

XPRESSENTRY

XPressEntry / Amadeus Integration Guide

Revision 06/02/2026

By



Table of Contents

Purpose	3
Prerequisites	3
Amadeus8 System Requirements	3
Configuring Devices in Amadeus8	3
User Setup in Amadeus8	6
XPressEntry Configuration	7
Step 1: Enable Amadeus8 Data Manager	7
Step 2: Configure Connection Settings	8
Step 3: Configure Sync Options	10
Pull Options	11
Push Options	11
Real-Time Updates	11
Step 4: Verify Connection	11
Step 5: Configure Sync Timers	11
Data Configuration	13
Users and Badges	13
Access Groups	15
Zones	17
Hazard Area Configuration	17
Tracked Hazard Area	17
Internal Muster Point	17
Offsite Location	17
Readers	18
Door Configuration	19
Handheld Device Doors	19
Amadeus8 Reader Doors	19
Reader Validations	21
Activity Logging	22
Best Practices	23
Troubleshooting	23
Connectivity Issues	23

Sync Problems	23
Real-Time Update Failures	24
Summary	24

Purpose

The **XPressEntry** integration with **Amadeus8** access control system serves as a middleware solution that facilitates communication between handheld devices and the Amadeus8 system. This integration enables seamless synchronization of access control data and real-time activity monitoring.

The integration retrieves and synchronizes the following data types from Amadeus8 to XPressEntry:

- **Cardholders** – User profile information
- **Badges** – Badge credentials and assignments
- **Access Information** – Permission levels and access rights
- **Occupancy Data** – Real-time location tracking for mustering support

Prerequisites

Amadeus8 System Requirements

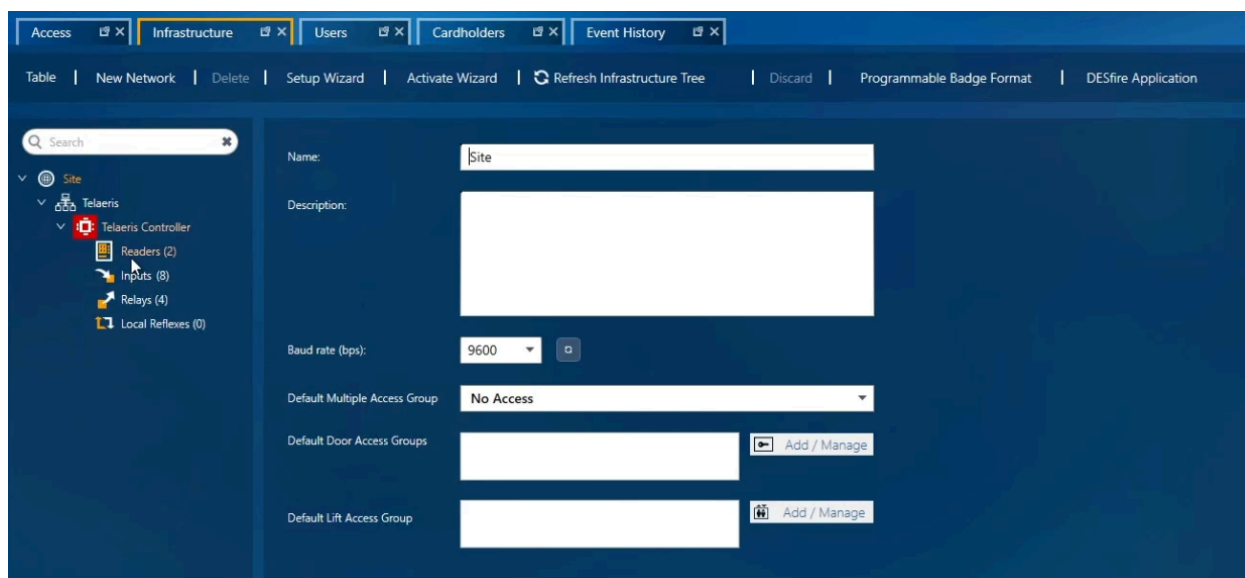
Before configuring the integration, ensure the following components are available:

1. **ACS API Service**
 - a. The Amadeus8 ACS API service must be installed and running
 - b. Note the port number where the service is hosted
2. **API User Credentials**
 - a. A user account with API permissions
 - b. An API key generated for this user

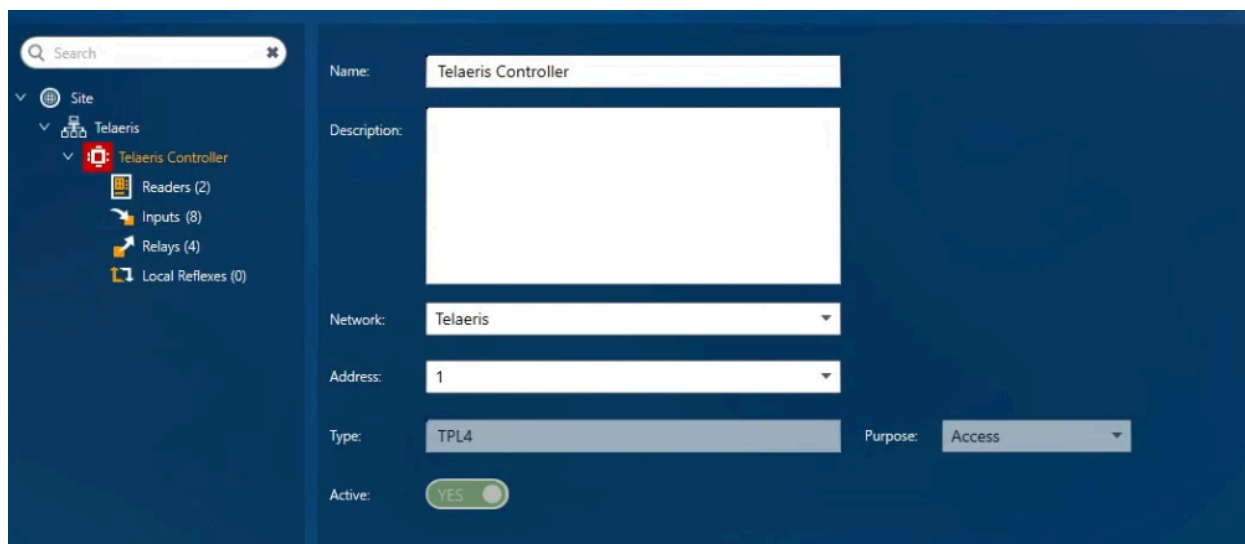
Configuring Devices in Amadeus8

Create placeholder (virtual) readers in Amadeus8 for each handheld device. Each virtual reader enables individual device tracking and accountability. These readers receive activity data from handheld scans.

1. First, create a **site** to hold the virtual controller and readers if you do not have one already.



2. Next, create a **virtual controller** to house your handheld readers.
 - a. Set **Active** to “Yes”



Note: Telaeris recommends creating two readers for each handheld device. One will be used to represent entry scans (e.g., Handheld 1 *Entry*) and the other will be used to represent exit and muster scans (e.g., Handheld 1 *Out/Muster*).

Handheld 1 Entry

Reader

Handheld 1 Entry



 Delete
  Download

 Save
  Save & Close

[Site](#) | [Telaeris](#) | [Telaeris Controller](#)

Main | Access Mode | Miscellaneous

Name:

Handheld 1 Entry

☐ Has slave reader

Number:

1

Badge types:

Proximity 125kHz

Description:

Door Control

Door contact:

Telaeris Controller_Input01

☐ Feedback

1st Relay:

Telaeris Controller_Relay01

2nd Relay:

<None>

☐ ByPass Relay

Door Type:

Access controller

T&A Reader:

<None>

From Area:

Undefined

To Area:

Undefined

Enrollment reader:

☐

Handheld 1 Out/Muster

Reader

Handheld 1 Out/Muster

 Delete
  Download
  Save
  Save & Close

 Site |
  Telaeris |
  Telaeris Controller

Main | Access Mode | Miscellaneous

Name: Handheld 1 Out/Muster
☐ Has slave reader
 Number: 2
 Badge types: Proximity 125kHz
 Description:

Door Control

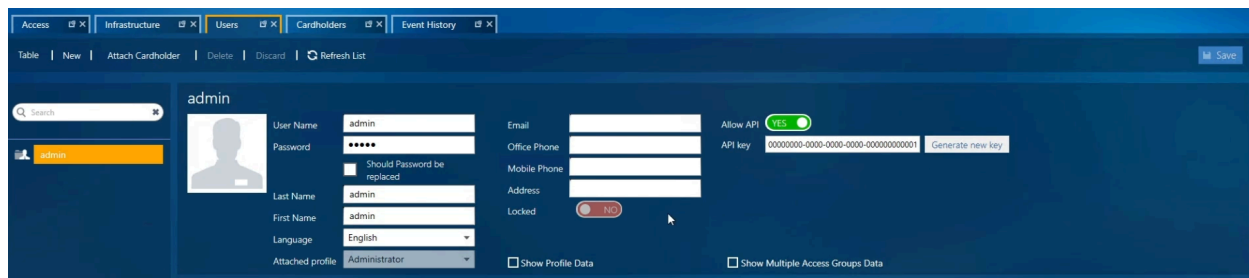
Door contact: Telaeris Controller_Input02 ☐ Feedback
 1st Relay: Telaeris Controller_Relay02
 2nd Relay: <None> ☐ ByPass Relay
 Door Type: Access controller
 T&A Reader: <None>
 From Area: Undefined
 To Area: Undefined
 Enrollment reader:

