XPressEntry

XPressEntry / Verkada Integration Guide

Revision 06/04/2026

By

TELAERIS

Table of Contents

Purpose

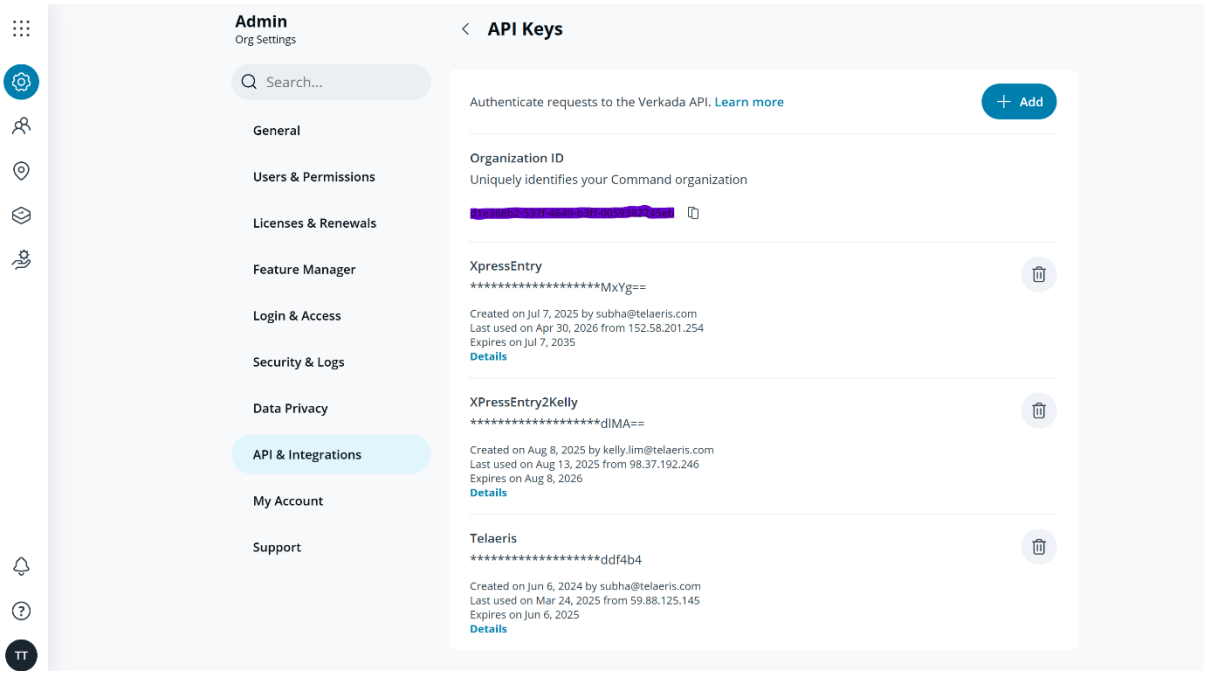
The **XPressEntry** integration with the **Verkada** access control system serves as a middleware solution that facilitates communication between handheld devices and the **Verkada** system. This integration enables seamless synchronization of access control data and real-time activity monitoring. It supports entry, exit, and mustering use cases. This document serves as a guide to completing the integration.

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

- **Users** – User profile information including name and photo.
- **Badges** – Badge credentials and assignments.
- **Access Information** – Access Groups and Device Permissions.
- **Activity Data** – Historic and real-time badge scan events.

Pre-Requisites

- Verkada System Requirements. Before configuring the integration, ensure the following components are available:
  - **Verkada Command Account**
  - An **organization account** with https://command.verkada.com/
  - The **Organization ID** from the Verkada system
  - **User Setup** in Verkada
  - A dedicated **administrator user account** for the XPressEntry integration
  - An **API Key** generated for the XPressEntry integration
  - The **username**, **password**, **Organization ID**, and **API Key** copied and securely stored



- **Network Configuration**
  - Ports **30000** and **30001** should be **open** for communication between the XPressEntry server and handhelds on the machine where XPressEntry is installed.

Limitations

There is no option to receive real-time or partial updates for user or badge changes. These changes are captured only during a full sync.

