds. The default is 10 seconds.

3.4.2 Extended Unlock Time

The extended unlock timer is used for cards with the extended unlock feature enabled. The timer starts when the door unlocks. When the extended unlock timer expires the door locks. The extended unlock timer is programmable from 10 to 300 seconds. The default is 15 seconds.

3.4.3 Door Held Open Warning

The door held open warning timer starts when a door is still open after the unlock or extended unlock timer expires. If the door is still open after the door held open timer expires, a ‘door held open’ warning is issued to the PC and the common trouble status becomes active. If the door closes during this interval, the timer resets and no warning report is sent to the PC.

The door held open warning timer is programmable from 10 to 900 seconds. The default is 30 seconds

3.4.4 Door Held Open Alarm

The door held open alarm timer starts when the door held open warning timer expires and the door remains open. If the door is still open when this timer expires, a 'door held open alarm' is issued to the PC and the common alarm status becomes active. The door held open alarm timer is programmable from 10 to 900 seconds. The default is 60 seconds.

3.4.5 Anti-passback

The anti-passback timer prevents the use of the same card by more than one person at an access point. The anti-passback timer starts when a valid card is swiped at an access point. During the anti-passback period, the same card cannot be used at that access point until the anti-passback timer expires. The anti-passback timer is programmable from 0 to 900 seconds. The default is 300 seconds.

3.4.6 High Security Swipe Timer

If an access card with the high security privilege is swiped four times in succession, the mode of the access point toggles between high security on and high security off. The four successive swipes must be performed before the high security swipe timer expires. The default is 10 seconds.

3.4.7 Lock/Unlock Swipe Timer

If an access card with the lock/unlock privilege is swiped twice in succession, the access point toggles between locked and unlocked mode. The two successive swipes must be performed before the expiry of the lock/unlock swipe timer. The default is 10 seconds.

3.4.8 Pin Timeout

If a card is swiped during the PIN required schedule, the card holder must enter the card's PIN before the timer expires in order to gain access. The default is 20 seconds.

The PIN required feature requires a wireless device with a keypad.

3.4.9 Setting the Timer Options for an Access Point

To set the timer options for an access point

1. Find the access point in the job tree.

   If you do not see the access point in your job tree, expand the Aperio Door Controller panel entry, and then expand the panel's `Access Point` entry.

2. Click on the access point.
3. Select the **Timers** tab.
4. Set the timers for the access point.

   Detailed information these timers can be found in sections 3.4.1 to 3.4.8.

Continue with your configuration settings. After you have completed all of your configuration settings, connect to your TX3 system and send the job (see section 3.13, Sending Your Configuration, on page 98).

3.5 Advanced Options

The following advanced options can be set for each Access Point. These options are found under the `Advanced` tab for the access point.

- High security
- PC decision required
- Deduct usage count
- First person in
- Facility code mode
- Inhibit ID
- Timed Anti-passback
- Report Not Initialized
- Report request to exit
- Report unknown format
- Report door not open
- Auto relock
- RTE bypass DC
- Disable forced entry alarm
- Ignore card facility code

These options are explained in more detail in sections 3.5.1 to 3.5.15. Section 3.5.16 explains how to set these options for an access point.

3.5.1 High security

When high security is selected, only access cards with the high security privilege are able to open the door. For information on how to set the high security privilege for a card, see section 3.10.2, Editing Card Details, on page 93.

3.5.2 PC decision required

This option does not apply to ASSA ABLOY devices.

3.5.3 Deduct usage count

For cards designated as “temporary” (that is, the usage counter option is enabled and set to a value below 255), this option decreases the usage counter by one every time the card is used at the access point. When the usage counter reaches zero, the card deactivates. For information on how to set the usage counter for a card, see section 3.10.2, Editing Card Details, on page 93.

3.5.4 First person in

If an access point is configured with an `Auto-unlock` schedule, selecting `First person in` causes the access point to remain locked at the start of the `Auto-unlock` schedule. When the first valid card with the `First person in` privilege is presented to the card reader, the access point unlocks and remains unlocked for the remainder of the `Auto-unlock` schedule. For information on how to set the first person in privilege for a card, see section 3.10.2, Editing Card Details, on page 93.

3.5.5 Facility code mode

Enabling this mode grants access to cards based on only their facility code. This allows nonprogrammed cards to have complete building access. Use only when necessary.

3.5.6 Inhibit ID

When enabled, the card code is not sent to the PC. This feature is used for logging and reporting purposes.

3.5.7 Timed Anti-passback

When enabled, if a card is swiped at the same access point before the timer expires, access will not be granted.

3.5.8 Report Not Initialized

Wireless devices have sensors that should be initialized at the factory. If a wireless device is not initialized, this is detected by the Aperio hub. Select this option to have the Aperio Door Controller log and report wireless devices that are not initialized.

3.5.9 Report request to exit

This option logs and monitors events and system status. When enabled any requests to exit are logged and reported to the configurator. Since the person exiting is not known, only the time and date and the request itself is logged and reported.

3.5.10 Report unknown format

When enabled, this option logs and reports access attempts with a card with an unknown format.

3.5.11 Report door not open

When enabled, this option logs and reports when access is granted but the door remains closed.

3.5.12 Auto relock

This option does not apply to ASSA ABLOY devices.

3.5.13 RTE bypass DC

This option does not apply to ASSA ABLOY devices.

3.5.14 Disable forced entry alarm

Disabling the forced entry alarm will not activate the forced entry alarm even if the door is opened without permission. Instead, an access granted sequence is started. This is usually used on access points where there is no request to exit (RTE) device.

3.5.15 Ignore card facility code

This option is enabled by default meaning that only the card number is processed. If this option is unchecked both the card number and the facility code of the card will be processed to grant access.

3.5.16 Setting Advanced Options for an Access Point

To set the advanced options for an access point

1. Find the access point in the job tree.

   If you do not see the access point in your job tree, expand the Aperio Door Controller panel entry, and then expand the panel's `Access Point` entry.

2. Click on the access point.

3. Select the **Advanced** tab.

4. Set or clear the options for your access point.

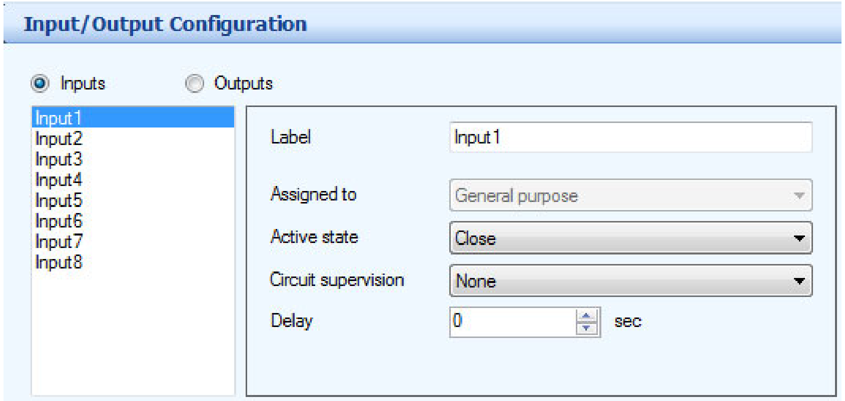
   Detailed information these timers can be found in sections 3.5.1 to 3.5.15.