User Setup in Amadeus8

Configure a dedicated user account for the XPressEntry integration:

1. Create or designate a user (e.g., *default admin*)

2. Enable API access for this user
3. Generate an API key
4. Copy and securely store the username, password, and API key

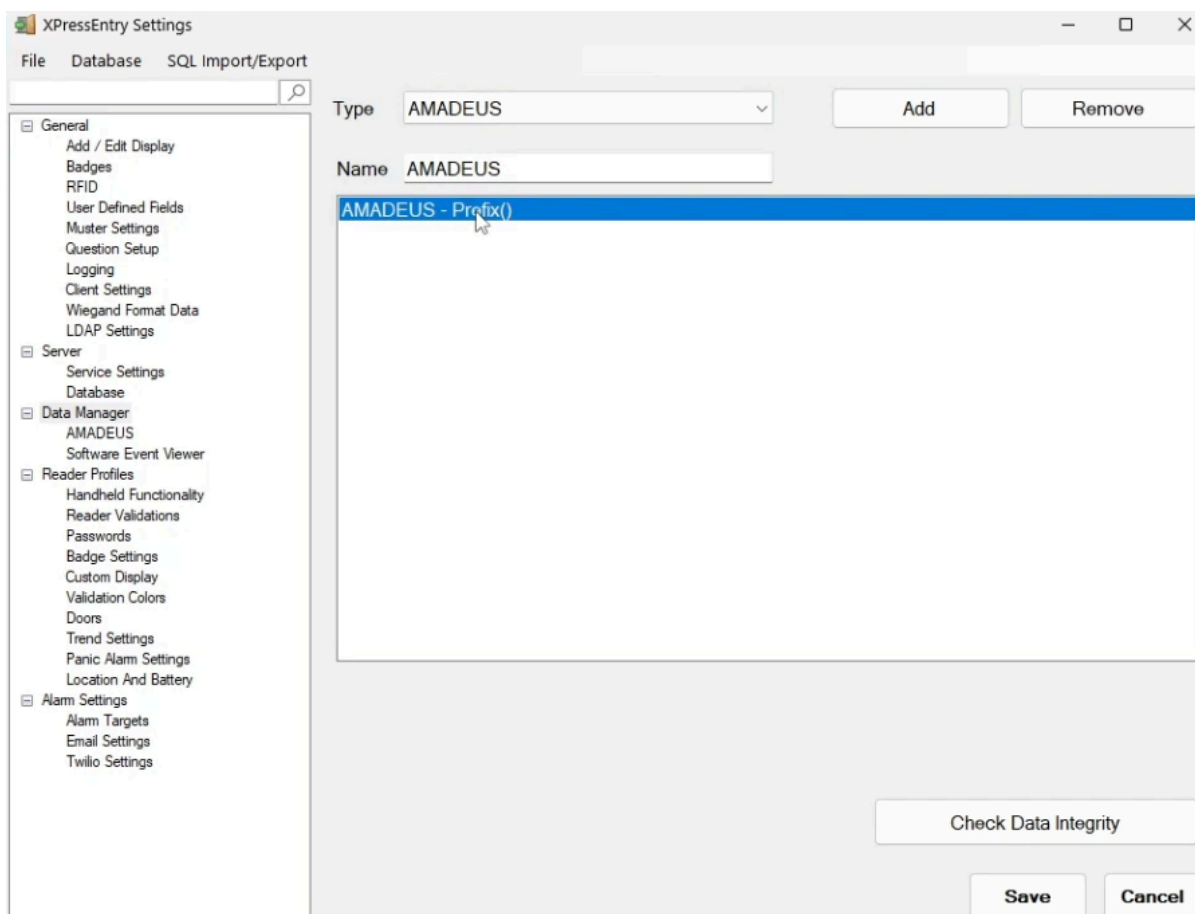


The screenshot shows the 'Users' tab in the XPressEntry interface. The user 'admin' is selected. The profile form includes fields for User Name, Password, Email, Office Phone, Mobile Phone, Address, and a 'Locked' toggle (currently 'NO'). The 'Allow API' toggle is set to 'YES'. An API key is displayed as '0000000-0000-0000-0000-000000000001' with a 'Generate new key' button. Other fields include Last Name, First Name, Language (English), and Attached profile (Administrator). There are checkboxes for 'Show Profile Data' and 'Show Multiple Access Groups Data'.

XPressEntry Configuration

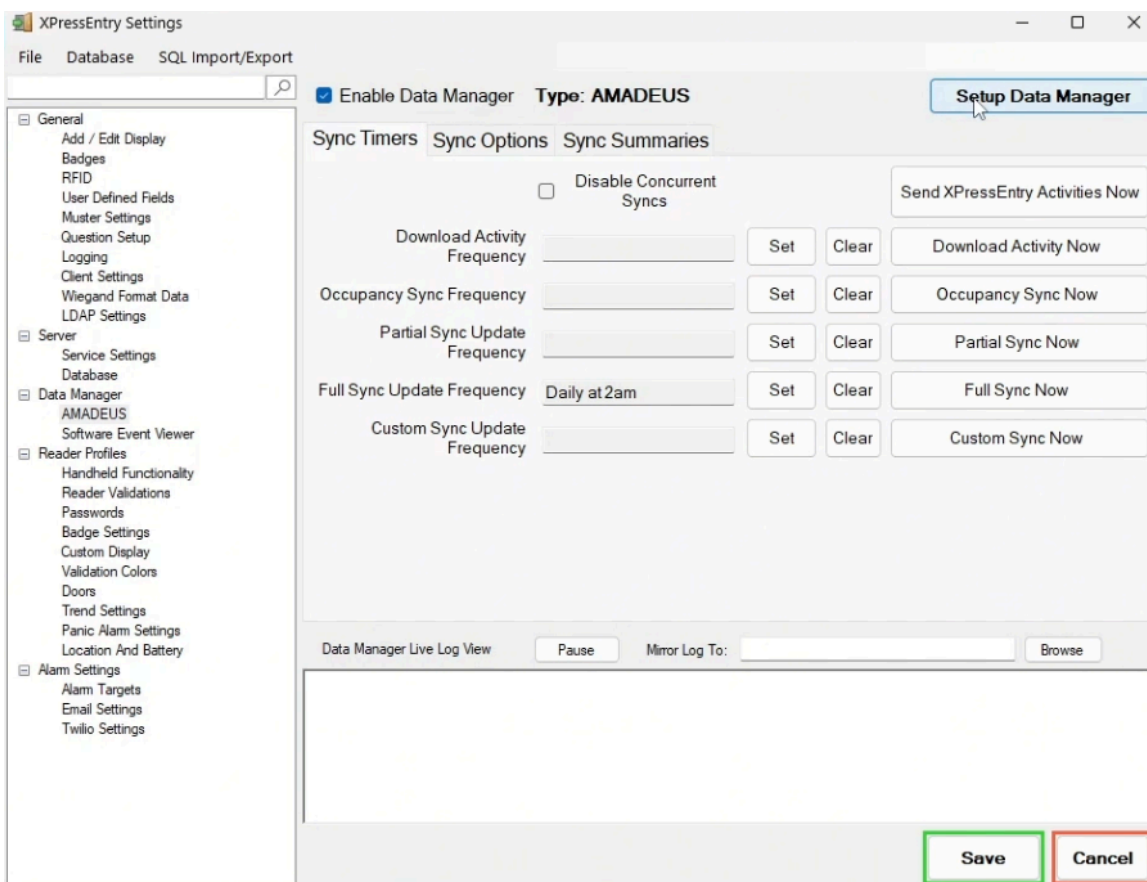
Step 1: Enable Amadeus8 Data Manager

1. Navigate to **Tools > Settings** to open the settings page.
2. Select the **Data Manager** tab on the left-hand side menu.
3. Select **AMADEUS** from the **Type** dropdown.
4. Click **Add** and **Save**.



