

# ***XPressEntry***

## **XPressEntry / Avigilon Unity Access**

**Revision 03/19/2024**

For use with the  
XPressEntry Mobile Access Control System

By



## **Important Notice**

Your right to copy XPressEntry software and this manual is limited by copyright laws. Making copies, adaptations, or compilation works (except copies of XPressEntry software for archival purposes as an essential step in the utilization of the program in conjunction with the equipment), without prior written authorization of Telaeris, Inc., is prohibited by law and constitutes a punishable violation of the law.

This software and documentation are copyrighted by Telaeris, Inc. The software and documentation are licensed, not sold, and may be used or copied only in accordance with the Telaeris License Agreement accompanying the software.

© 2024 Telaeris, Inc.

All rights reserved worldwide.

Information in this document is subject to change without notice.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, scanning, digitizing, or otherwise, without the prior written consent of Telaeris, Inc.

### **Trademark Acknowledgements**

XPressEntry is a trademark of Telaeris, Inc.

Other company and product names may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Telaeris, Inc.

4101 Randolph Street

San Diego, California 92103

United States of America

(858) 627-9700

[www.telaeris.com](http://www.telaeris.com)

## Contents

Purpose.....	4
Requirements .....	4
Overall Order of Operations .....	4
Setting up Unity Access to Synchronize with XPressEntry .....	4
Create Event Push Collaboration .....	4
Sync Historical Activities .....	5
Real-Time Events in Avigilon .....	6
Badge Scans .....	6
Identity Updates .....	7
Set up Areas + Doors .....	7
Door Permissions .....	8
Enabling Data Manager Synchronization in XPressEntry .....	8
Data Manager Tab .....	9
Sync Timers .....	9
Sync Options .....	11
Avigilon Unity Access Setup Page .....	12

## Purpose

This document is intended to instruct system administrators on how to synchronize an XPressEntry system with the Avigilon Unity Access (ACM) access control system.

## Requirements

It is assumed that a version of Avigilon ACM and XPressEntry are installed on computers or virtual machines that can talk to each other the same computer or virtual machine. To install XPressEntry, you should have Administrator privileges on its respective machine. You should additionally be an Administrator or super user in the Avigilon Unity Access (ACM) system.

1. XPressEntry 3.5+
2. ACM Version 6.0+ (including Unity Access)
3. Windows 7 / 8 / 8.1 / 10 or server type equivalent
4. Avigilon Reader Licenses
5. Collaborations: Events – Generic XML
6. REST API

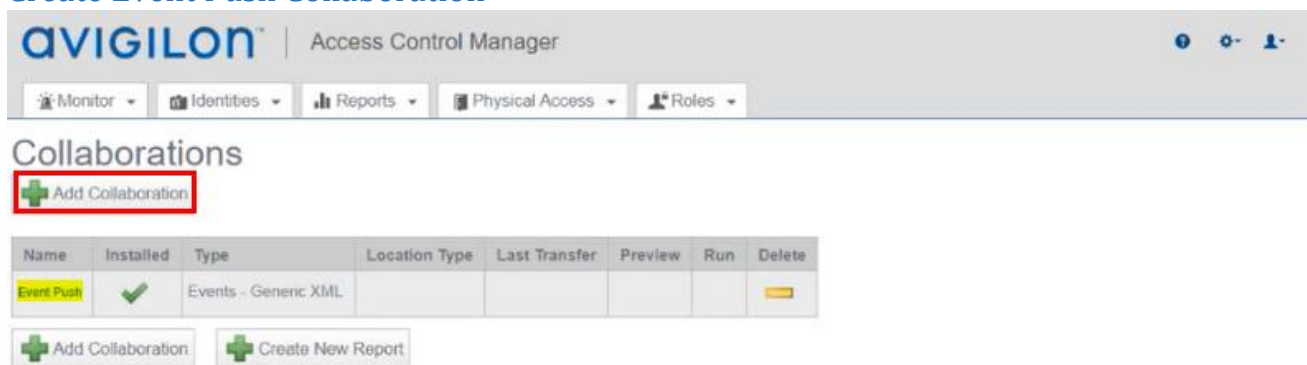
## Overall Order of Operations

1. Setting up Unity Access (ACM) to Synchronize with XPressEntry
2. Enabling Data Manager Synchronization in XPressEntry
3. Configuring XPressEntry Using Avigilon Unity Access Data

## Setting up Unity Access to Synchronize with XPressEntry

It is assumed that Avigilon Unity Access is installed on a server. XPressEntry has been tested with Avigilon ACM Versions 6.0+. Please contact Telaeris to confirm compatibility with integrations into other versions of ACM.