Continue with your configuration settings. After you have completed all of your configuration settings, connect to your TX3 system and send the job (see section 3.13, Sending Your Configuration, on page 98).

3.6 Aperio Door Controller Inputs

Each Aperio Door Controller has eight general purpose inputs. Inputs are used in correlations (see section 3.8) to trigger an action based on the state of the input. For example, a correlation can be written to turn on one of the general purpose outputs or to turn on high security mode when an input becomes active.

To access the inputs for a panel in the TX3 Configurator, expand the panel in the job tree, select `Inputs/Outputs`, and then select the `Inputs` option in the right pane. The available inputs and settings for the inputs are shown in the right pane (see Figure 40).



Input/Output Configuration

● Inputs ○ Outputs

Input1
Input2
Input3
Input4
Input5
Input6
Input7
Input8

Label: Input1
Assigned to: General purpose
Active state: Close
Circuit supervision: None
Delay: 0 sec

Figure 40. The Inputs configuration window

Inputs 1 to 8 in Figure 40 correspond to inputs 1 to 8 on the Aperio Door Controller panel. If you connected inputs to your Aperio Door Controller panel (see section 2.4, Connecting the Inputs, on page 24), you must enter the information regarding these inputs into the TX3 Configurator. If the information is not entered into the TX3 Configurator, the panel will not be able to monitor the inputs properly.

The following options can be entered for each input:

- Label
- Assigned to
- Active state
- Circuit supervision
- Alarm delay

These options are explained in more detail in sections 3.6.1 to 3.6.5. Section 3.6.6 explains how to configure these options for an input.

3.6.1 Label

Use this option to provide a descriptive name for the input (for example, “Call security button” or “Accessible door button”).

3.6.2 Assigned to

This option is not configurable for Aperio Door Controller panels. All inputs are general purpose inputs for these panels.

3.6.3 Active state

Select the active state of the input. The options available are:

- Open
- Close

3.6.4 Circuit supervision

Select the type of supervision used on the input. This must match the type of circuit supervision installed with the input. The options available are:

- None
- Open circuit
- Short circuit
- Open and short circuit

3.6.5 Alarm delay

Alarm delay specifies the amount of time the input must be active before an alarm is raised.

3.6.6 Configuring Inputs

To configure the inputs for an Aperio Door Controller panel

1. Expand the entry for your panel in the job tree, and then select the `Inputs/Outputs` entry for the panel.

2. Select the `Inputs` option in the right pane.

3. Select an input and then set the following options for that input:

   - Label
   - Active state
   - Circuit supervision
   - Alarm delay

   Information on each of these options can be found in sections 3.6.1 to 3.6.5.

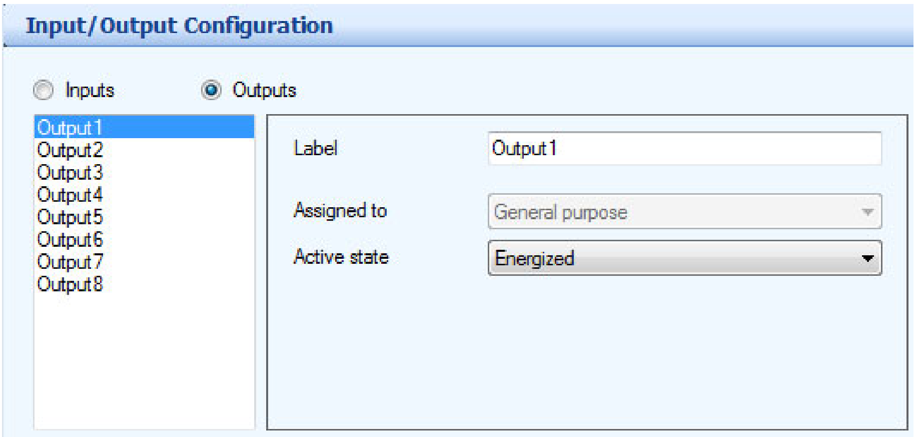
4. Repeat step 3 for all of the inputs that you have installed on your panel.

Continue with your configuration settings. After you have completed all of your configuration settings, connect to your TX3 system and send the job (see section 3.13, Sending Your Configuration, on page 98).

3.7 Aperio Door Controller Outputs

Each Aperio Door Controller has eight general purpose outputs. Outputs can be turned off or on in a correlation when an input becomes active or when an access point is in a certain state (see section 3.8). For example, a correlation can be written to turn on one of the general purpose outputs when an input becomes active or when an access point reports a forced entry alarm.

To access the outputs for a panel in the TX3 Configurator, expand the panel in the job tree, select `Inputs/Outputs`, and then select the `Outputs` option in the right pane. The available outputs and settings for the outputs are shown in the right pane (see Figure 41).



Input/Output Configuration

○ Inputs ● Outputs

Output1
Output2
Output3
Output4
Output5
Output6
Output7
Output8

Label: Output1
Assigned to: General purpose
Active state: Energized

Figure 41. The Outputs configuration window

Outputs 1 to 8 in Figure 41 correspond to outputs 1 to 8 on the Aperio Door Controller panel. If you connected outputs to your Aperio Door Controller panel (see section 2.5, Connecting the Outputs, on page 28), you must enter the information regarding these outputs into the TX3 Configurator. If the information is not entered into the TX3 Configurator, the panel will not be able to control the outputs properly.

The following information and options can be entered for each output:

- Label
- Assigned to
- Active state

These options are explained in more detail in sections 3.7.1 to 3.7.3. Section 3.7.4 explains how to configure these options for an output.

3.7.1 Label

Use this option to provide a descriptive name for the output (for example, “Aperio hub 1 power” or “Accessible door”).

3.7.2 Assigned to

This option is not configurable for Aperio Door Controller panels. All outputs are general purpose outputs for these panels.

3.7.3 Active state

Select the active state of the output. The available options are:

- Energized
- De-energized

Note: If you are using Outputs 7 and 8 to power hubs, leave them as `De-energized`.