Step 2: Configure Connection Settings

1. After adding the integration, a new tab will appear in the side menu. Navigate to the new tab, **DISABLED-AMADEUS**
2. Check **Enable Data Manager**
3. Click **Setup Data Manager**



XPressEntry Settings

File Database SQL Import/Export

☒ Enable Data Manager Type: AMADEUS [Setup Data Manager](#)

Sync Timers Sync Options Sync Summaries

☐ Disable Concurrent Syncs [Send XPressEntry Activities Now](#)

Download Activity Frequency [Set](#) [Clear](#) [Download Activity Now](#)

Occupancy Sync Frequency [Set](#) [Clear](#) [Occupancy Sync Now](#)

Partial Sync Update Frequency [Set](#) [Clear](#) [Partial Sync Now](#)

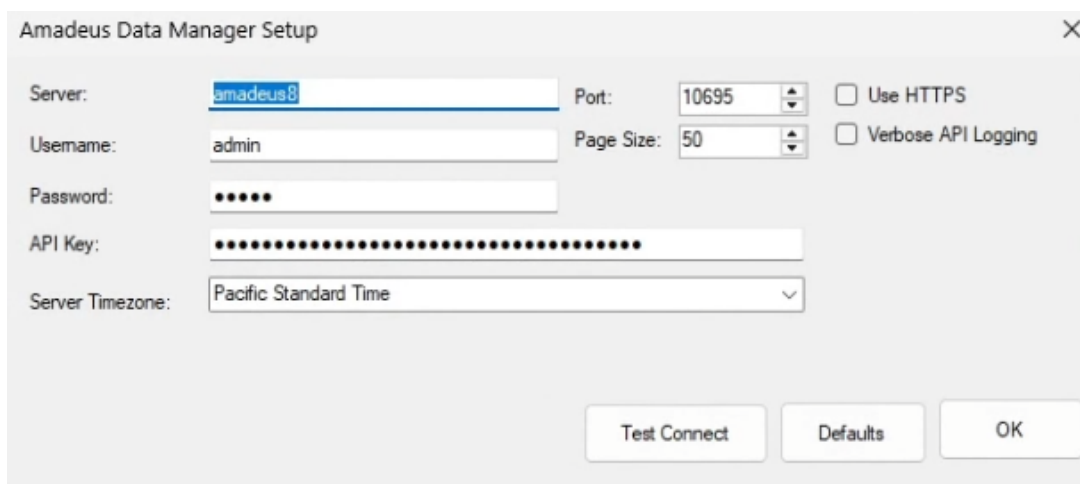
Full Sync Update Frequency [Set](#) [Clear](#) [Full Sync Now](#)

Custom Sync Update Frequency [Set](#) [Clear](#) [Custom Sync Now](#)

Data Manager Live Log View [Pause](#) Mirror Log To: [Browse](#)

[Save](#) [Cancel](#)

4. Enter the following connection details:
 - a. **Server IP or Hostname** – The Amadeus8 server address
 - b. **Port** – The port where the ACS API service is running
 - c. **Username** – API user credentials
 - d. **Password** – API user password
 - e. **API Key** – Generated API Key from Amadeus8
 - f. **Server Timezone** – Set to the time zone of the Amadeus8 server
 - g. **Page Size** – Maximum 100 records per request (optional)
 - h. **HTTPS** – Enable if using secure connection (optional)
 - i. **Verbose API logging** – Enable for troubleshooting (optional)



Amadeus Data Manager Setup

Server: Port: ☐ Use HTTPS

Username: Page Size: ☐ Verbose API Logging

Password:

API Key:

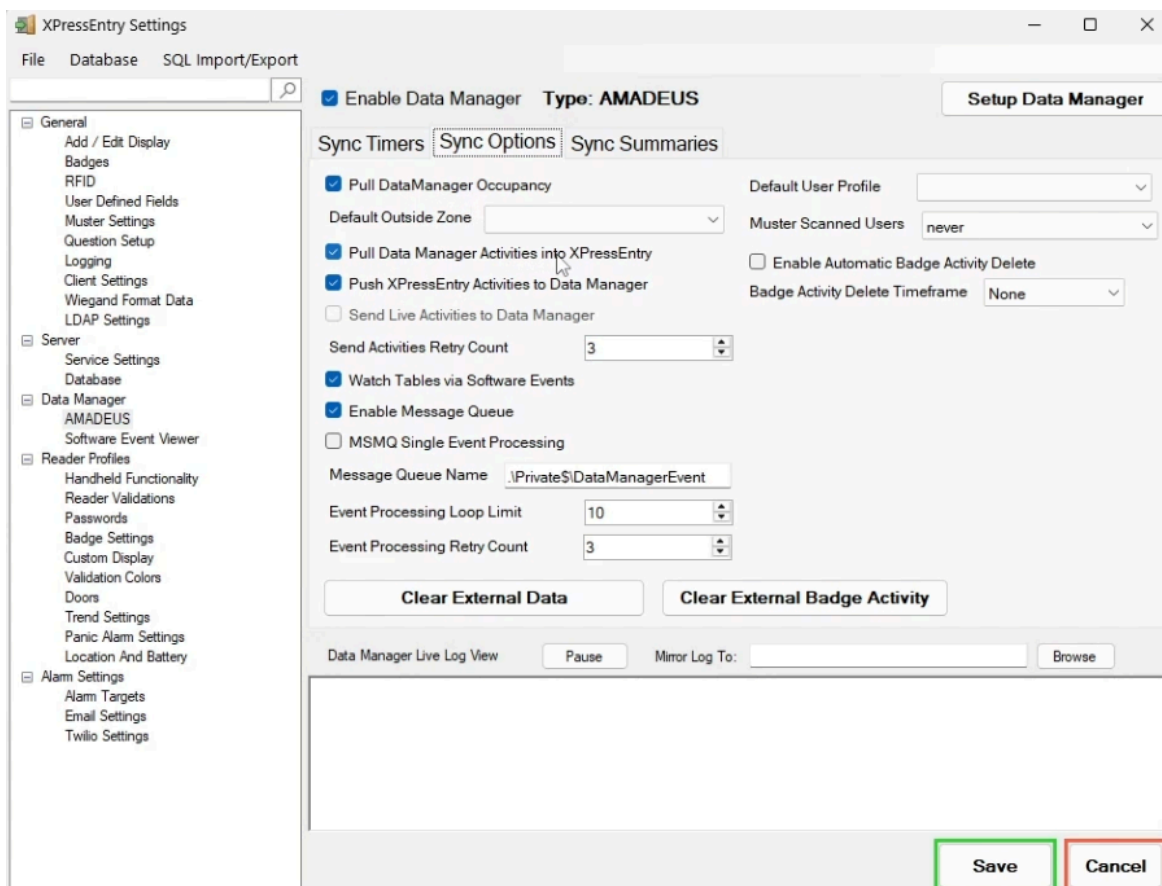
Server Timezone:

Test Connect Defaults OK

5. Click **Test Connection** to verify the connection
6. Click **OK** to save the settings

Step 3: Configure Sync Options

Navigate to the **Sync Options** tab and configure the following options:



XPressEntry Settings

File Database SQL Import/Export

☒ Enable Data Manager Type: AMADEUS Setup Data Manager

Sync Timers Sync Options Sync Summaries

☒ Pull DataManager Occupancy Default User Profile

Default Outside Zone

☒ Pull Data Manager Activities into XPressEntry Muster Scanned Users

☒ Push XPressEntry Activities to Data Manager ☐ Enable Automatic Badge Activity Delete

☐ Send Live Activities to Data Manager Badge Activity Delete Timeframe

Send Activities Retry Count

☒ Watch Tables via Software Events

☒ Enable Message Queue

☐ MSMQ Single Event Processing

Message Queue Name

Event Processing Loop Limit

Event Processing Retry Count

Clear External Data Clear External Badge Activity

Data Manager Live Log View Pause Mirror Log To: Browse

Save Cancel

Pull Options

1. **Pull Data Manager Occupancy or Activities**
 - a. When both are checked, the system pulls activities (transactions from Amadeus8 mapped to XPressEntry badge activities table)
 - b. Can be configured to pull occupancy only for mustering functionality

Push Options

1. **Enable Push XPressEntry Activities to Data Manager**
 - a. Sends handheld scan data to Amadeus8
 - b. Enables viewing of handheld activities in Amadeus8 event logs

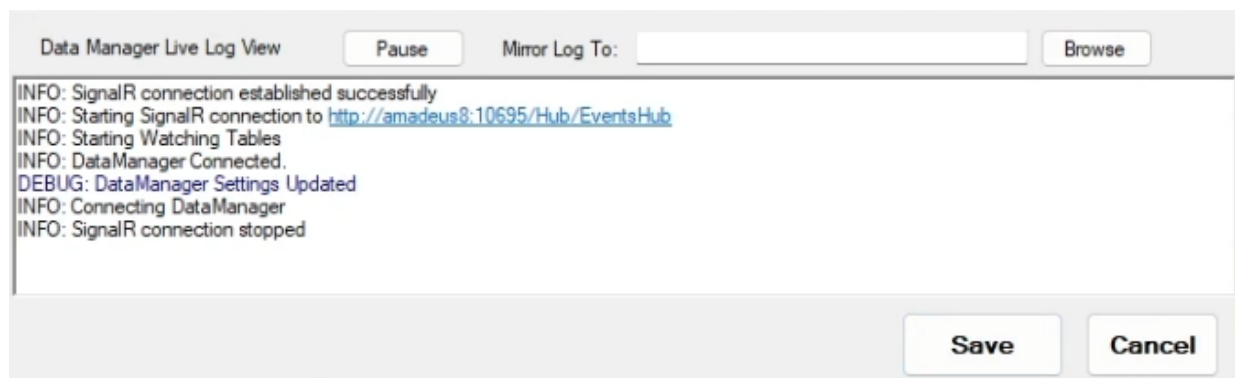
Real-Time Updates

1. **Enable Watch Tables via Software Events**
2. **Enable Message Queue**
 - a. Both settings are required for real-time updates from Amadeus8
 - b. Receives occupancy updates
 - c. Receives data changes (cardholders, badges, pictures, access rights)