## Create Event Push Collaboration



Set up a Collaboration for an Event Push. This engages two features:

1. Provides **badge scans** live in XPressEntry
2. Changes to **Identities** come in live to XPressEntry (i.e., changing a name, validating a badge, access, etc.)

**Collaboration: Edit**

XML Events

Name: Event Push

Appliance: Avigilon-vm

Type: Events - Generic XML

☒ Installed

Partitions: East Coast, West Coast

Host: 10.10.245.11 ☒ Require TCP

Port Number: 5544

☒ Save ☐ Cancel Changes

To create an Event Push:

1. Add **Collaboration**
2. Set Name as **Event Push**
3. Select Collaboration Type as **Events – Generic XML**
4. Input the Host IP – this will be the **XPressEntry** host IP
5. Add a **Port Number** – the number *must match* in the Avigilon Data Manager setup in XPressEntry and in the Avigilon Access Control Manager.
  - a. Ensure the firewall is open
6. Navigate to the **Events** tab on the Event Push and ensure **User Audit** and **Valid Credential** are selected.

Avigilon ACM Data Manager Setup

General Custom Mapping

Server: avigilon.ad.telara.com

Port: 443

User: admin

Password: \*\*\*\*\*

☐ Validate SSL Certificate ☒ Use SSL

☒ Verbose API Data

XML Events Port: 5544

From Area: Offsite

To Area: San Diego Onsite

Status

## Sync Historical Activities

We will now set up the Avigilon Appliance. Go to the wheel at the top right of the access control manager and select **Setup & Settings > Appliance**.

**Appliance: Edit**

Appliance Access Ports Replication Backups Logs Software Update SSL Certificate About

Appliance Name: Avigilon-vm

System Name: avigilon-vm

Host Name: avigilon-vm

Name Server: 10.10.1.3

Time Server:

Time Zone: America - Los Angeles

☐ Hot Standby

☐ Enable Remote TCP/IP Management

Authorization Code:

Splunk URL:

APB reset Reboot Appliance Shutdown Appliance

Uptime: 5 days 3 hours 59 minutes 38 seconds

Appliance Time: 03/11/2024 16:30:09

Set Date/Time

Max Stored Transactions: 1000000

Max Days Stored:

Hardware Type: Professional

Web Server Port: 443

Alarm Gateway Port:

Edge Listen Port:

LDAP Connect Port:

Transactions Connect Port: 1670

Mercury Client Port:

☒ Mercury Require TLS

☐ Mercury Require Certificate

1. Define the **Transactions Connect Port**
  - a. This is used to pull **historical activities** from Avigilon
  - b. Must match in Avigilon Data Manager Setup
2. The database in Avigilon Data Manager must be **TransactionDB**.
3. Server will be your Avigilon server or server IP.

PostGRE Transactions Connection Settings

Server:	avigilo\ad.telearts.com
Port:	670
Database:	TransactionDB
Username:	admin
Password:	*****

## Real-Time Events in Avigilon

### Badge Scans

Once a Full Sync is run in XPressEntry and the data manager is successfully setup, you will see badge scans from the XPressEntry handheld devices or Avigilon readers populate in real-time under **Monitor > Events**.

**avigilon** | Access Control Manager


Monitor | Identities | Reports | Physical Access | Roles

Events | Search | Alarms | Verification | Dashboard | Maps | Intrusion Status

Pause | Clear | Live Video | Recorded Video | Notes | Instructions | Identity | History | Save Settings | Select Columns

Icon	Priority	Panel Time	Event Name	Source	Last Name	First Name	Internal Token No
	100	03/11/2024 16:33:34	Local Grant	WestCoast In	Dagohoy	Allen	930
	100	03/11/2024 16:33:28	Local Grant	WestCoast In	Rivers	Caleb	717
	100	03/11/2024 16:33:19	Local Grant	WestCoast Out	Rivers	Caleb	717
	100	03/11/2024 16:33:12	Local Grant	WestCoast Out	Dagohoy	Allen	930