3.7.4 Configuring Outputs

To configure the outputs for an Aperio Door Controller panel

1. Expand the entry for your panel in the job tree, and then select the `Inputs/Outputs` entry for the panel.
2. Select the `Outputs` option in the right pane.
3. Select an output and then set the following options for that input:
   - Label
   - Active state

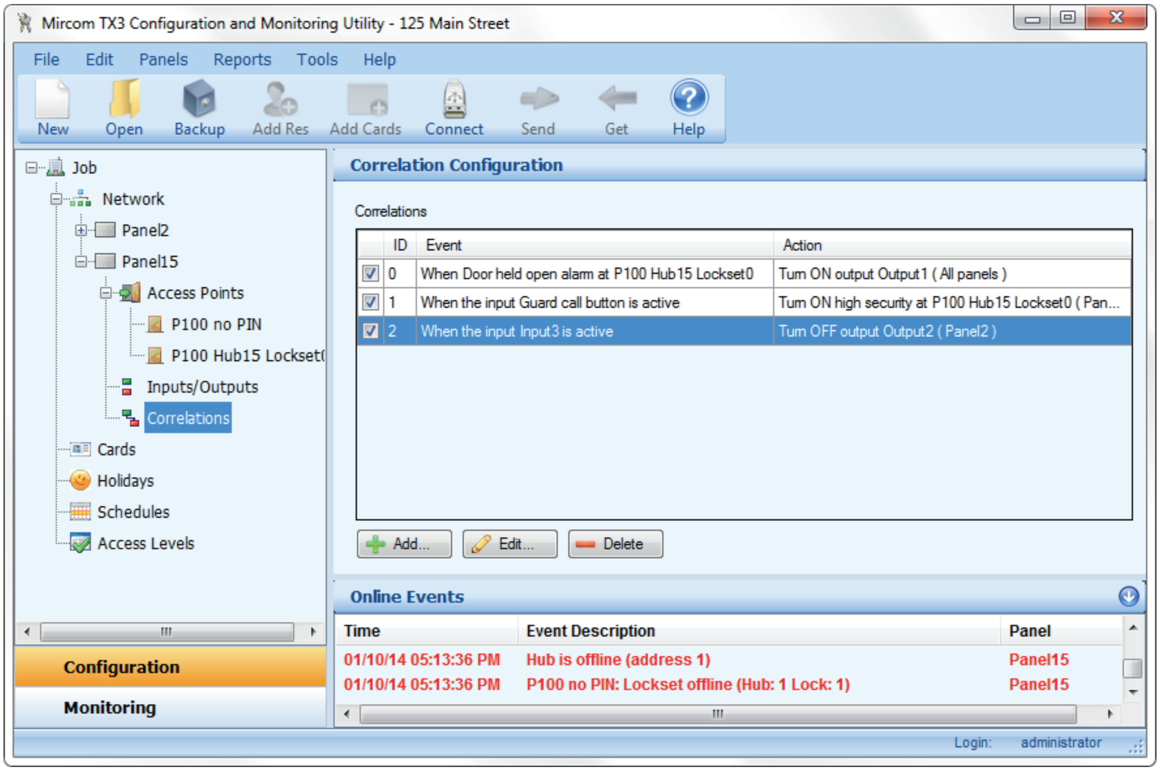
   Information on each of these options can be found in sections 3.7.1 and 3.7.3.
4. Repeat step 3 for all of the outputs that you have installed on your panel.

Continue with your configuration settings. After you have completed all of your configuration settings, connect to your TX3 system and send the job (see section 3.13, Sending Your Configuration, on page 98).

3.8 Correlations

Correlations let you establish specific relationships between events at a panel (for example, an input becomes active or an access point reports a forced entry) and the action to perform when that event happens (for example, energize an output or go into high security mode). You can also tie a correlation to a schedule, so that actions are only performed during certain days and times of the week. A maximum of 32 correlations are allowed.

To access the correlations for a panel in the TX3 Configurator, expand the panel in the job tree, and then select the `Correlations` entry for that panel. The right pane shows the Correlation Configuration window for your panel (see Figure 41). The Correlation Configuration window shows the panel's correlations, whether or not the correlation is active (that is, selected), the ID for the correlation, the event that triggers the correlation, and the action to perform when the event happens.



Correlation Configuration

Correlations

	ID	Event	Action
☑	0	When Door held open alarm at P100 Hub15 Lockset0	Turn ON output Output1 (All panels)
☑	1	When the input Guard call button is active	Turn ON high security at P100 Hub15 Lockset0 (Pan...
☑	2	When the input Input3 is active	Turn OFF output Output2 (Panel2)

Online Events

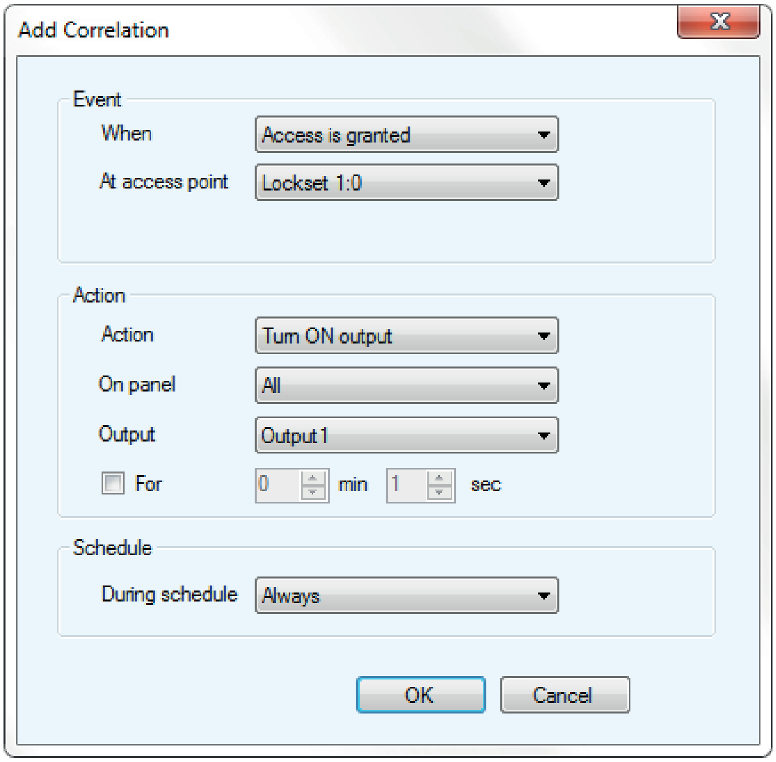
Time	Event Description	Panel
01/10/14 05:13:36 PM	Hub is offline (address 1)	Panel15
01/10/14 05:13:36 PM	P100 no PIN: Lockset offline (Hub: 1 Lock: 1)	Panel15

Figure 42. The Correlations Configuration window

The following information and options define a correlation:

- Event
- Action
- Schedule

These options are explained in sections 3.8.1 to 3.8.3. The settings for these options are made in the Add Correlation window (see Figure 43). To open the Add Correlation window, click `Add` in the Correlation Configuration window.