Step 4: Verify Connection

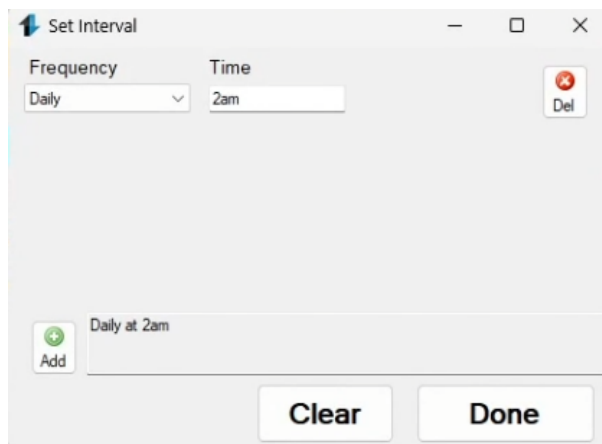
After clicking **Save**, verify the following status indicators:

- “DataManager connected”
- “SignalR connection established successfully”

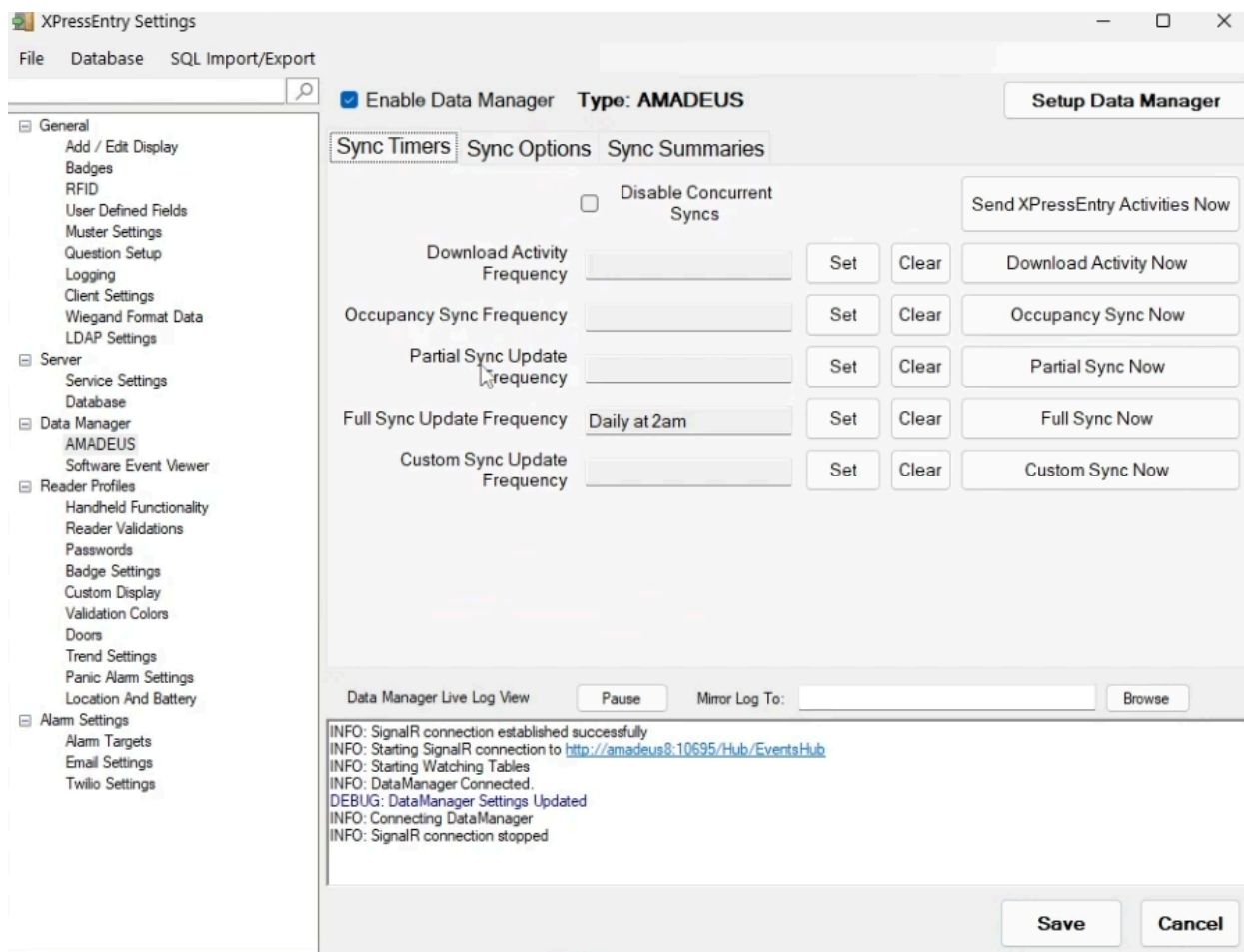


Step 5: Configure Sync Timers

1. Navigate to **Sync Timers**
2. Set a daily full sync interval (recommended is 2:00 AM)
 - a. Click **Set** next to **Full Sync Update Frequency**
 - b. Select **Daily** and choose a low-usage time window



3. A full sync performs complete data synchronization including:
 - a. All user data
 - b. All badge information
 - c. All group assignments
 - d. Deletion of records no longer existing in Amadeus8



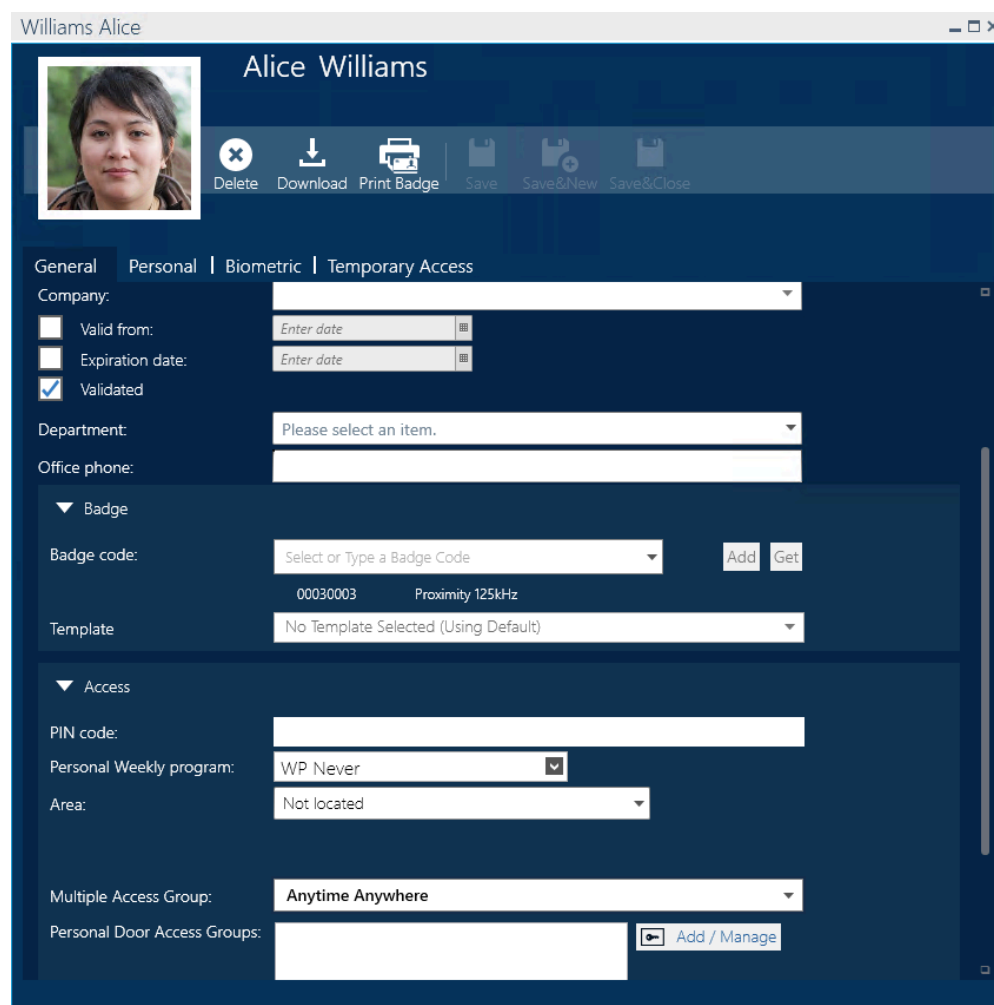
Data Configuration

Users and Badges

After running a full sync, the following data will be available in XPressEntry:

- User profiles with pictures
- Badge assignments and credentials
- Permission groups and access rights

An example of an integrated user profile in Amadeus8 and XPressEntry is shown below:



The screenshot displays the 'Alice Williams' user profile configuration window. The interface includes a header with the user's name and a toolbar with icons for Delete, Download, Print Badge, Save, Save&New, and Save&Close. Below the header, there are tabs for General, Personal, Biometric, and Temporary Access. The General tab is active, showing fields for Company, Valid from, Expiration date, Validated (checked), Department, and Office phone. The Badge section includes a Badge code field (00030003, Proximity 125kHz) and a Template dropdown (No Template Selected (Using Default)). The Access section includes a PIN code field, Personal Weekly program (WP Never), Area (Not located), Multiple Access Group (Anytime Anywhere), and Personal Door Access Groups.