All Zones (Occupancy: 2)




Dagohoy, Allen

Entered: 03/11 04:33:34 PM

Time In Zone: 00:00:00

Badge #: 930

Zone: San Diego Onsite



Rivers, Caleb

Entered: 03/11 04:33:28 PM

Time In Zone: 00:00:05

Badge #: 717

Zone: San Diego Onsite

**Occupancy** pulled is based off **live events/activities** in Avigilon and how the **doors** are set up in Avigilon.

## Identity Updates

Any changes to **user data** in Avigilon also update in XPressEntry. In the example below, you will see how changing the last name of a badge holder identity in **Avigilon** also updates the last name of the badge holder in **XPressEntry > Add/Edit Info**.

The screenshot shows the 'Identity: Edit' form in Avigilon. The 'Identity Information' section has 'Last Name' set to 'Adamson' and 'First Name' set to 'Jake'. The 'Account Information' section has 'Login' set to 'jake@gmail.com'. The 'Address Information' section is empty. The 'Partitions' section shows 'East Coast' and 'West Coast'. The 'Remote Authentication?' checkbox is checked. The 'Allow Remote Access?' checkbox is checked. The 'Add Identity' button is highlighted. The 'Add/Edit Info' button is highlighted. The 'Add Identity' button is highlighted. The 'Add Identity' button is highlighted.

## Set up Areas + Doors

**Doors** and **Areas** are set up in the **Physical Access** section of the Avigilon Access Control Manager. Please refer to the [Avigilon ACM setup documentation](#) on how to set these items up.

The screenshot shows the Avigilon Access Control Manager interface. The 'Physical Access' section is selected. The 'Doors' tab is active, showing a list of doors. The 'Areas' tab is active, showing a list of areas. The 'Area: Edit' form is open, showing the 'Name' field set to 'San Diego Onsite'. The 'Appliance' field is set to 'Avigilon-vm'. The 'Maximum Occupancy' field is set to 20. The 'Log Min Reached' field is set to 0. The 'Log Max Reached' field is set to 0. The 'Partitions' field is set to 'East Coast' and 'West Coast'. The 'Doors In' field is set to 'WestCoast In XPE Test Door 1'. The 'Doors Out' field is set to 'WestCoast Out -'. The 'Add Area' button is highlighted. The 'Add Area' button is highlighted. The 'Add Area' button is highlighted. The 'Add Area' button is highlighted.

Name	Appliance	Enabled	Door Count	Delete
San Diego Onsite	Avigilon-vm	Yes	3	
Office	Avigilon-vm	Yes	1	
Outside	Avigilon-vm	Yes	0	
Building	Avigilon-vm	Yes	0	
Lab	Avigilon-vm	No	0	



## Door Permissions

1. Ensure there are **two** doors for each area (one representing IN and one representing OUT)
2. Under **Door > Operations** assign whether this door represents the entry or the exit of a defined area. See below pictures for important fields to set.

The screenshot shows the 'Door: Edit' window in the Avigilon Access Control Manager. The 'Name' field is set to 'EastCoast In'. The 'Partitions' dropdown is set to 'East Coast'. The 'Panel' dropdown is set to 'East Coast Bldg 1'. The 'Into Area' dropdown is set to 'East Coast Building'. The 'Out of Area' dropdown is set to 'Don't Care'. The 'LED Mode' is set to '1'. The 'Held Pre-Alarm' is set to '5'. The 'Access time when open' is set to '5'. The 'Standard Access Time' is set to '10'. The 'Held Open Time' is set to '30'. The 'Extended Access' is set to '10'. The 'Extended Held Open Time' is set to '60'. The 'Strike Mode' is set to 'Cut short when open'. The 'Simple Macros' section shows a '24 Hours Active' macro. The 'Save' button is highlighted.