Event

When: Access is granted

At access point: Lockset 1:0

Action

Action: Turn ON output

On panel: All

Output: Output 1

□ For 0 min 1 sec

Schedule

During schedule: Always

Figure 43. The Add Correlation window

Section 3.8.4 explains how to add a correlation to your job.

3.8.1 Event

The `Event` section is where you define what triggers the correlation. To define an event, you have to specify the type of event (for example, access is granted at an access point or an input becomes active) and where the event happens (either an access point or an input).

To specify the type of event, make a selection from the `When` list. The choices in the `When` list are the following:

- **Access is granted** (*at an access point*)
- **Access is denied** (*at an access point*)
- **Forced entry alarm** (*at an access point*)
- **Forced entry alarm restored** (*at an access point*)
- **Door held open alarm** (*at an access point*)

- **Door held open alarm restored** (*at an access point*)
- **Door held open warning** (*at an access point*)
- **Door held open warning restored** (*at an access point*)
- **Door not open** (*at an access point*)
- **Request to Exit.** A request to exit has been made.
- **Input is active.** Select a panel input from 1 to 8.
- **Input is normal.** The general purpose input becomes inactive.
- **Unlock mode is on** (*at an access point*)
- **Unlock mode is off** (*at an access point*)
- **High security is on** (*at an access point*)
- **High security is off** (*at an access point*)
- **Tamper detected** (*at an access point*)
- **Tamper restored** (*at an access point*)
- **Battery is normal** (*at an access point*)
- **Battery is low** (*at an access point*)
- **Battery is flat** (*at an access point*)
- **Lockset is offline.** The lockset is not communicating with its Aperio hub.
- **Lockset is online.** The lockset has resumed communicating with its Aperio hub.

To specify where the event happens, you must select one of the inputs or access points on your Aperio Door Controller panel configuration. What you can select from depends on the type of event you chose:

- If you selected an event that is related to an access point, then the `At access point` list appears. This list shows all of the access points configured on your panel.
- If you selected an event that is related to an input (that is, Input is active), the `Input label` list appears. This list shows all of the inputs configured on your panel.

3.8.2 Action

The Action section is where you define what to do when an event happens. To define an action, you need to specify:

- what action to take
- where the action will happen
- for how long to perform the action.

To specify what action to take, select an action from the `Action` list. The available choices from the `Action` menu are the following:

- **Turn ON output**: turn on one or more outputs.
- **Turn OFF output**: turn off one or more outputs.
- **Turn ON high security**: turn on high security mode on one or more access points. When you turn on high security mode at an access point, only cards with the high security privilege can open the door.
- **Turn OFF high security**: turn off high security mode on one or more access points.

To specify where the action will happen, you have to choose the panel(s) and either the output(s) or the access point(s) on the panel(s).

To choose a panel, select one of the following options from the `On panel` list:

- **Panel**: choose a panel from the list of panels in your job.
- **All**: apply the correlation to all of the Aperio Door Controller panels, Card Access panels, Telephone Access panels, and Touch Screen panels in your job.
- **Custom**: apply the correlation to a custom target. This option is only available if you have a TCP/IP network connection to your TX3 system. If you select the Custom option, click the `Custom` button to open the Custom Correlation Target window, and then select the targets for your correlation. You can choose from the following targets:
  - **All nodes on the RS-485 network of the Master Node**: select a Master Node from the list. The correlation affects all of the nodes on the Master Node's RS-485 subnetwork.
  - **All Master Nodes only**: the correlation affects only the Master Nodes on your TCP/IP network.
  - **All panels with RS485 address**: select an RS-485 address from the list. The correlation affect all panels with this RS-485 address on all of the RS-485 subnetworks.

Note: Correlation signals cannot be transmitted by Touch Screen Master Nodes. If you plan on using the All or Custom correlation options, you should not have any Touch Screen Master Nodes on your network.

  - **Nano -** Apply the correlation to a TX3 Nano. This option is only available for TCP/IP network connections. When you select this option, you can click on the `Nano` button and enter the IP address of a TX3 Nano. Click `Find` to find any TX3 Nanos on the network.

After you have selected the panel(s) to apply the correlation to, you must select the output or access point that is affected by the correlation. What choices are available (that is, outputs or access points) depends on the choice you made for Action.

- If you chose either **Turn ON high security** or **Turn OFF high security** from the Action list, you will get a list of access points to choose from in the At access point list.
- If you chose either **Turn ON output** or **Turn OFF output** from the Action list, you will get a list of outputs to choose from in the Output list.

Note: If one or both of outputs 7 and 8 are used to provide power to Aperio hubs, do **not** include the output(s) in any of your correlations.

Finally, you can specify how long the action should take place. The For option lets you set the duration of the action in minutes and seconds up to a maximum of 600 minutes. To set a duration, check the For box, and then specify the min (minutes) and sec (seconds) settings. Uncheck the box if you want the action to continue indefinitely.

3.8.3 Schedule

The Schedule section lets you specify when the correlation should be active. By default, the Always schedule is selected, which means that the correlation is always applied when the event happens. However, if you want a correlation to be applied only during specific days and times (for example, during regular working hours), then you must specify that schedule.

To specify a schedule, select the schedule from the During schedule list. For a schedule to appear on this list, it must first be defined (see section 3.11, Schedules, on page 96).

3.8.4 Adding a Correlation

To add a correlation

1. Expand the entry for your panel in the job tree, and then select the Correlations entry for the panel.
2. Click Add.
3. In the Add Correlation window, set the following options for the correlation:
   - Event
   - Action

- Schedule

  Information on each of these options can be found in sections 3.8.1 to 3.8.3.

4. Click `OK`.

Continue with your configuration settings. After you have completed all of your configuration settings, connect to your TX3 system and send the job (see section 3.13, Sending Your Configuration, on page 98).

3.8.5 Changing the Active Setting on a Correlation

Correlations have an active setting. When the active setting is cleared, the correlation is deactivated will not be applied. This is useful if you want to temporarily disable a correlation without changing its settings. At a later time you can activate the correlation.

To change the active state of a correlation

1. Expand the entry for your panel in the job tree, and then select the `Correlations` entry for the panel.

2. Activate or deactivate the correlation by doing one of the following:
   - To activate a correlation, select the check box next to the correlation.
   - To de-activate a correlation, clear the check box next to the correlation.

Continue with your configuration settings. After you have completed all of your configuration settings, connect to your TX3 system and send the job (see section 3.13, Sending Your Configuration, on page 98).

3.8.6 Editing a Correlation

To edit a correlation

1. Expand the entry for your panel in the job tree, and then select the `Correlations` entry for the panel.

2. Select the correlation you want to edit.

3. Click `Edit`.

4. In the `Edit Correlation` window, set the following options for the correlation:
   - Event

- Action
- Schedule

Information on each of these options can be found in sections 3.8.1 to 3.8.3.