Overall Order of Operations

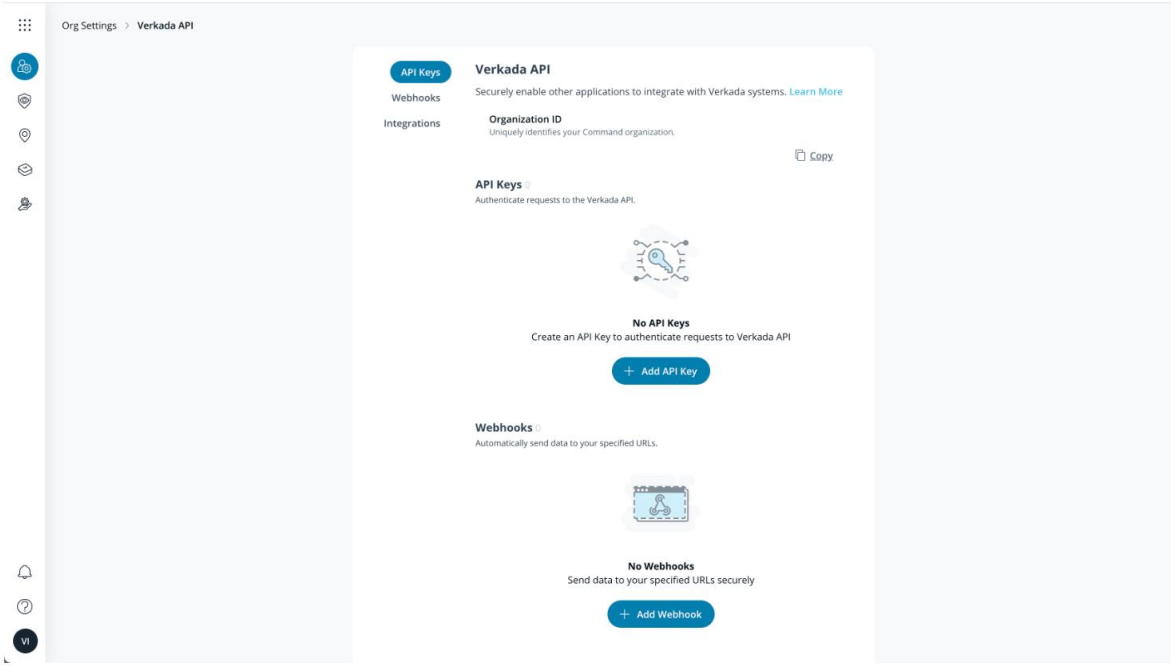
1. Set up Verkada to enable the API integration.
2. Enable Data Manager synchronization from XPressEntry.
3. Perform the initial data synchronization and configure XPressEntry data.
4. Set up XPressEntry Handheld Readers.
5. Scan data on the card reader and validate functionality.

Setting Up Verkada to Synchronize with XPressEntry

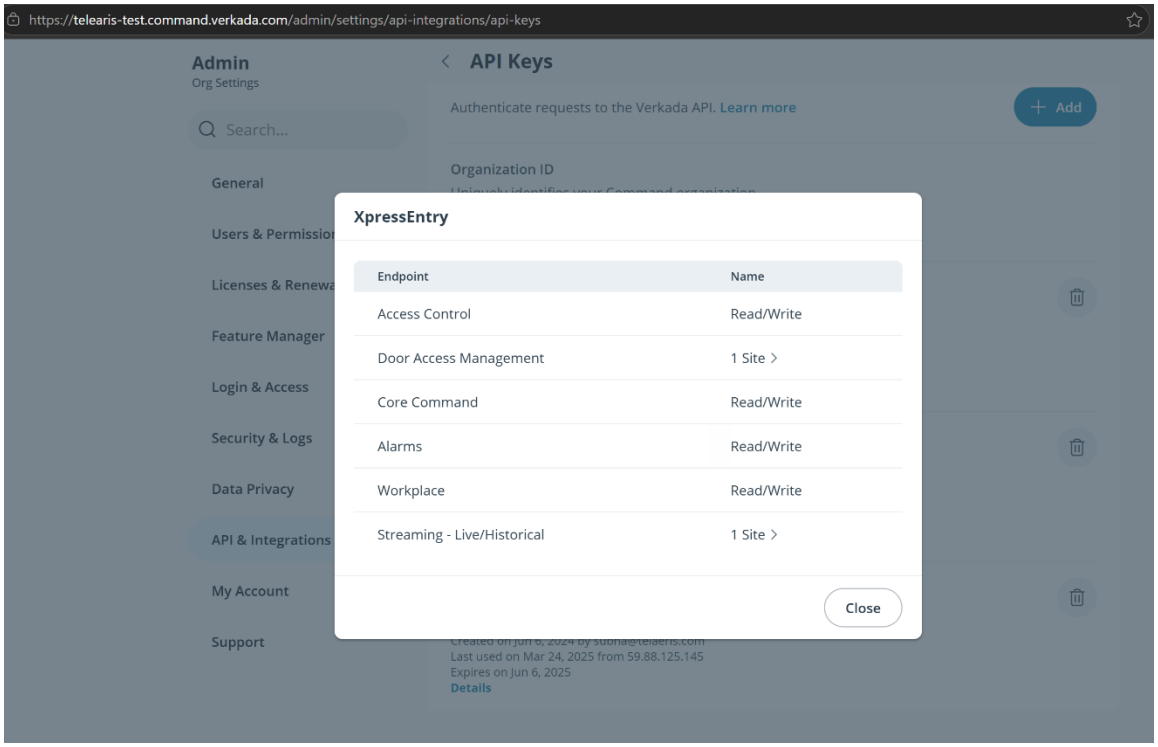
It is assumed that there is an existing Verkada Command account.

An API Key is required for authentication.

To create a new API Key (Organization Admin only), navigate to the Verkada API tab under the Organization Settings page. Click the '+ New API Key' button to add a new API Key for your organization.



You will then be prompted to provide a name for the API Key you are creating. Naming your keys makes them easier to manage across the organization. That said, we recommend creating API Keys only when required and reusing the same key across applications wherever possible.