The screenshot shows the 'Door: Edit' window in the Avigilon Access Control Manager. The 'Name' field is set to 'EastCoast Out'. The 'Partitions' dropdown is set to 'East Coast'. The 'Panel' dropdown is set to 'East Coast Bldg 1'. The 'Into Area' dropdown is set to 'Don't Care'. The 'Out of Area' dropdown is set to 'East Coast Building'. The 'LED Mode' is set to '1'. The 'Held Pre-Alarm' is set to '5'. The 'Access time when open' is set to '5'. The 'Standard Access Time' is set to '10'. The 'Held Open Time' is set to '30'. The 'Extended Access' is set to '10'. The 'Extended Held Open Time' is set to '60'. The 'Strike Mode' is set to 'Cut short when open'. The 'Simple Macros' section shows a '24 Hours Active' macro. The 'Save' button is highlighted.

## Enabling Data Manager Synchronization in XPressEntry

XPressEntry uses a module called **Data Manager** to synchronize all data with Unity Access (ACM). From the main page of XPressEntry, go to **XPressEntry > Settings** (ALT+S or Tools > Settings).

The screenshot shows the XPressEntry interface. The 'Zones / Doors' section on the left lists 'All Zones (17)', 'Building A (7)', 'Building B (0)', 'Main Lobby (10)', 'Door A', 'Door B', 'The Yard (0)', and 'Bus 123'. The 'All Zones (Occupancy: 17)' section displays a grid of 17 users with their photos, names, and entry details. The 'Activity Occurring in Last Day' section shows a table of activity.

User	User Image	Time Stamp	Start Zone	End Zone	Door	Reader	Entry Granted
Mcgee, Adan		03/13 03:00:11 PM	Outside	Main Lobby	Main Door	Handheld 2	True
Mora, Juliana		03/13 03:00:08 PM	Outside	Main Lobby	Main Door	Handheld 2	True
Frazier, Emma		03/13 03:00:06 PM	Outside	Main Lobby	Main Door	Handheld 2	True
Benjamin, Cody		03/13 03:00:03 PM	Outside	Main Lobby	Main Door	Handheld 2	ACCESS DENIE...



## Data Manager Tab

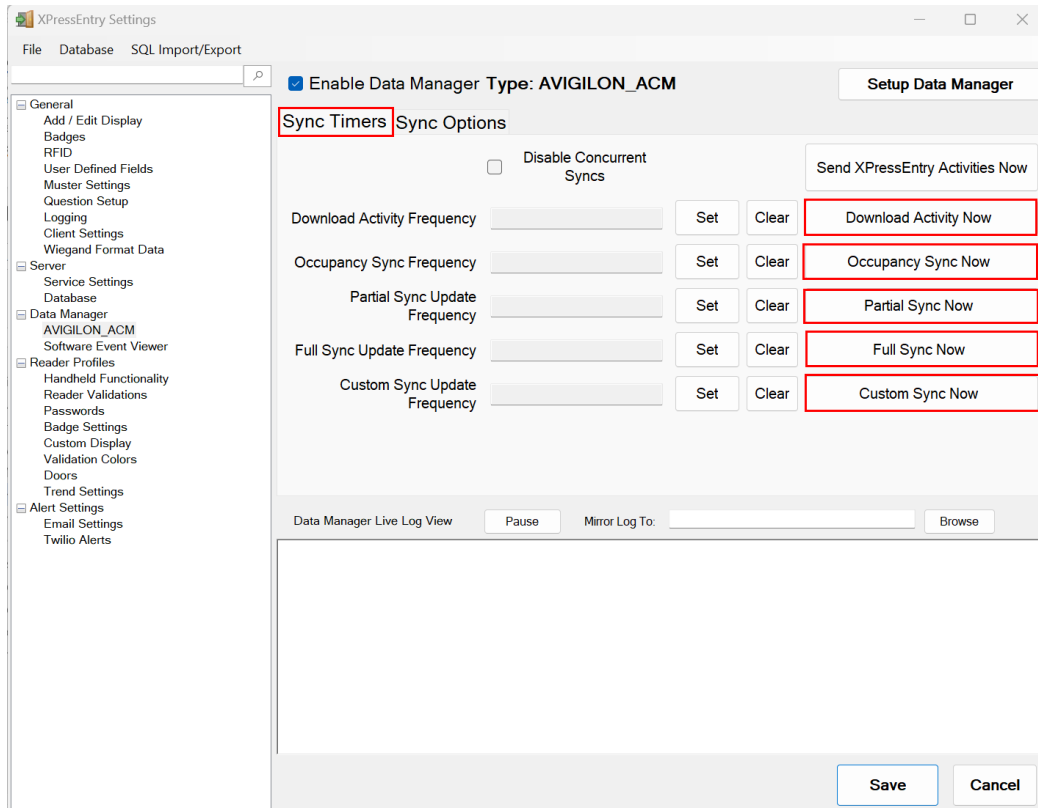
From the Settings page select the Data Manager Tab.