5. Click OK.

Continue with your configuration settings. After you have completed all of your configuration settings, connect to your TX3 system and send the job (see section 3.13, Sending Your Configuration, on page 98).

3.8.7 Deleting a Correlation

To delete a correlation

1. Expand the entry for your panel in the job tree, and then select the Correlations entry for the panel.

2. Select the correlation you want to delete.

3. Click Delete.

Continue with your configuration settings. After you have completed all of your configuration settings, connect to your TX3 system and send the job (see section 3.13, Sending Your Configuration, on page 98).

3.9 Access Levels and Elevator Control

See LT-995 on the USB flash or **http://www.mircom.com** for information on access levels and elevator control.

3.10 Cards

Select Cards from the job tree to see a list of all of the currently configured cards and their details in the Right Pane.

3.10.1 Adding a Card

To add a card, you must know the card number and facility code for the card. These are usually printed on the card. If you cannot find this information on the card, you can find the information by connecting to your TX3 system and then swiping the card at a wireless device; the online events section of the TX3 Configurator displays the card’s number and facility code. For information on how to connect to your TX3 network, see section 3.13.1, Connecting to Your TX3 System, on page 98.

To add a card

1. Select `Add Cards` from the Menu Bar or right click in the Card Configuration window and select `Add Cards`.

2. Enter the following information:

   Total number of cards to add. Specify the number of cards to add.

   Name. Provide a name for the card holder.

   Card number. Enter the card number.

   Access level. Select up to three access levels for the card.

   Facility Code. Provide the facility code for the card.

3. Click `OK`.

The new card is added to the Card Configuration window. At this point, you should configure the options for this card by editing the card details (see section 3.10.2, Editing Card Details).

Continue with your configuration settings. After you have completed all of your configuration settings, connect to your TX3 system and send the job (see section 3.13, Sending Your Configuration, on page 98).

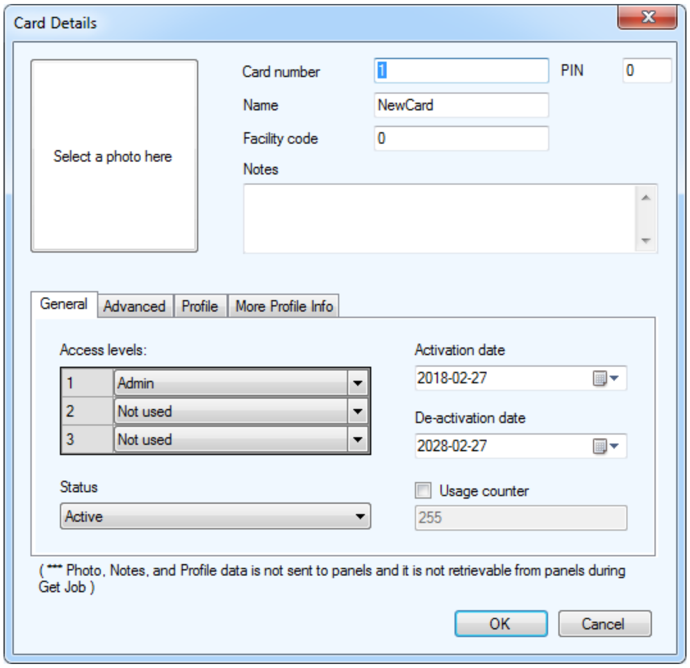
3.10.2 Editing Card Details

The Card Details window lets you set more options for each card. It is here where you can, for example, set an activation date for a card and give a card certain privileges.

To edit card details

1. Double-click on the card you want to edit.

   The Card Details window appears.



Card Details

Card number: 1

PIN: 0

Name: NewCard

Facility code: 0

Notes

Access levels:

1	Admin
2	Not used
3	Not used

Activation date: 2018-02-27

De-activation date: 2028-02-27

Status: Active

☐ Usage counter: 255

(*** Photo, Notes, and Profile data is not sent to panels and it is not retrievable from panels during Get Job)

Figure 44. The Card Details window

2. Set the following options:

   Select a photo here. Click this area and then select the card holder's photo.

   Notes. Provide any notes for this card.

   You can also change some of the information that you entered when you added the card (**Card Number**, **PIN**, **Name**, and **Facility Code**).

3. Select the **General** tab, and then set the following options:

   Access level. Select up to three access levels for the card.

   Activation date. Select the date from which the card starts to be active in the system.

   De-activation date. Select the date from which the card is no longer active on the system.

   Status. The status of the access card is marked as either:

   - Active

- Inactive

Inactive cards are not granted access. Active cards are granted access provided all the other conditions like access level and privilege are met.

Usage counter. The usage counter is used for temporary cards. Select the checkbox and specify a value from 1 to 255. Using 255 means there is no restriction on usage. If any other value is used, it means the card is only usable for that number of times.

Note: For the usage counter to function, you must select the deduct usage count option for the access point (see section 3.5.3, Deduct usage count).

4. Select the **Advanced** tab, and then set the following options:

High security privilege. When this option, the card has the following privileges:

- Opens doors in high security mode.
- Enables and disables high security mode by presenting the card four times in succession.

Extended unlock time. When this option is enabled the door opens for the extended unlock time (see section 3.4.2, Extended Unlock Time). This option is normally given to seniors and persons with mobility issues.

Ignore anti-passback. When this option is enabled the card holder is not restricted by the timed anti-passback mode.

Handicap. When this option is enabled the output designated as accessible is activated along with the main door.

Note: This option does not apply to Aperio Door Controller because all of their outputs are general purpose outputs. However, if your job contains any TX3-CX Two Card Access Controllers that have outputs designated as accessible, this option will apply for those outputs.

Lock/Unlock privilege. When this option is enabled the user has the privilege of unlocking the door by presenting the card to the reader twice in succession.

First person in. This option works only for access points with both an **Auto-unlock schedule** and the **First person in** option set. If this option is enabled, the user can set the access point to unlock mode by presenting the card during the **Auto-unlock schedule**. The access point remains unlocked until the end of the **Auto-unlock schedule**.

5. Select the **Profile** tab, and then enter the following information:

   First name. First name of the card holder.

   Last name. Last name of the card holder.

   Phone. The phone number of the card holder.

   Mobile Phone. The mobile phone number of the card holder.

   E-mail. The e-mail address of the card holder.

   Department. The business department of the card holder.

   Profile ID. *Reserved for future use*.

   Select Profile. *Reserved for future use*.

6. Select the **More profile Info** tab, and then enter the following card holder information:

   Address.

   Apt#.

   City.

   Province/State.

   Country/Region.

   Postal/zip code.

7. Click `OK`.

Continue with your configuration settings. After you have completed all of your configuration settings, connect to your TX3 system and send the job (see section 3.13, Sending Your Configuration, on page 98).