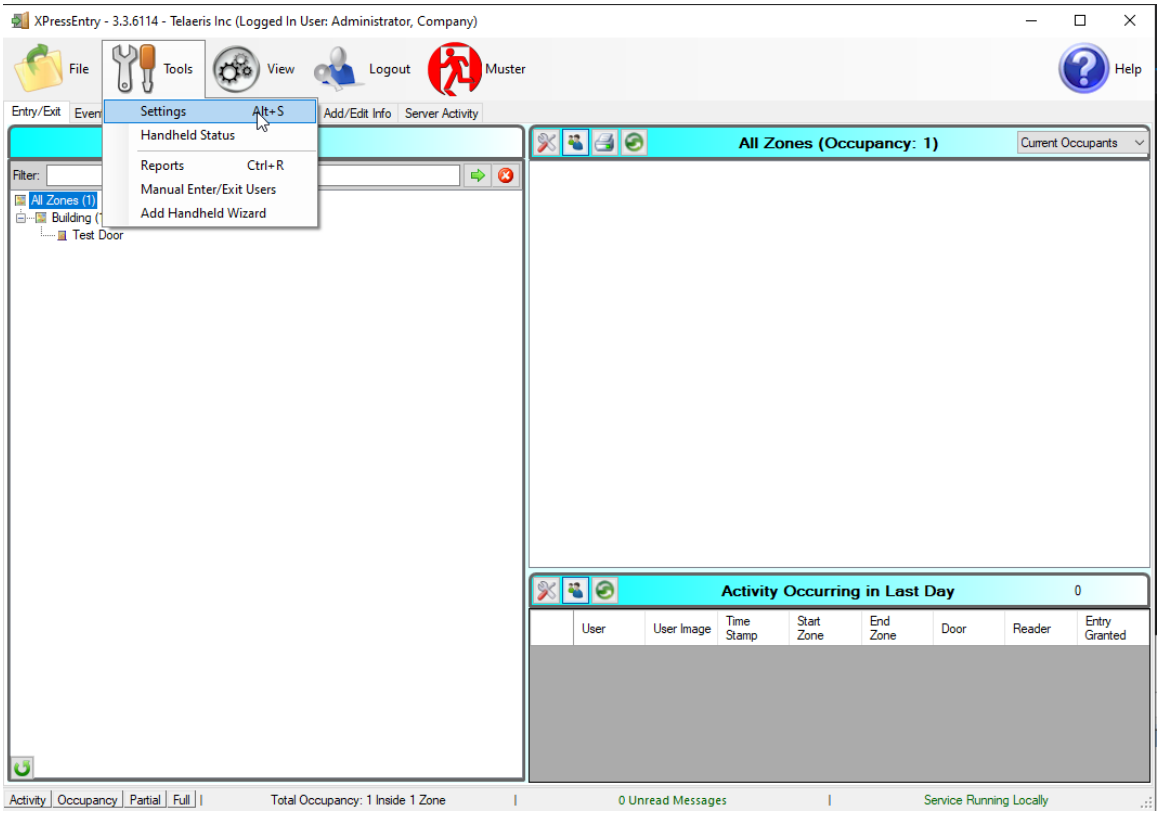


Physical Verkada controllers are mapped to XPressEntry handhelds, so that when badge activities from an XPressEntry handheld are sent to Verkada, the corresponding doors can be controlled.