The screenshot shows the 'XPressEntry Settings' window with the 'Data Manager' tab selected in the sidebar. The sidebar menu includes categories like General, Server, Data Manager, Reader Profiles, and Alert Settings. Under 'Data Manager', 'AVIGILON\_ACM' is highlighted. The main area shows a form for adding a new integration type. The 'Type' dropdown is set to 'AVIGILON\_ACM'. The 'Name' field contains 'AVIGILON\_ACM' and the 'Prefix' field is empty. Below these fields is a text area containing 'AVIGILON\_ACM - Prefix()'. At the bottom right, there are 'Save' and 'Cancel' buttons, with a red arrow pointing to the 'Save' button. A 'Sanity Check Data' button is also visible above the 'Save' and 'Cancel' buttons.

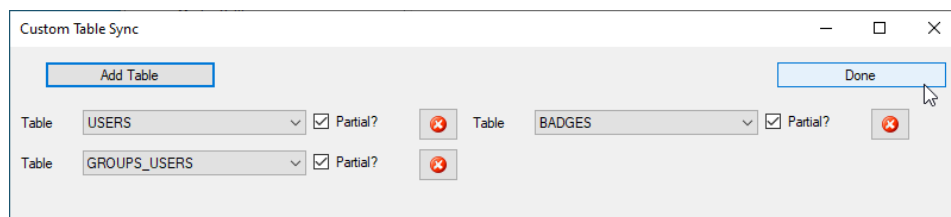
1. **Type** – This is the integration type. Select **AVIGILON\_ACM** > **Add** > **Save**.
2. Go to **Data Manager** > **AVIGILON\_ACM** in sidebar menu.
3. **Setup Data Manager** – This sends you to the setup form for Avigilon's data manager.

## Sync Timers

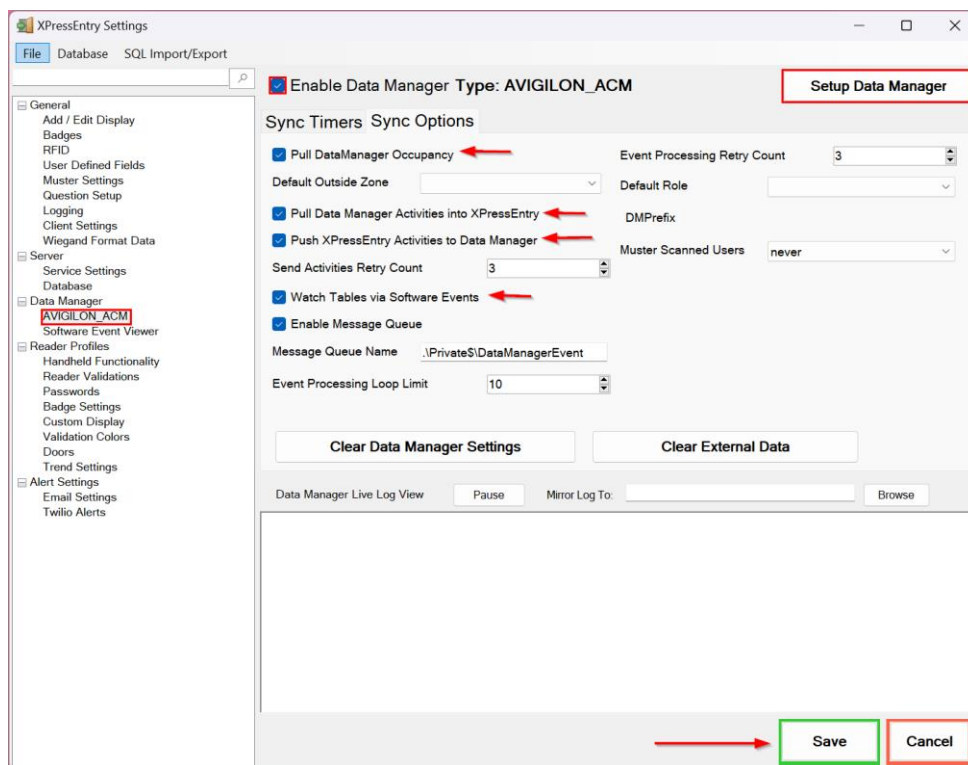
XPressEntry uses Timers to pull Avigilon Unity Access (ACM) Data into XPressEntry.