3.11 Schedules

Schedules let you set up a timetable to establish when certain actions are permitted to occur, such as door access. These schedules are designated and listed by name in the configurator software, and are available for selection wherever it is necessary to invoke access permission.

The system can store up to 64 schedules. Each schedule consists of eight periods with each period consisting of

- Start time and end time in hours: minutes format
- Days of the week and Holiday selection

Each schedule has an ID and a label to identify the schedule for use in the configurator software.

If the current time and day satisfies any one of the eight periods in a schedule, the schedule is considered to be active; otherwise, it is inactive.

By default the following two schedules cannot be edited:

- 'Always' schedule
- 'Never' schedule

Schedules are used for the following:

- Timer schedule
- Correlations
- Auto-unlock
- PIN required schedule
- Access levels

For more information on Schedules, see LT-995.

3.12 Holidays

Up to 128 holidays can be entered in the system. Each holiday consists of the following:

- start time/date
- end time/date

If a holiday falls on the same date each year it can be programmed as an annual event.

Each holiday has a holiday ID and label to identify the holiday for use in the configurator software.

By default, New Year (January 1) is already programmed into the system.

For more information on managing holidays, see LT-995.

3.13 Sending Your Configuration

Configuration changes can only be made when you are not connected to your TX3 system. Once you have finished setting your options in the TX3 Configurator, you must connect to your system and then send the job for the configuration to be programmed into the panel(s) in your system.

3.13.1 Connecting to Your TX3 System

Connecting to your TX3 system establishes a communication link between your PC and the panel(s) on your TX3 system. You must connect to the TX3 system in order to send your job and monitor the panels in your system.

To connect to your panel(s), each panel must have the same level 3 passcode. By default, this passcode is 3333. See LT-995 for more information about the passcode and how to set it (if necessary).

To connect to your TX3 system

1. Establish a physical connection to either a panel or to the TCP/IP network that your TX3 system is on. To determine the best type of physical connection, note the following:

   - If your TX3 system is either a single panel or more than one panel connected on a single RS-485 network, you can connect by USB connection to the USB connector on a panel, by connecting to the COM port on a panel, or by dialling in to a panel using a modem on your PC (the panel must have a modem card installed).
   - If your TX3 system is on a TCP/IP network, connect your PC to the TCP/IP network using an ethernet cable.

2. Click `Network` from the job tree.

3. Select the type of connection you are using from the `PC Connection` list.

   If you selected either `COM Port` or `Modem`, you must make the following configuration settings:

   `COM Port`: select the COM port number on your PC that your are using to connect to the panel.

   `Modem`: Enter the following parameters:

   - **Modem.** Select a modem currently configured on your PC.
   - **Phone #.** Provide the telephone number the panel is connected to. If necessary use a comma for a pause.

- **Extra initialization commands.** Provide any extra modem initialization commands. The characters "AT" are automatically added before the initialization commands. Refer to the manufacturer's modem documentation for additional information.

4. Click `Advanced`.

5. Enter the following parameters:

   Network passcode. The network passcode is used for logging into each panel. All panels on the network must use this passcode as their highest level passcodes.

   Network timeout. The timeout is the time the software will wait for each panel to respond to a communication command. Increasing this value may help when there are many communication errors.

6. Click `OK`.

7. Click `Connect` from the Tool Bar.

When a panel is successfully connected, a message displays in the Lower Pane Online Events indicating it is currently online. If unsuccessful, an error message appears.

3.13.2 Sending Your Job

Configuration changes made to your job must be sent to your TX3 system in order for them to be applied.

To send your job

1. If you have not already done so, connect to your TX3 system (see section 3.13.1, Connecting to Your TX3 System).

2. Click `Send` in the Tool Bar.

3.14 System Status

The controller monitors inputs for trouble and alarm conditions.

3.14.1 Common Trouble

The common trouble indicator is active when any of the following inputs receive a trouble condition:

- Any supervised input
- Power (AC and battery)

- Door held open warning
- Battery low or flat
- Lockset offline
- Hub offlline
- Lock jammed

The common trouble status clears only if all the above inputs or statuses are back in their normal states. When the common trouble status is active, the common trouble LED flashes at a slow rate.

3.14.2 Common Alarm

The common alarm status is active when any of the following inputs receive an alarm condition:

- forced entry alarm
- door held open alarm
- tamper alarm (from the device)

The common alarm status clears only if all the above inputs and statuses are back in their normal states. When the common alarm status is active, the common alarm LED flashes at a fast rate.

4 Monitoring

This chapter explains

- Monitoring
- Opening the Device Remotely
- Access Point Details

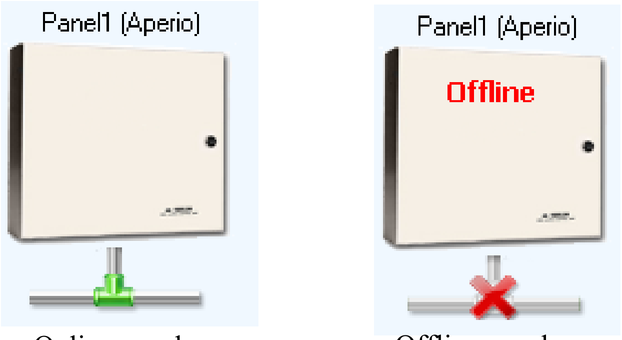
4.1 Monitoring

The TX3 Configurator has a monitoring feature that lets you check the system for problems.

1. Connect the TX3 Configurator to the Aperio Door Controller.
2. Click the `Monitoring` tab in the lower right corner of the window.

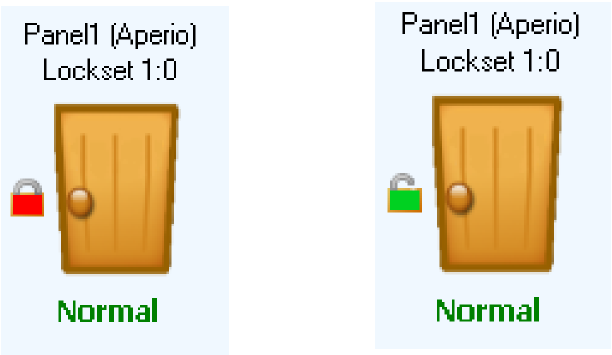
   The status of the controllers appear in the `Network Status` pane.

   The status of the locksets appear in the `Access Point Status` pane.



Online panel   Offline panel

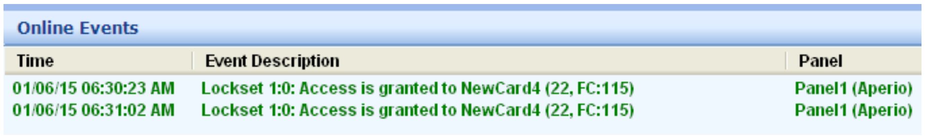
Figure 45. Online and offline panels



Access point locked   Access point unlocked

Figure 46. Access point locked and unlocked

Every time access is granted, a message appears in the Online Events pane.