XPressEntry (Administrator) - 3.6.9999 - Telaeris Inc (Logged In User: admin)

File Tools View Logout Entry/Exit Muster Help

Entry/Exit Muster Activity History Add/Edit Info Logs

Filtered on: williams

Filter: williams

Users Logins Companies Groups Zones Doors Readers Roles User Profiles Timezones

User Groups Zones Timezones Vehicle Types Contact Info UDFs

First Name Last Name MI Photo FP

Alice Williams

Company

Emp ID

Zone Not located

Start Date

End Date

User Profile

Create Login

Badges (1)

Add Badge Delete Badge View History Print Badge

Badge	Activated Date	Expired Date	Invalid	Badge Type
30003				

External Record: 3a2356d2-d1e8-4f66-a26e-99c0a367df12

Add New Delete Save Cancel

Time to Read 6 Records: 0.04

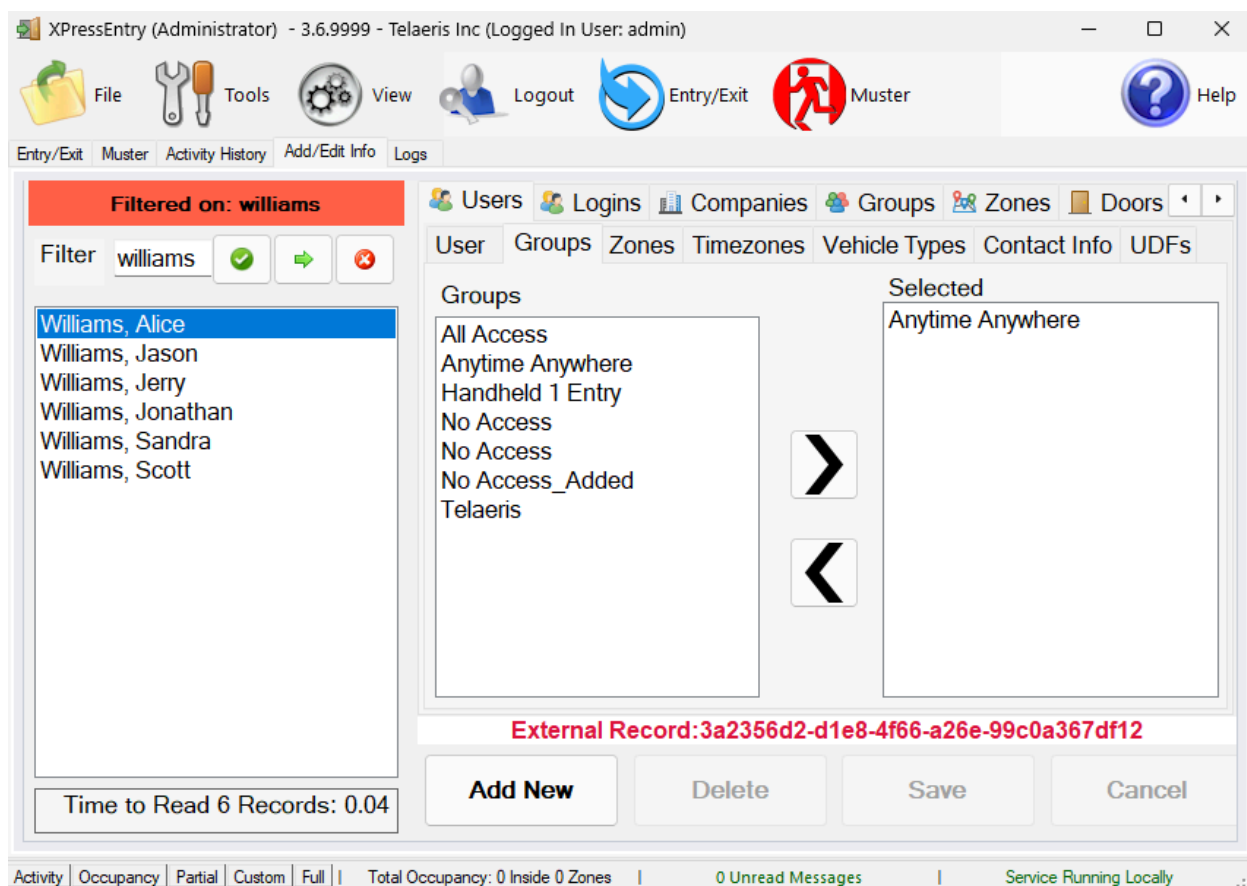
Activity Occupancy Partial Custom Full

Total Occupancy: 0 Inside 0 Zones

0 Unread Messages

Service Running Locally

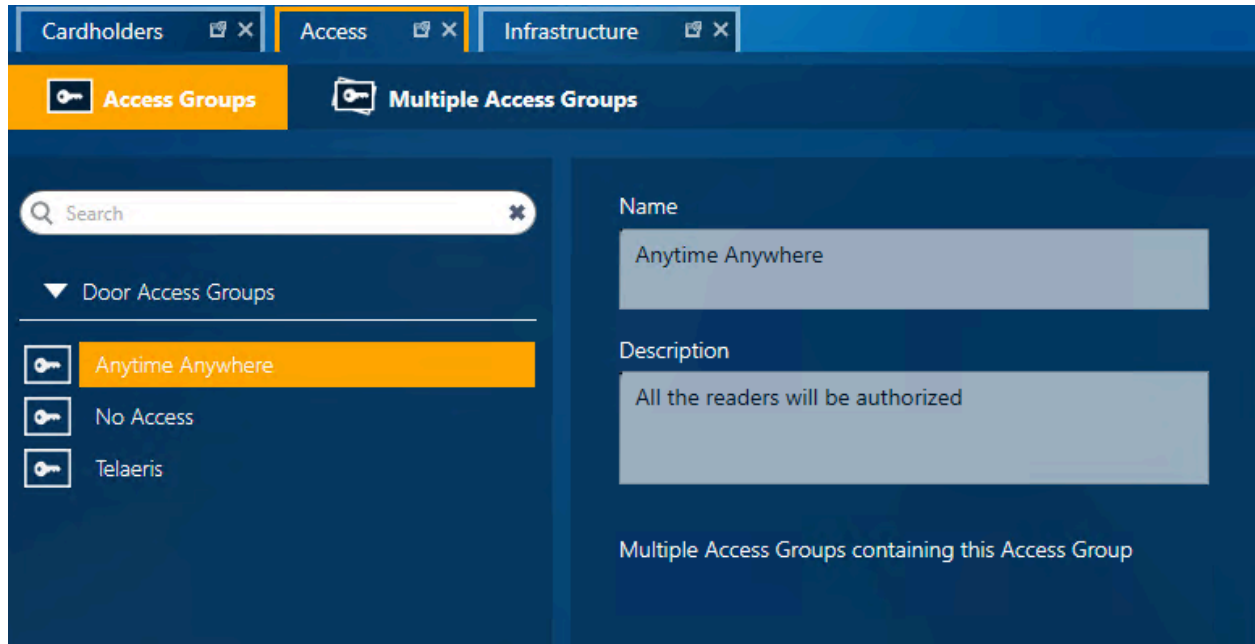
The Groups subtab lists the Access Groups a user has access to:



Access Groups

- Access groups synchronized from Amadeus8
- Associated readers for each group
- Permission mappings

Example Access Group:



Select Readers

Drag a column header and drop it here to group by that column

	Network	Controller	Reader	Reader Type	Weekly Program
	Telaeris	Telaeris Controller	Handheld 1 Entry	Proximity 125kHz	WP Always
	Telaeris	Telaeris Controller	Handheld 1 Out/Muster	Proximity 125kHz	WP Always

Synchronized Group in XPressEntry:

XPressEntry (Administrator) - 3.6.9999 - Telaeris Inc (Logged In User: admin)

File Tools View Logout Entry/Exit Muster Help

Entry/Exit Muster Activity History Add/Edit Info Logs

Filter: [] [] []

Users Logins Companies Groups Zones Doors Readers Roles User Profiles Timezones

Name: Anytime Anywhere

☐ Is Default Group ☐ Group Allows Reader Login

Readers Zones Holidays

Readers: Handheld 1, Handheld 1 Entry, Handheld 1 Out/Muster, Handheld 2, Server Reader : TOUCAN

Selected: Handheld 1 Entry, Handheld 1 Out/Muster

Timezones: WP Always, WP Never, WP Personal

External Record: 1111111-1111-1111-1111-111111111111

Add New Delete Save Cancel

Time to Read 7 Records: 0.04

Activity Occupancy Partial Custom Full | Total Occupancy: 0 Inside 0 Zones | 0 Unread Messages | Service Running Locally

Zones

Zones must be properly configured for accurate occupancy tracking and mustering.