1. **Download Activity Frequency** – Pulls reader scan records into XPressEntry and stores them in XPressEntry’s activity table. This function also updates the zone occupancy.
2. **Occupancy Sync Frequency** – Updates the zone occupancy without storing the activity records.
3. **Partial Sync Frequency** – Pulls all data excluding cardholder data, including readers, areas, access levels.
4. **Full Sync Update Frequency** – Updates all tables by pulling all necessary records from Unity Access (ACM). This function may take some time.
  - a. It is recommended to run a full sync **once per day** in the middle of the night when the system is not busy.
5. **Custom Sync Frequency** – Updates a set of tables that the user configures.
  - a. To configure, right click **Custom Sync Now** and select **Edit Custom Sync**.



## Sync Options



1. **Pull Data Manager Occupancy** – Enables use of the Occupancy Sync.
2. **Pull Data Manager Activities into XPressEntry** – Enables use of the Activity Sync.
3. **Push XPressEntry Activities to Data Manager** – Enables XPressEntry to push Scan data to Avigilon .
4. **Send Activities Retry Count** – Number of times XPressEntry will attempt to resend an activity if it fails.
5. **Watch Tables via Software Events** – Creates a live data connection to the Access Control System to watch for system changes.
6. **Enable Message Queue** – Turns on Message Queue for software events to be used instead of database queue.
7. **Message Queue Name** – Name of windows message queue for software events.
8. **Event Processing Loop limit** – Max records to process from event queue.
9. **Event Processing Retry Count** – Number of times XPressEntry will attempt to process a message queue event on failure.
10. **Default Role** – The default XPressEntry Role that will be assigned to users if the integration does not otherwise assign a role. Entrants are recommended but not required.
11. **Muster Scanned Users** – Enables sync to convert scans from specific readers to be converted into Muster Scans which mark users as safe. Muster readers must be configured in the reader data. Please see ***Mustering Documentation*** for more details.
12. **Setup DataManager Button** – Opens Unity Access (ACM) specific settings.
13. **Clear DataManager Settings** – Resets all settings on the two above tabs, as well as the Unity Access (ACM) specific settings.
14. **Clear External Data** – Deletes all data synced from Unity Access (ACM) from the XPressEntry Database

## Avigilon Unity Access Setup Page

Avigilon ACM Data Manager Setup

General Custom Mapping

Server: avigilon.ad.telaeris.com

Port: 443

User: admin

Password: ••••••••

☐ Validate SSL Certificate ☒ Use SSL

☐ Verbose API Data

XML Events Port: 5544

Doors From Area  
Outside

Doors To Area  
Main Lobby

☒ Partial Sync Modified Identities

☒ Use Local Grant for Activity Success

Test Connect Defaults OK

Status

PostGRE Transactions Connection Settings

Server: avigilon.ad.telaeris.com

Port: 1670

Database: TransactionDB

Username: admin

Password: ••••••••

1. **Server** – IP address of the system where Avigilon server is hosted.
2. **User** – Avigilon admin username
3. **Password** – Avigilon admin user password
4. **XML Events Port** – This port number must match what is listed in the Collaborations Events Push XML within the Avigilon access control manager.
5. **Partial Sync Modified Activities** – Check this to ensure a partial sync will use a last updated date to grab any identities that were modified since they were last pulled.
6. **PostGRE Transactions Connection Settings**
  - a. **Server** – IP address of the system where Avigilon server is hosted.
  - a. **Port** – This is used to pull historical activities from Avigilon. It must match what is defined in the **Transactions Connect Port** field under **Appliance** in the Avigilon access control manager.
  - b. **Database** – Must be TransactionDB

Click **Test Connect** after entering all the data correctly. This will connect to the Avigilon Unity Access (ACM) system using the given username and password.