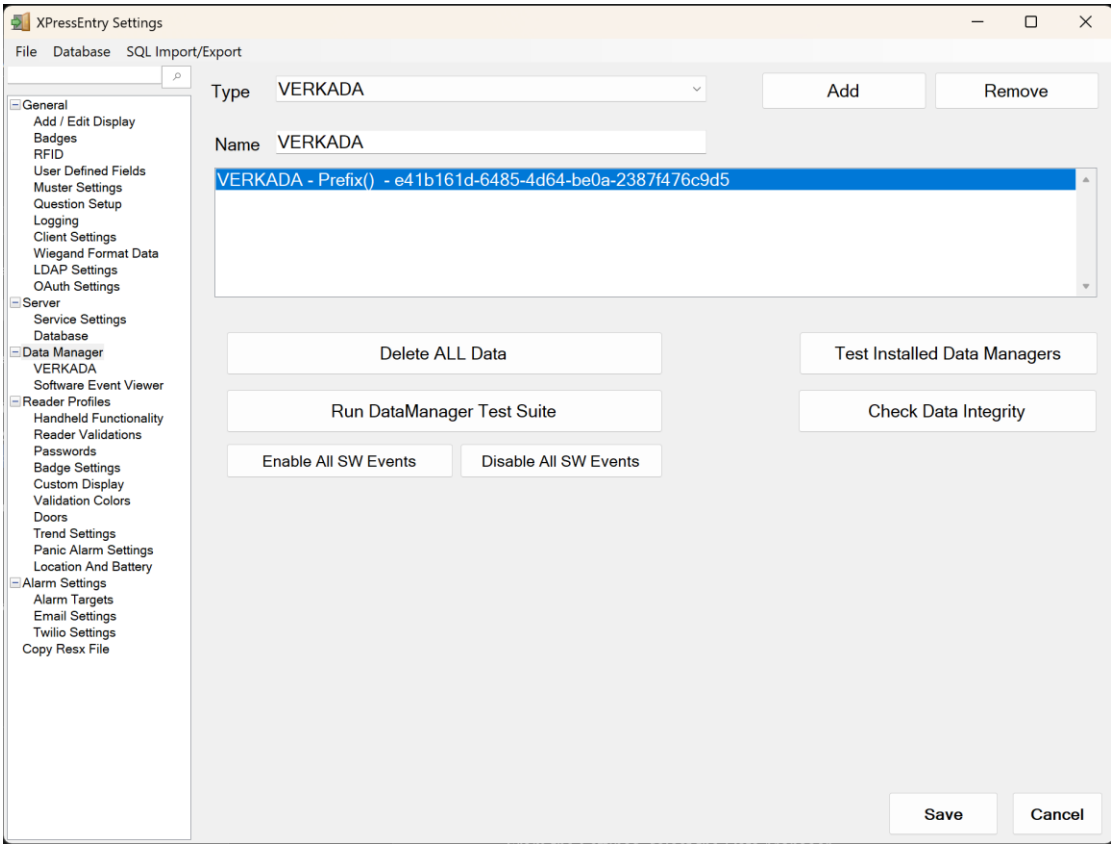
Enable XPressEntry Synchronization

XPressEntry uses a module called **Data Manager** to synchronize all data with Verkada.

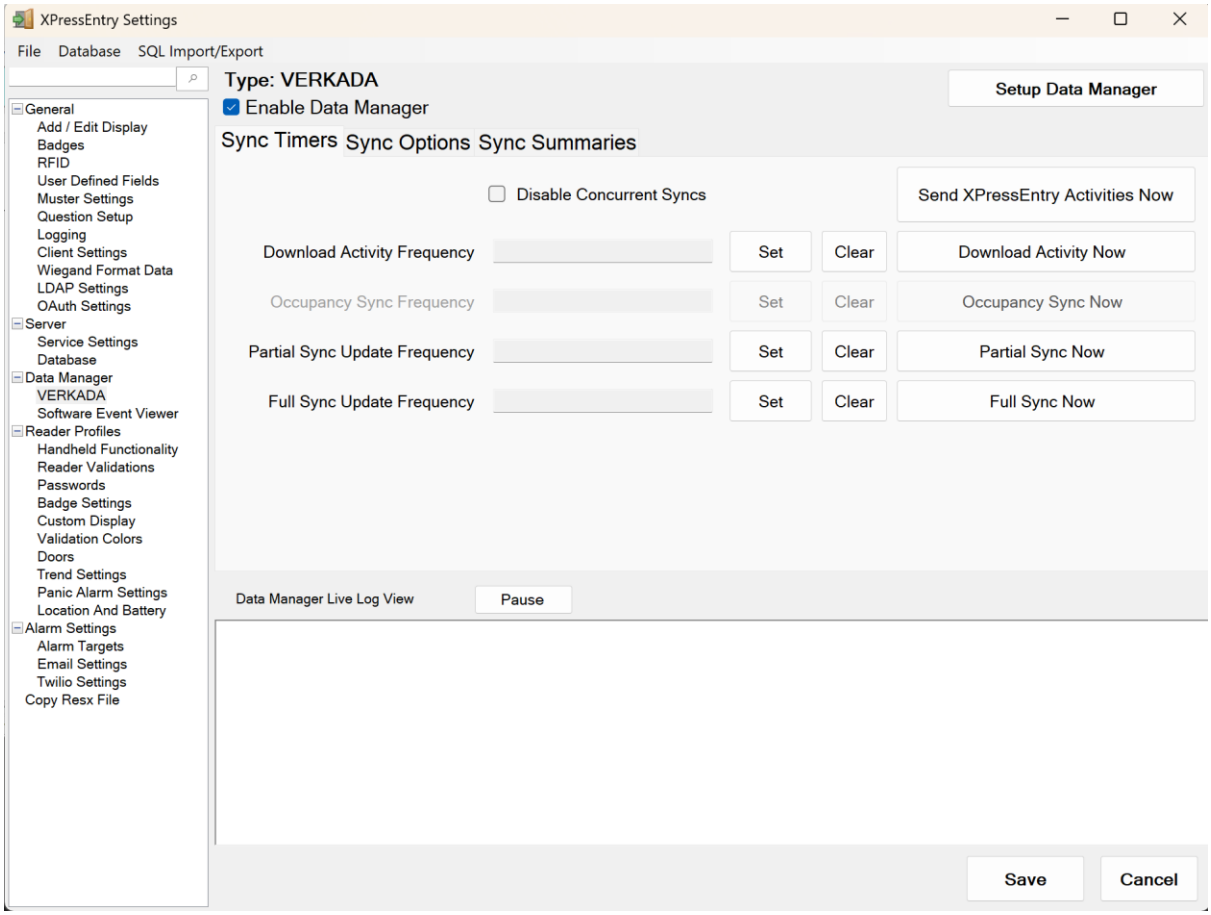
1. From the main page of XPressEntry, navigate to **Tools** > **Settings**.



2. Select the **Data Manager** tab and select **VERKADA** from the dropdown menu for **Type**. Click **Add**, then **Save**.



3. Once **VERKADA** is selected and saved as the type, select the **VERKADA** sub-settings tab. The following controls are available:
    a. **Enable Data Manager** – Check this box and click Setup Data Manager to configure Verkada-specific settings.
    b. **Type** – The integration type. Select VERKADA.
    c. **Setup Data Manager** – Opens the setup form for Verkada Data Manager settings.
    d. **Save and Apply Settings** – Saves all settings from the setup form, update frequencies, and activity synchronization options.
    e. **Update Frequency Options** – Sets and clears the intervals at which the Data Manager updates XPressEntry.
        i. Set the **Update Frequency** to the desired interval for full system updates. Note that only one update can run at a time; if this value is very low, the system will continuously attempt to update.
    f. **Sync Now Functions** – Runs an immediate update.
    g. **Send XPressEntry Activities Now** – Used to send XPressEntry handheld activities to Verkada.