XPressEntry (Administrator) - 3.6.9999 - Telaeris Inc (Logged In User: admin)

File Tools View Logout Entry/Exit Muster Help

Entry/Exit Muster Activity History Add/Edit Info Logs

Users Logins Companies Groups Zones Doors Readers Roles User Profiles Timezones

Name: Site

Description:

Parent Zone:

☐ Zone is Outside ☐ Max Occupancy 0

☐ Zone is a Muster Point

☒ Zone is a Hazard Area

☐ Zone is Global

Door	Start Zone	End Zone	External Entry Reader	External Exit Reader
Handheld 1 Door	Offsite	Site	Handheld 1 Entry	Handheld 1 Out/Muster

External Record: 00000000-0000-0000-0000-100000000002

Add New Delete Save Cancel

Time to Read 5 Records: 0.05

Activity Occupancy Partial Custom Full | Total Occupancy: 0 Inside 0 Zones | 0 Unread Messages | Service Running Locally

Hazard Area Configuration

Tracked Hazard Area

- **Zone is a Hazard Area** – Checked
- **Zone is Outside** – Unchecked
- **Zone is a Muster Point** – Unchecked

Internal Muster Point

- **Zone is a Hazard Area** – Checked
- **Zone is a Muster Point** – Checked

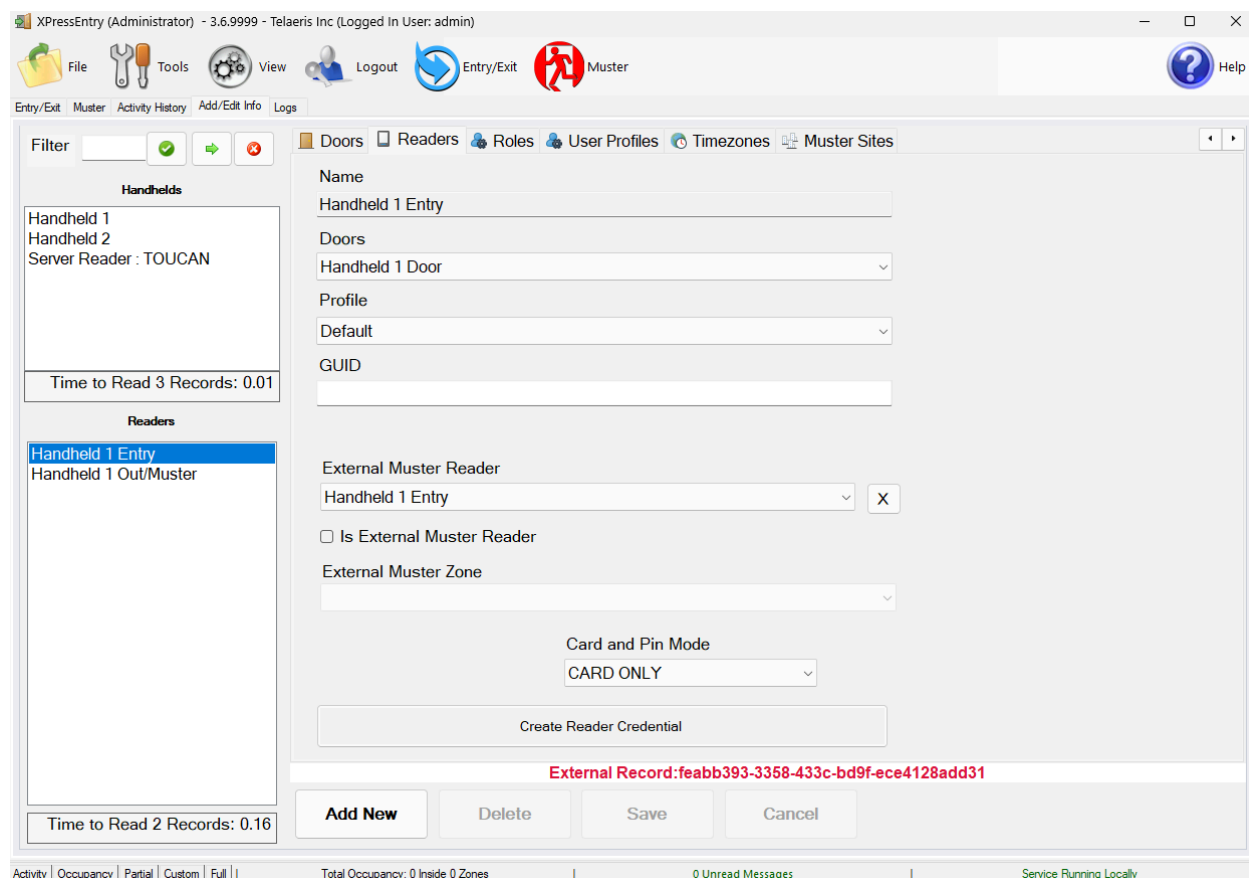
Offsite Location

- **Zone is Outside** – Checked (prevents occupancy tracking)
- **Zone is a Muster Point** – Optional

Readers

External readers from the Amadeus8 system are synchronized and available for configuration.

	#	Name	Badge Types	Door Contact	1st Relay	Weekly Program
X	1	Handheld 1 Entry	Proximity 125kHz	Telaeris Controller_Input01	Telaeris Controller_Relay01	WP Always
X	2	Handheld 1 Out/Muster	Proximity 125kHz	Telaeris Controller_Input02	Telaeris Controller_Relay02	WP Always



XPRESSEntry (Administrator) - 3.6.9999 - Telaeris Inc (Logged In User: admin)

File Tools View Logout Entry/Exit Muster

Entry/Exit Muster Activity History Add/Edit Info Logs

Filter [] [] [] []

Doors Readers Roles User Profiles Timezones Muster Sites

Handhelds

Handheld 1
Handheld 2
Server Reader : TOUCAN

Time to Read 3 Records: 0.01

Readers

Handheld 1 Entry
Handheld 1 Out/Muster

Time to Read 2 Records: 0.16

Name: Handheld 1 Entry

Doors: Handheld 1 Door

Profile: Default

GUID:

External Muster Reader: Handheld 1 Entry X

☐ Is External Muster Reader

External Muster Zone:

Card and Pin Mode: CARD ONLY

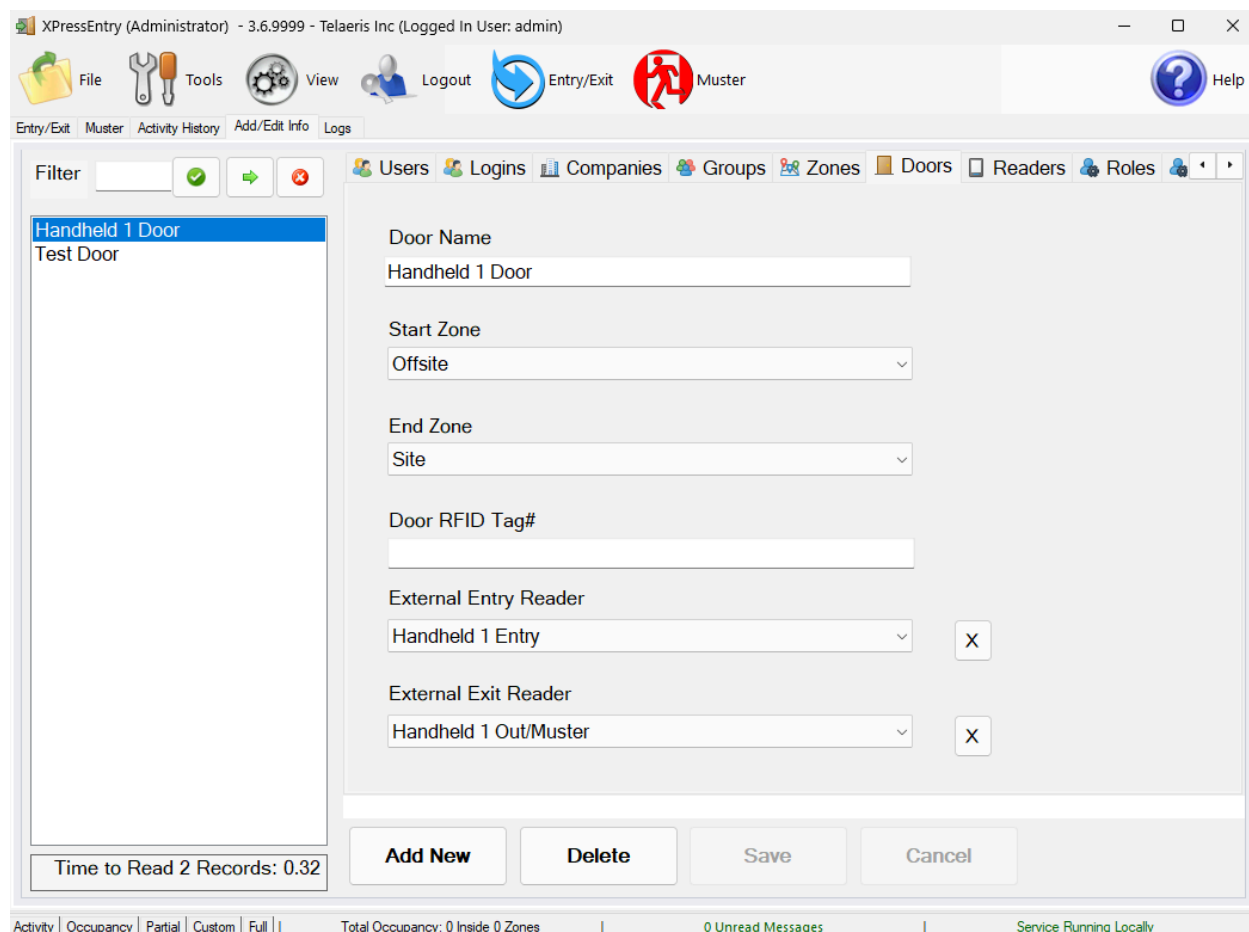
Create Reader Credential

External Record: feabb393-3358-433c-bd9f-ece4128add31

Add New Delete Save Cancel

Activity | Occupancy | Partial | Custom | Full | Total Occupancy: 0 Inside 0 Zones | 0 Unread Messages | Service Running Locally

Door Configuration



Handheld Device Doors

Create doors in the **Doors** tab for handheld device scanning:

1. Create a door for each handheld device
2. Associate the virtual readers (created in Amadeus8) with the corresponding door
3. Configure zone assignments:
 - a. **Start Zone** – Where users begin before scanning
 - b. **End Zone** – Where users are placed after scanning in entry mode
 - c. In exit mode, users are transported from the end zone back to the start zone.

Amadeus8 Reader Doors

For occupancy tracking of physical readers in Amadeus8:

1. Create a door for each Amadeus8 reader you want to track
 - a. Example: *“Office Controller_Reader1”*:

Office Controller_Reader1

Reader

Office Controller_Reader1



 Delete
  Download

 Save
  Save & Close

[Site](#) | [Telaeris](#) | [Office Controller](#)

Main | Access Mode | Miscellaneous

Name:

Office Controller_Reader1

☐ Has slave reader

Number:

1

Badge types:

Proximity 125kHz

Description:

Door Control

Door contact:

Office Controller_Input01

☐ Feedback

1st Relay:

Office Controller_Relay01

2nd Relay:

<None>

☐ ByPass Relay

Door Type:

Access controller

T&A Reader:

<None>

From Area:

Undefined

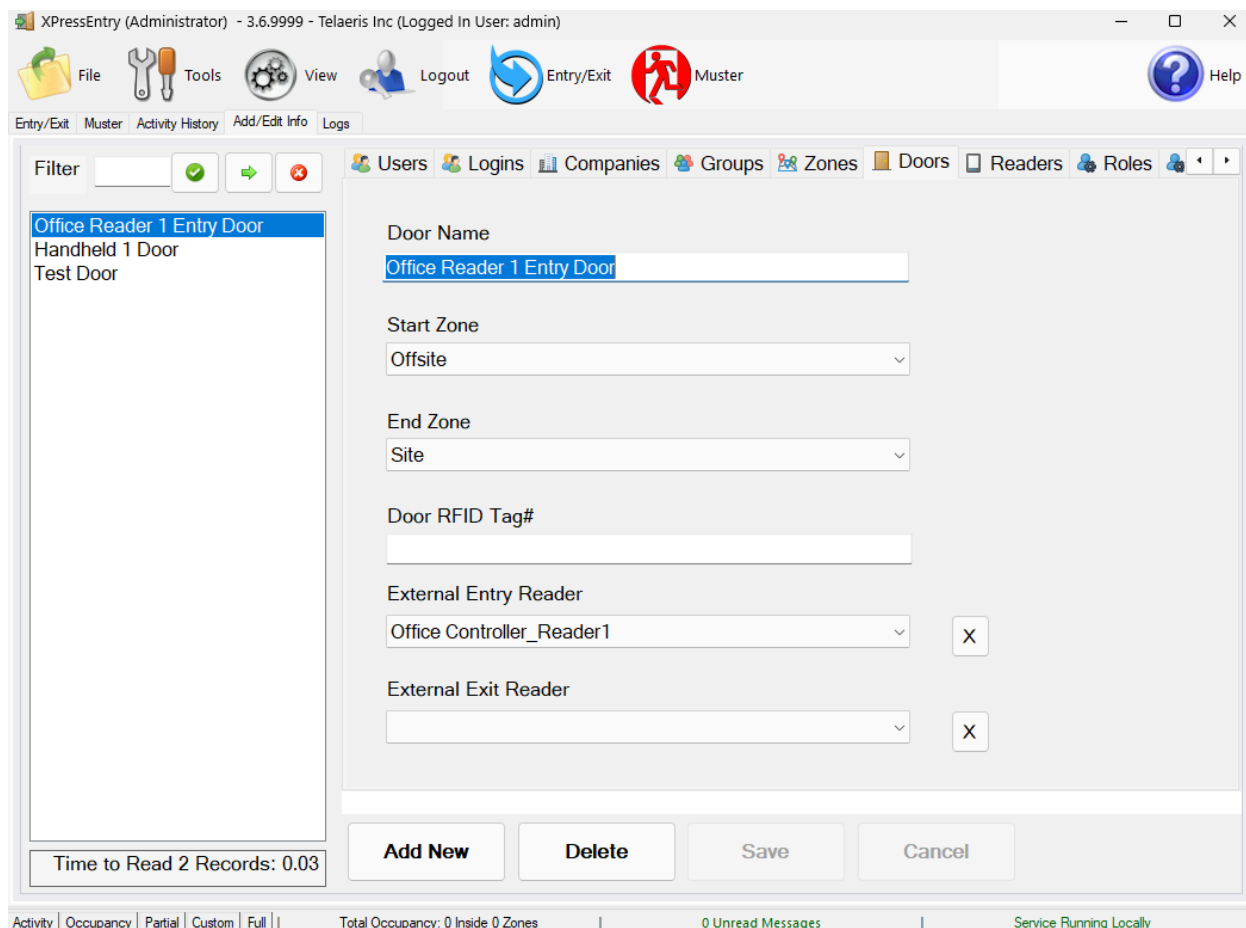
To Area:

Undefined

Enrollment reader:

☐

b. Example Door in XPressEntry:

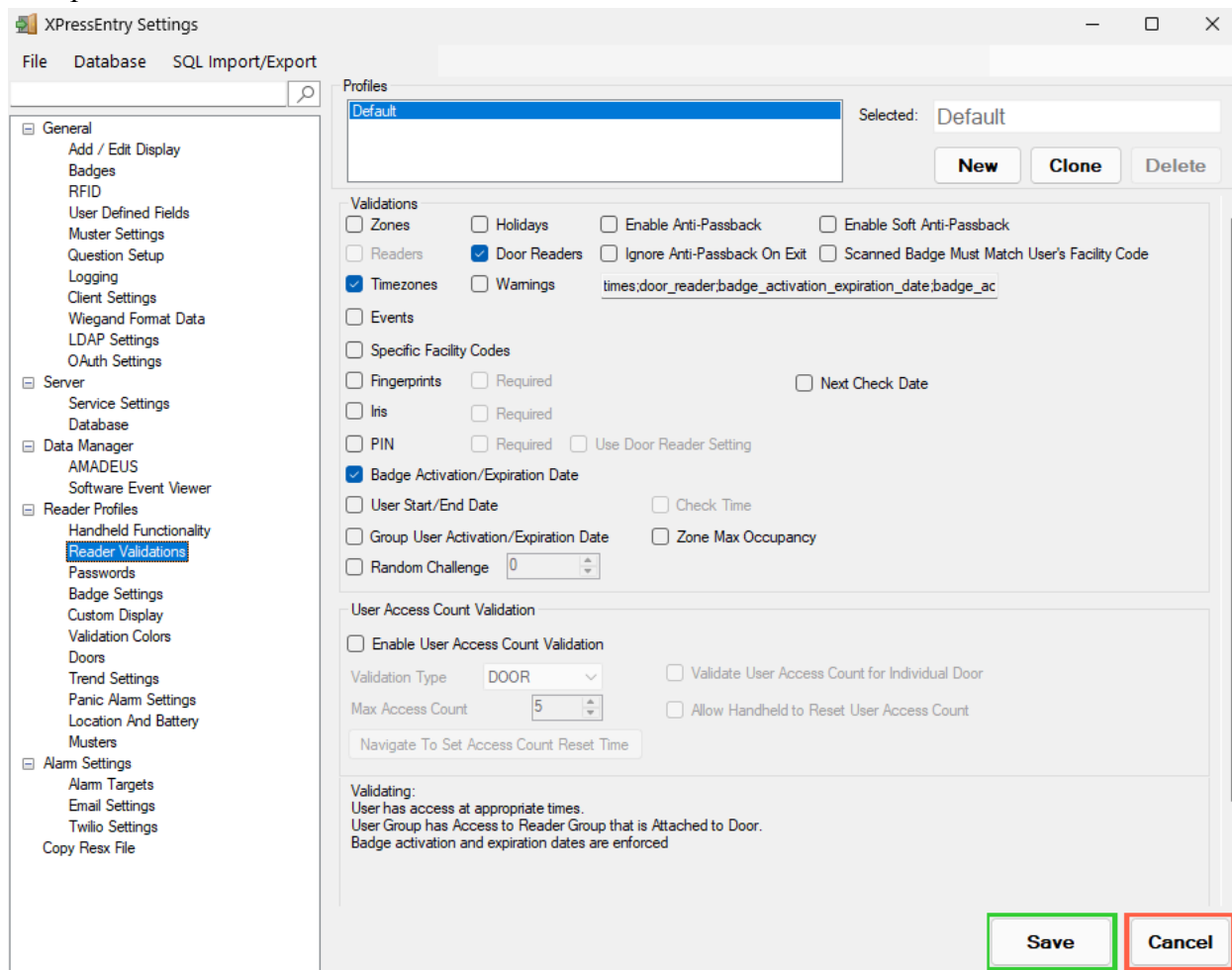


2. Set the **End Zone** appropriately (e.g., “Site”)
3. Users scanning on that physical reader will be transported to the configured zone within XPressEntry.

Reader Validations

1. Go to **Tools > Settings > Reader Validations**
2. Enable the following validations:
 - a. Door Readers (*if configured; note this is not currently synchronized and must be set up manually — contact support for assistance*)
 - b. Time Zones (*if configured; note this is not currently synchronized and must be set up manually — contact support for assistance*)
 - c. Badge Activation / Expiration Date
3. Click **Save**.

Note: Reader validations are profile specific. Repeat this for each reader profile if you have multiple.

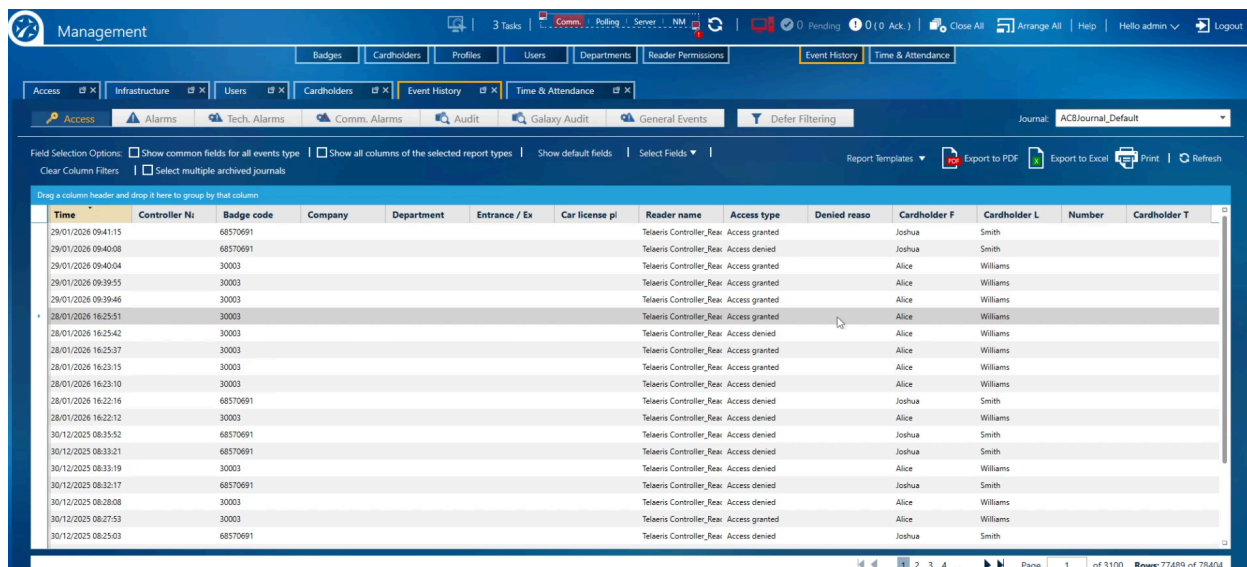


The screenshot shows the 'XPressEntry Settings' application window. The left sidebar contains a tree view with categories like General, Server, Data Manager, Reader Profiles, and Alarm Settings. Under 'Reader Profiles', 'Reader Validations' is selected. The main area displays configuration options for the 'Default' profile. The 'Validations' section includes checkboxes for Zones, Readers, Timezones, Events, Fingerprints, Iris, PIN, and Badge Activation/Expiration Date. The 'User Access Count Validation' section includes checkboxes for enabling validation and setting a max access count. The 'Save' button is highlighted with a green border, and the 'Cancel' button is highlighted with a red border.

Activity Logging

All handheld scans are pushed to the Amadeus8 event history when the push option is enabled:

- **Timestamp** – When the scan occurred
- **Badge Number** – The scanned credential
- **Reader** – Which virtual reader (handheld) performed the scan
- **Result** – Whether the scan was granted or denied



Time	Controller N	Badge code	Company	Department	Entrance / Ex	Car license pl	Reader name	Access type	Denied reason	Cardholder F	Cardholder L	Number	Cardholder T
29/01/2026 09:41:15		68570691					Telaeris Controller,Real	Access granted		Joshua	Smith		
29/01/2026 09:40:08		68570691					Telaeris Controller,Real	Access denied		Joshua	Smith		
29/01/2026 09:40:04		30003					Telaeris Controller,Real	Access granted		Alice	Williams		
29/01/2026 09:39:55		30003					Telaeris Controller,Real	Access granted		Alice	Williams		
29/01/2026 09:39:46		30003					Telaeris Controller,Real	Access granted		Alice	Williams		
28/01/2026 16:25:51		30003					Telaeris Controller,Real	Access granted		Alice	Williams		
28/01/2026 16:25:42		30003					Telaeris Controller,Real	Access denied		Alice	Williams		
28/01/2026 16:25:37		30003					Telaeris Controller,Real	Access granted		Alice	Williams		
28/01/2026 16:23:15		30003					Telaeris Controller,Real	Access granted		Alice	Williams		
28/01/2026 16:23:10		30003					Telaeris Controller,Real	Access denied		Alice	Williams		
28/01/2026 16:22:16		68570691					Telaeris Controller,Real	Access denied		Joshua	Smith		
28/01/2026 16:22:12		30003					Telaeris Controller,Real	Access denied		Alice	Williams		
30/12/2025 08:35:52		68570691					Telaeris Controller,Real	Access denied		Joshua	Smith		
30/12/2025 08:33:21		68570691					Telaeris Controller,Real	Access denied		Joshua	Smith		
30/12/2025 08:33:19		30003					Telaeris Controller,Real	Access denied		Alice	Williams		
30/12/2025 08:32:17		68570691					Telaeris Controller,Real	Access denied		Joshua	Smith		
30/12/2025 08:28:08		30003					Telaeris Controller,Real	Access denied		Alice	Williams		
30/12/2025 08:27:53		30003					Telaeris Controller,Real	Access granted		Alice	Williams		
30/12/2025 08:25:03		68570691					Telaeris Controller,Real	Access denied		Joshua	Smith		

Best Practices

The following recommendations help ensure a reliable connection and successful integration:

1. **Daily Full Sync** – Schedule a full sync daily (e.g., 2:00 AM) to ensure data consistency
2. **Virtual Readers** – Create 2 virtual readers per handheld device for accurate accountability, *unless strictly using entry mode*, in which case one is sufficient.
3. **Zone Configuration** – Properly configure hazard areas, muster points, and outside locations for accurate occupancy tracking
4. **API Logging** – Enable verbose API logging during initial setup and troubleshooting
5. **Connection Monitoring** – After saving settings, verify that both “**DataManager connected**” and “**SignalR connection established successfully**” messages are logged
6. **Real-Time Updates** – Ensure **Enable Message Queue** and **Watch Tables via Software Events** are enabled for immediate data synchronization

Troubleshooting

Connectivity Issues

- Verify the API service is running on the configured port
- Confirm the API user has appropriate permissions
- Check that the API key is valid and correctly entered
- Enable verbose API logging to capture detailed error messages

Sync Problems

- Run a manual full sync to re-synchronize the XPressEntry system with Amadeus8
- Verify the page size setting (maximum 100)
- Check network connectivity between XPressEntry and Amadeus8 servers

Real-Time Update Failures

- Confirm SignalR connection is established
- Ensure **Enable Message Queue** and **Watch Tables via Software Events** are enabled
- Check firewall rules allow bidirectional communication

Summary

The XPressEntry integration with Amadeus8 provides a robust solution for mobile access control management with real-time synchronization capabilities. Proper configuration of virtual readers, zones, and sync options ensures accurate occupancy tracking, mustering support, and comprehensive activity logging across both systems.