Online Events

Time	Event Description	Panel
01/06/15 06:30:23 AM	Lockset 1:0: Access is granted to NewCard4 (22, FC:115)	Panel1 (Aperio)
01/06/15 06:31:02 AM	Lockset 1:0: Access is granted to NewCard4 (22, FC:115)	Panel1 (Aperio)

Figure 47. Online Events

4.2 Opening the Device Remotely

If the lockset is configured for Remote Open (section 2.7.4 on page 49), you can open the lock from the Configurator software.

1. Connect the TX3 Configurator to the Aperio Door Controller.
2. Click the `Monitoring` tab in the lower right corner of the window.
3. Click `Access Point Status` in the left pane.
4. Select the access point, and then select `Unlock mode ON` from the menu.

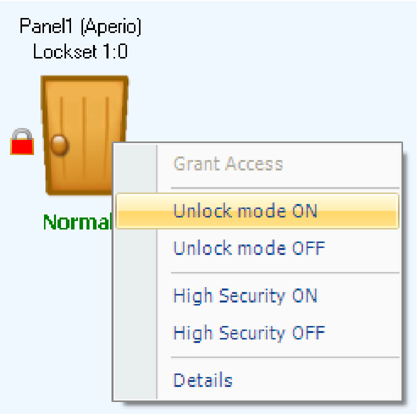


Figure 48. Unlock mode ON

Note: The lockset unlocks and stays unlocked until you turn the Unlock mode off.

5. To lock the door, select the access point, and then select `Unlock mode OFF`.

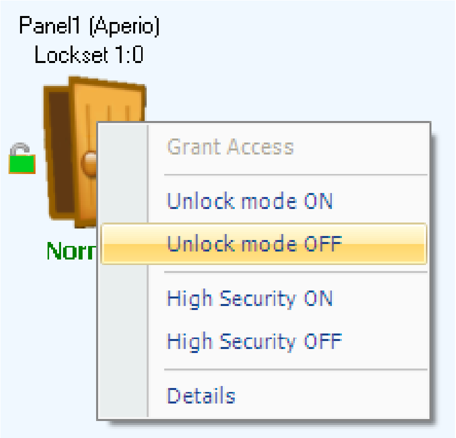


Figure 49. Unlock mode OFF

4.3 Access Point Details

Right-click the access point and select `Details` to get information about the device.

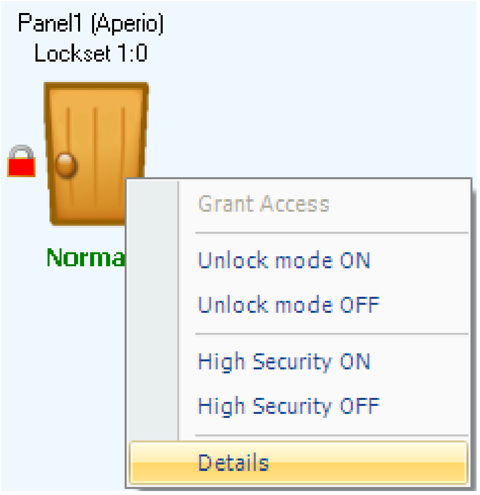
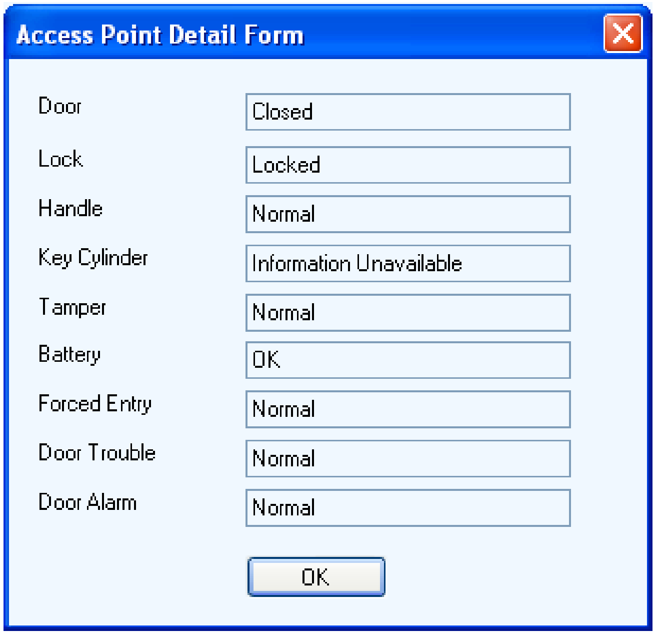


Figure 50. Access Point Details



Door	Closed
Lock	Locked
Handle	Normal
Key Cylinder	Information Unavailable
Tamper	Normal
Battery	OK
Forced Entry	Normal
Door Trouble	Normal
Door Alarm	Normal

Figure 51. Access Point Detail Form

- **Door:** Indicates if the door is closed or open.
- **Lock:** Indicates if the door is locked or unlocked.
- **Handle:** Indicates if the handle is in normal position or turned.
- **Key Cylinder:** This is not used.
- **Tamper:** Indicates if the lock has been tampered with.
- **Battery:** Indicates the lock’s battery life.
- **Forced Entry:** A forced entry message appears if the door is open but the lock is still locked. Some locks require an external door sense device in order to sense this.
- **Door Trouble:** A trouble message appears when the Door Held Open Warning timer expires and the door is still open.
- **Door Alarm:** An alarm message appears when the Door Held Open Alarm timer expires and the door is still open.

These messages also appear in the `Online Events` pane.

5 Warranty and Warning Information

WARNING!

Please read this document **CAREFULLY**, as it contains important warnings, life-safety, and practical information about all products manufactured by the Mircom Group of Companies, including Mircom and Secutron branded products, which shall include without limitation all fire alarm, nurse call, building automation and access control and card access products (hereinafter individually or collectively, as applicable, referred to as "**Mircom System**").

NOTE TO ALL READERS:

1. **Nature of Warnings.** The within warnings are communicated to the reader out of an abundance of caution and create no legal obligation for Mircom Group of Companies, whatsoever. Without limiting the generality of the foregoing, this document shall NOT be construed as in any way altering the rights and obligations of the parties, governed by the legal documents that apply in any given circumstance.

2. **Application.** The warnings contained in this document apply to all Mircom System and shall be read in conjunction with:

   a. the product manual for the specific Mircom System that applies in given circumstances;

   b. legal documents that apply to the purchase and sale of a Mircom System, which may include the company's standard terms and conditions and warranty statements;

   c. other information about the Mircom System or the parties' rights and obligations as may be application to a given circumstance.