Available Sync Types:

- **Full Sync Update** – Retrieves all relevant records from Verkada and updates them in XPressEntry. This sync can take time if there are a large number of users in Verkada.
- **Partial Sync Update** – Retrieves records for Doors, Access Groups, and Timezones only.
- **Activity Sync Update** – Pulls historic badge activities from the Verkada API.

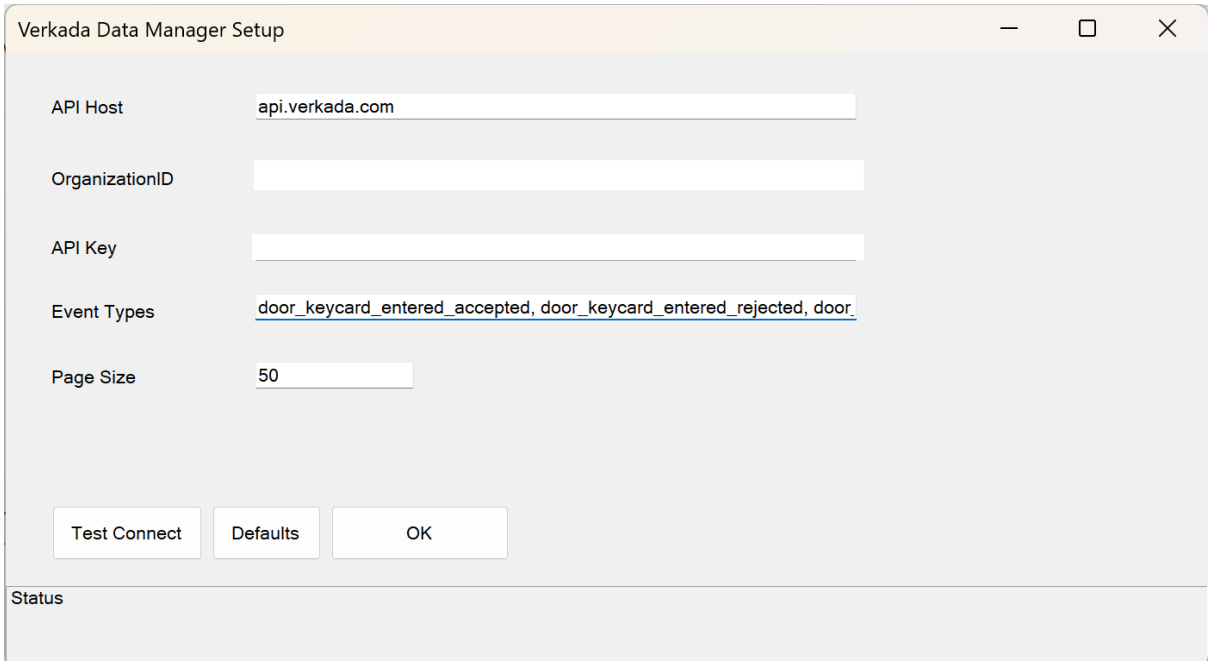
All options can be changed at any time and take effect immediately.

Configure Verkada Settings

Click Setup Data Manager and enter the following connection details:

- **API Host** – The URL of the Verkada API service.
- **Organization ID** – The Organization ID from the Verkada system.
- **API Key** – The API Key generated for XPressEntry in Verkada.

- **Event Types** – The event types to consider when fetching activities from Verkada.
- **Page Size** – The pagination size for API requests.



Click **Test Connect** after entering all details. This will attempt to connect to the Verkada API using the provided credentials. The result will display "Connection Success!" if connected successfully, or an error message if the connection fails.

The Defaults button clears all entered data and restores default values.