The result will display **Connection Success!** if connected to Avigilon successfully. If there is any error in the connection it will show in the same result window.

Exit out of this form. On the Data Manager tab of the Settings form, select **Save**. It is now time to begin syncing data.

## Configuring XPressEntry Using Avigilon Unity Access Data

Now that XPressEntry has been synchronized with the Avigilon database, it needs to be configured to use this information. The tabs that need to be configured are the Doors, Readers, and Zones.

In the XPressEntry system, editing of any external data is **disabled by default**. To enable the settings, go to **XPressEntry Settings > General Tab > Add/Edit Display** then check the option **Allow Editing of External Data** in the External Data Section.

### Configuring Doors

Entry/Exit permissions in XPressEntry are set by doors. Doors contain **two** readers – an **exit** and an **entry** reader. Door access is determined by the User's access to the door's reader.

- For **entry**, permission is based on the user's access to the door's **external entry reader**.
- For **exit**, permission is based on the user's access to the door's **external exit reader**.

Doors should be set by the user for each Handheld Reader in XPressEntry.

The XPressEntry Integration with Avigilon can use **Areas** assigned in Avigilon as **Zones**.

The screenshot shows the 'Door: Edit' configuration page in the Avigilon Access Control Manager. The 'Parameters' tab is active. Key fields include: Name (East Coast Out), Partitions (East Coast, West Coast), Panel (East Coast Bldg 1), Vendor (Mercury Security), and a list of Card Formats (26 bit weigand, 34 bit weigand, 37 bit HID10304, 35 bit Corporate Format, 56 bit Avigilon). The 'Simple Macros' section at the bottom allows for scheduling (24 Hours Active) and output configuration.

1. **Zones** – For each door, set the **start** zone and **end** zone in **Avigilon**. This will “enter” a user in the specified zone when they enter or exit (or scan at an Avigilon door/panel).
2. **External Readers** – The External Entry Reader is automatically set to the **Panel** that is associated from the **door**.
  - a. If no panel is associated, default to a respective XPressEntry handheld reader.

There should be a door in XPressEntry for **each** physical station that an employee will have a handheld.

Doors can also be added for each of the physical readers. If XPressEntry is set up to pull activities, it will move people in the system based on the reader they were scanned at and the zones attached to the door.

## Configuring Readers

In XPressEntry's Avigilon integration, it is not necessary to associate any reader in the system with a handheld. This association can be done on the handheld when it comes time to scan.

A handheld unit can logically represent any reader in the building. When the handheld is issued to an employee at a specific door, the employee must first set the door on the handheld. The XPressEntry Reader that the handheld represents is based on whether the handheld is in entry mode or exit mode.

For example, let us say that you have handheld A stationed at door A. Door A has two readers associated with it: Reader A-Entry and Reader A-Exit. The employee holding the handheld sets the handheld's door to Reader A. When the employee sees a cardholder walking towards the building, he sets the handheld to Entry mode and scans the cardholder's badge. The handheld in entry mode identifies itself as reader A-Entry and sends an activity to the server.

Later, there is heavy volume exiting Door B. Door B has two readers associated with it: Reader B-Entry and Reader B-Exit. The employee from door A is called to help and brings handheld A. He sets the door on his handheld to Door B and the mode to Exit. When he begins scanning people walking out of the door, the handheld identifies itself as Reader B-Exit and sends each scan as an activity to the server.

## Activities

XPressEntry will synchronize activities to Avigilon if that option has been set in the Data Manager.

1. If XPressEntry is configured to "push" activities, they will appear in the **Monitor** section of the **Avigilon** access control manager.
2. If XPressEntry is configured to "pull" activities, the **occupancy** within XPressEntry will **change** each time a person scans at a reader that is mapped to a door in **XPressEntry**.

You may want to pull activities if:

1. You want to use XPressEntry to manage Emergency Evacuations.
  - a. XPressEntry uses Avigilon activities to determine who is on and who is off site.
  - b. In the case of a mustering event, XPressEntry will have an up-to-date list of who is on site on this day.
  - c. Using this list, XPressEntry can be utilized to "muster" or mark people as safe to create a list of people who are still on site.
2. You want to use XPressEntry's features to determine who is on site, and what areas/zones people are in.

For more information about the functionality of XPressEntry, please review the XPressEntry manual.