3. **Security and Insurance.** Regardless of its capabilities, no Mircom System is a substitute for property or life insurance. Nor is the system a substitute for property owners, renters, or other occupants to act prudently to prevent or minimize the harmful effects of an emergency situation. Building automation systems produced by the Mircom Group of Companies are not to be used as a fire, alarm, or life-safety system.

NOTE TO INSTALLERS:

All Mircom Systems have been carefully designed to be as effective as possible. However, there are circumstances where they may not provide protection. Some reasons for system failure include the following. As the only individual in contact with system users, please bring each item in this warning to the attention of the users of this Mircom System. Failure to properly inform system end-users of the circumstances in which the system might fail may result in over-reliance upon the system. As a result, it is imperative that you properly inform each customer for whom you install the system of the possible forms of failure:

4. **Inadequate Installation.** All Mircom Systems must be installed in accordance with all the applicable codes and standards in order to provide adequate protection. National standards require an inspection and approval to be conducted by the local authority having jurisdiction following the initial installation of the system and following any changes to the system. Such inspections ensure installation has been carried out properly.
5. **Inadequate Testing.** Most problems that would prevent an alarm a Mircom System from operating as intended can be discovered by regular testing and maintenance. The complete system should be tested by the local authority having jurisdiction immediately after a fire, storm, earthquake, accident, or any kind of construction activity inside or outside the premises. The testing should include all sensing devices, keypads, consoles, alarm indicating devices and any other operational devices that are part of the system.

NOTE TO USERS:

All Mircom Systems have been carefully designed to be as effective as possible. However, there are circumstances where they may not provide protection. Some reasons for system failure include the following. The end user can minimize the occurrence of any of the following by proper training, testing and maintenance of the Mircom Systems:

6. **Inadequate Testing and Maintenance.** It is imperative that the systems be periodically tested and subjected to preventative maintenance. Best practices and local authority having jurisdiction determine the frequency and type of testing that is required at a minimum. Mircom System may not function properly, and the occurrence of other system failures identified below may not be minimized, if the periodic testing and maintenance of Mircom Systems is not completed with diligence and as required.
7. **Improper Operation.** It is important that all system users be trained in the correct operation of the alarm system and that they know how to respond when the system indicates an alarm. A Mircom System may not function as intended during an emergency situation where the user is

unable to operate a panic or emergency switch by reason of permanent or temporary physical disability, inability to reach the device in time, unfamiliarity with the correct operation, or related circumstances.

8. **Insufficient Time.** There may be circumstances when a Mircom System will operate as intended, yet the occupants will not be protected from the emergency due to their inability to respond to the warnings in a timely manner. If the system is monitored, the response may not occur in time enough to protect the occupants or their belongings.

9. **Carelessness or Safety Hazards.** Moreover, smoke detectors may not provide timely warning of fires caused by carelessness or safety hazards such as smoking in bed, violent explosions, escaping gas, improper storage of flammable materials, overloaded electrical circuits or children playing with matches or arson.

10. **Power Failure.** Some Mircom System components require adequate electrical power supply to operate. Examples include: smoke detectors, beacons, HVAC, and lighting controllers. If a device operates only by AC power, any interruption, however brief, will render that device inoperative while it does not have power. Power interruptions of any length are often accompanied by voltage fluctuations which may damage Mircom Systems or other electronic equipment. After a power interruption has occurred, immediately conduct a complete system test to ensure that the system operates as intended.

11. **Battery Failure.** If the Mircom System or any device connected to the system operates from batteries it is possible for the batteries to fail. Even if the batteries have not failed, they must be fully charged, in good condition, and installed correctly. Some Mircom Systems use replaceable batteries, which have a limited life-span. The expected battery life is variable and in part dependent on the device environment, usage and type. Ambient conditions such as high humidity, high or low temperatures, or large temperature fluctuations may reduce the expected battery life. Moreover, some Mircom Systems do not have a battery monitor that would alert the user in the event that the battery is nearing its end of life. Regular testing and replacements are vital for ensuring that the batteries function as expected, whether or not a device has a low-battery monitor.

12. **Physical Obstructions.** Motion sensors that are part of a Mircom System must be kept clear of any obstacles which impede the sensors' ability to detect movement. Signals being communicated by a Mircom System may not reach the receiver if an item (such as metal, water, or concrete) is placed on or near the radio path. Deliberate jamming or other inadvertent radio signal interference can also negatively affect system operation.

13. **Wireless Devices Placement Proximity.** Moreover all wireless devices must be a minimum and maximum distance away from large metal objects, such as refrigerators. You are required to consult the specific Mircom System manual and application guide for any maximum distances required between devices and suggested placement of wireless devices for optimal functioning.

14. **Failure to Trigger Sensors.** Moreover, Mircom Systems may fail to operate as intended if motion, heat, or smoke sensors are not triggered.

    a. Sensors in a fire system may fail to be triggered when the fire is in a chimney, walls, roof, or on the other side of closed doors. Smoke and heat detectors may not detect smoke or heat from fires on another level of the residence or building. In this situation the control panel may not alert occupants of a fire.

    b. Sensors in a nurse call system may fail to be triggered when movement is occurring outside of the motion sensors' range. For example, if movement is occurring on the other side of closed doors or on another level of the residence or building the motion detector may not be triggered. In this situation the central controller may not register an alarm signal.

15. **Interference with Audible Notification Appliances.** Audible notification appliances may be interfered with by other noise sources such as stereos, radios, televisions, air conditioners, appliances, or passing traffic. Audible notification appliances, however loud, may not be heard by a hearing-impaired person.

16. **Other Impairments.** Alarm notification appliances such as sirens, bells, horns, or strobes may not warn or waken a sleeping occupant if there is an intervening wall or door. It is less likely that the occupants will be alerted or awakened when notification appliances are located on a different level of the residence or premise.

17. **Software Malfunction.** Most Mircom Systems contain software. No warranties are provided as to the software components of any products or stand-alone software products within a Mircom System. For a full statement of the warranties and exclusions and limitations of liability please refer to the company's standard Terms and Conditions and Warranties.

18. **Telephone Lines Malfunction.** Telephone service can cause system failure where telephone lines are relied upon by a Mircom System. Alarms and information coming from a Mircom System may not be transmitted if a phone line is out of service or busy for a certain period of time. Alarms and information may not be transmitted where telephone lines have been compromised by criminal tampering, local construction, storms or earthquakes.

19. **Component Failure.** Although every effort has been made to make this Mircom System as reliable as possible, the system may fail to function as intended due to the failure of a component.

20. **Integrated Products.** Mircom System might not function as intended if it is connected to a non-Mircom product or to a Mircom product that is deemed non-compatible with a particular Mircom System. A list of compatible products can be requested and obtained.

Warranty

Purchase of all Mircom products is governed by:

https://www.mircom.com/product-warranty

https://www.mircom.com/purchase-terms-and-conditions

https://www.mircom.com/software-license-terms-and-conditions