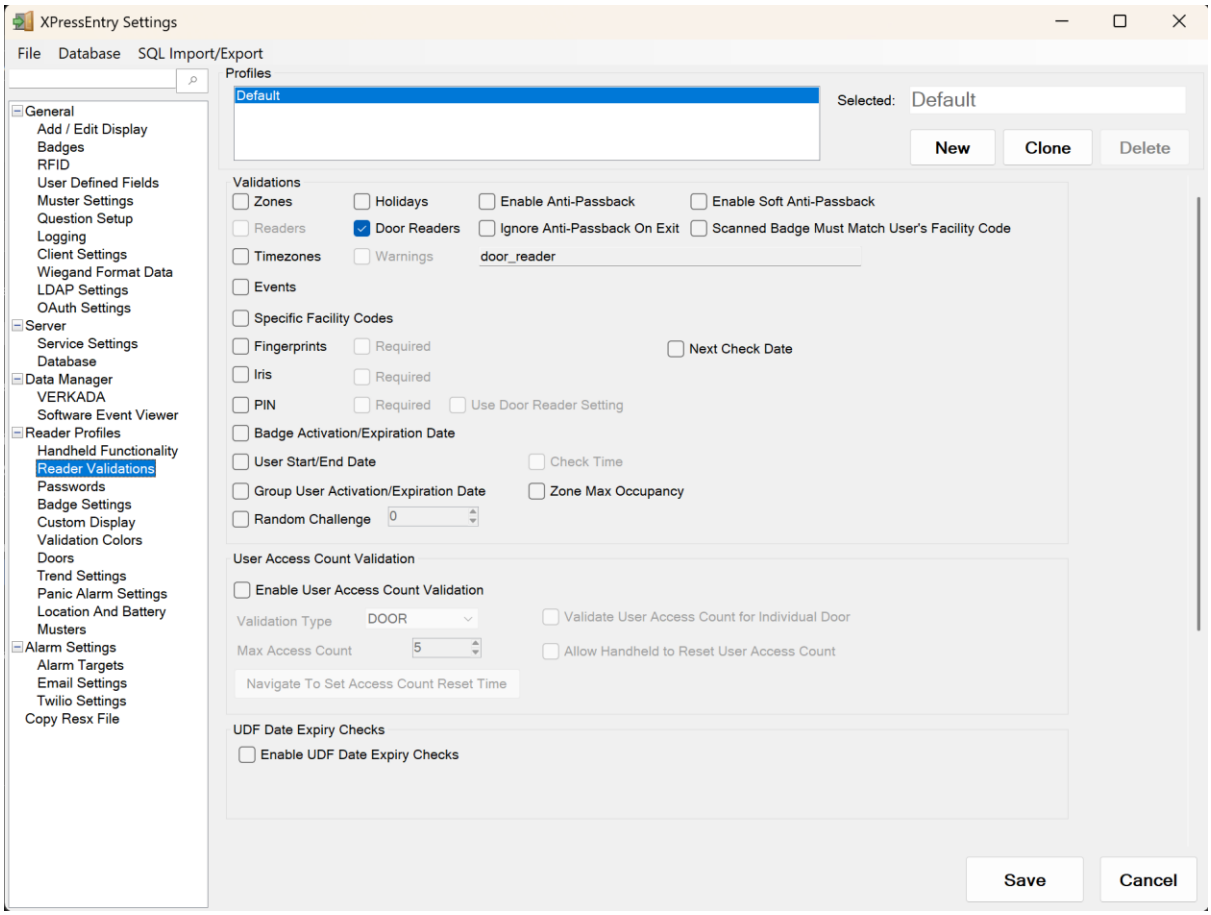
After closing the form, click **Save and Apply Settings** on the Data Manager tab. Then click **Full Sync Now** to pull all data from Verkada. Once the sync is completed, all relevant Verkada records will be available in XPressEntry.

Reader Profiles

The **Reader Profile** tab is where handheld devices are configured. Reader validations control which checks the handheld performs on each scan.

1. Go to **Tools** > **Settings** > **Reader Profiles** and enable the following validations:
    a. **Door Readers** – Required so the handheld only accepts scans from users with permission on the mapped reader.
    b. **Badge Activation** / **Expiration Date** – Enforces credential validity dates from Verkada.

2. Click **Save** at the bottom right when finished.



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

Verkada Sync Check

This section helps the administrator understand what data XPressEntry pulls from Verkada.

Verkada – XPressEntry Mapping

Mapping Data

The mapping of each data type pulled from Verkada is shown below:

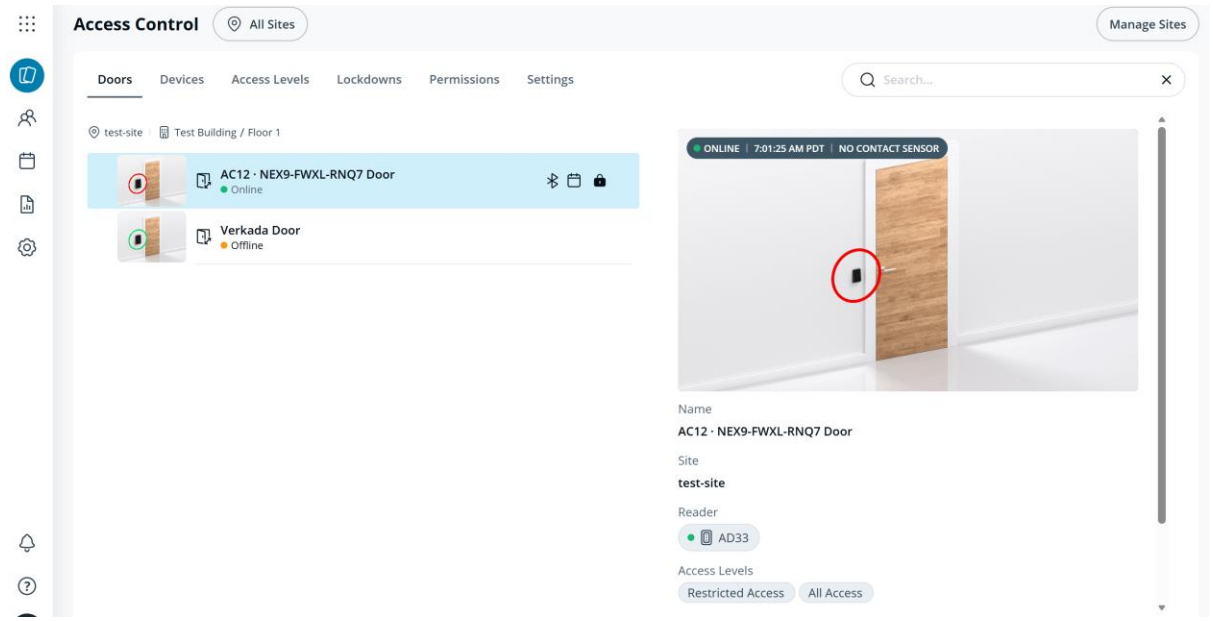
Verkada	XPressEntry
Device	Reader
Door	Door
Users	Users
Badges	Badges
Access Levels	Groups

Note: All external records sourced from Verkada will display in red as an "External Record" at the top of the form. This label will not appear for any records created from within XPressEntry.

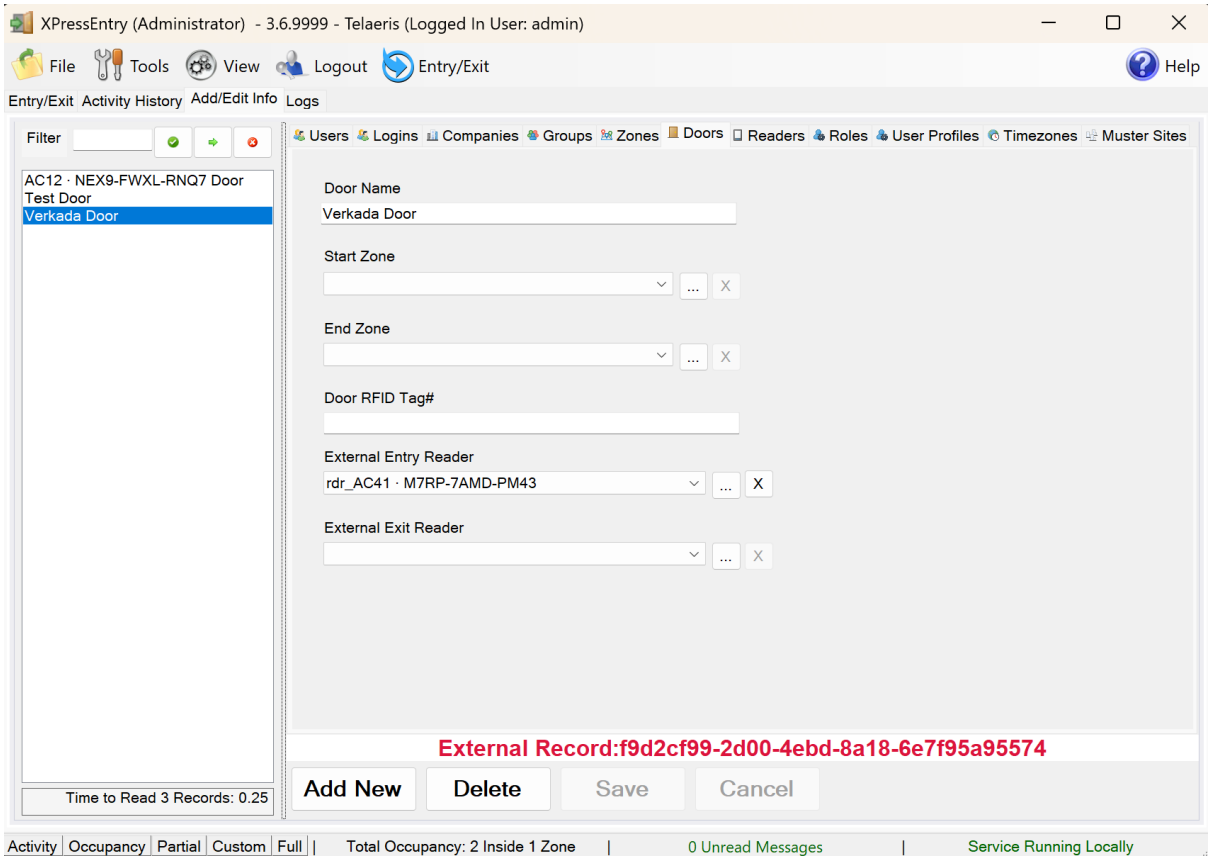
Doors

Doors are fetched directly from Verkada Doors. After a full sync, all Verkada doors will appear in XPressEntry with their corresponding configuration.

Verkada Doors



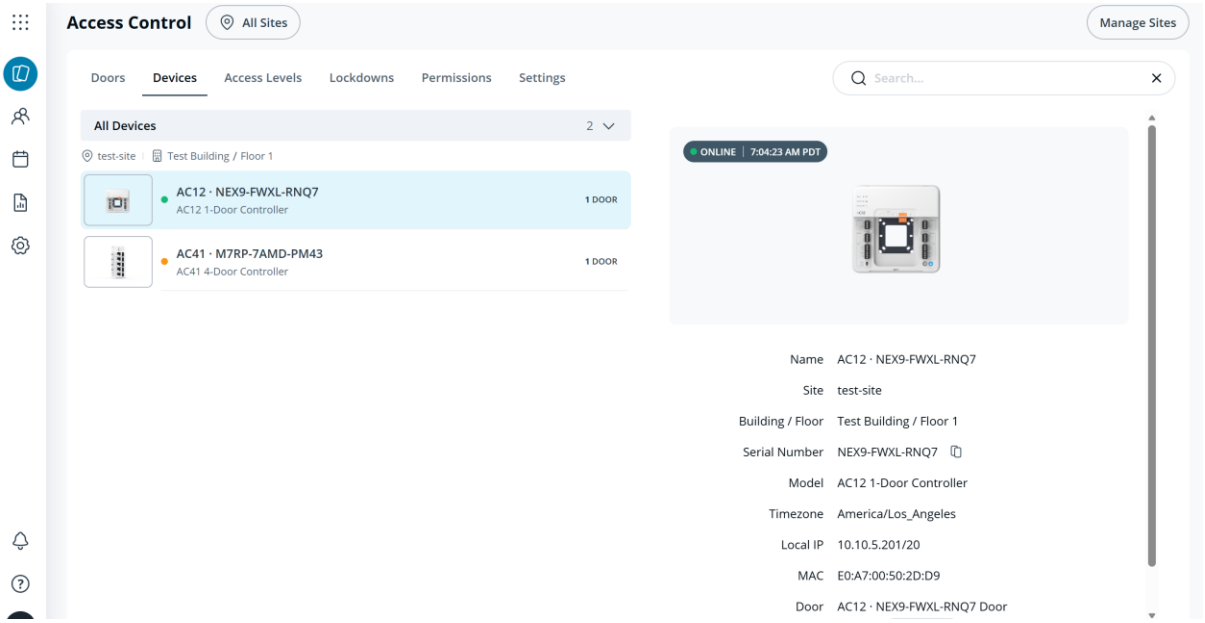
XPressEntry Doors



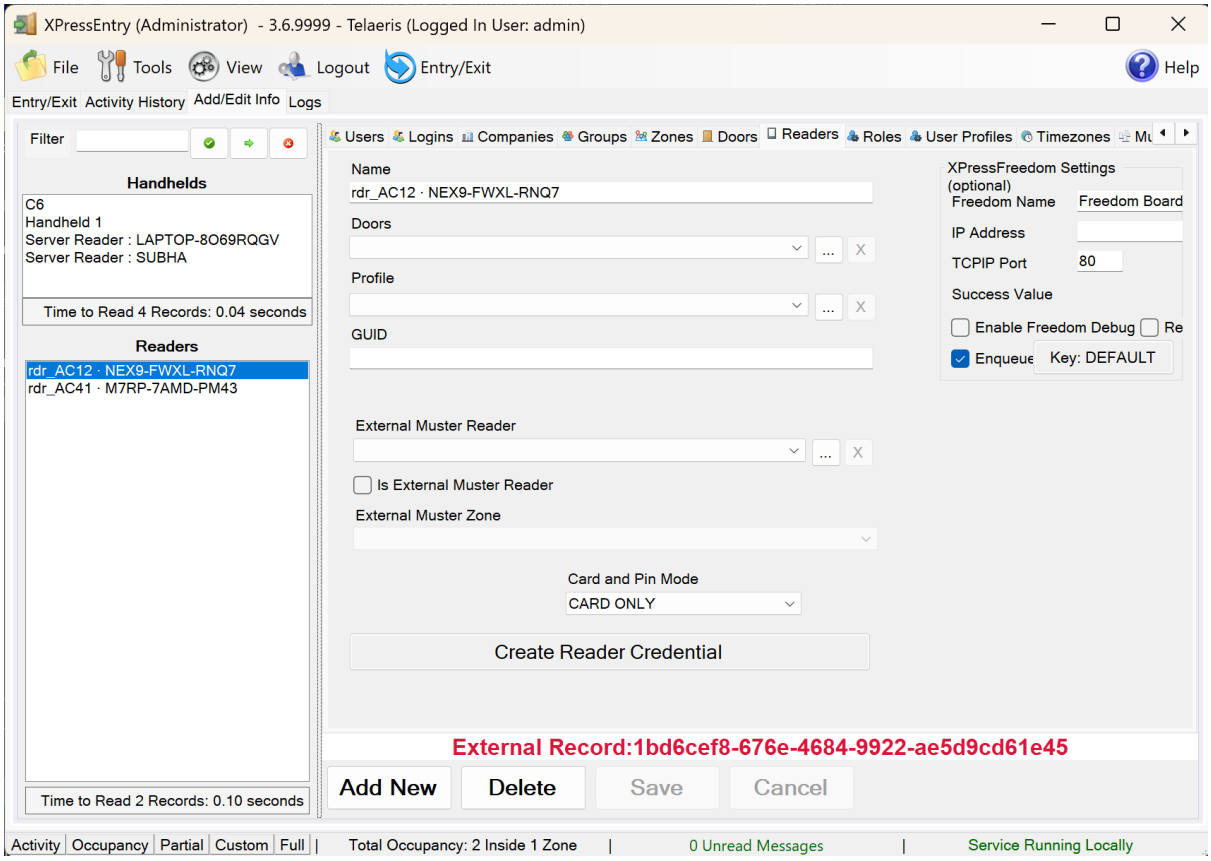
Devices / Readers

Devices from Verkada are synchronized and available in the XPressEntry Readers list. All devices from the Verkada system are mapped as **Readers** in XPressEntry.

Verkada Devices



XPressEntry Readers

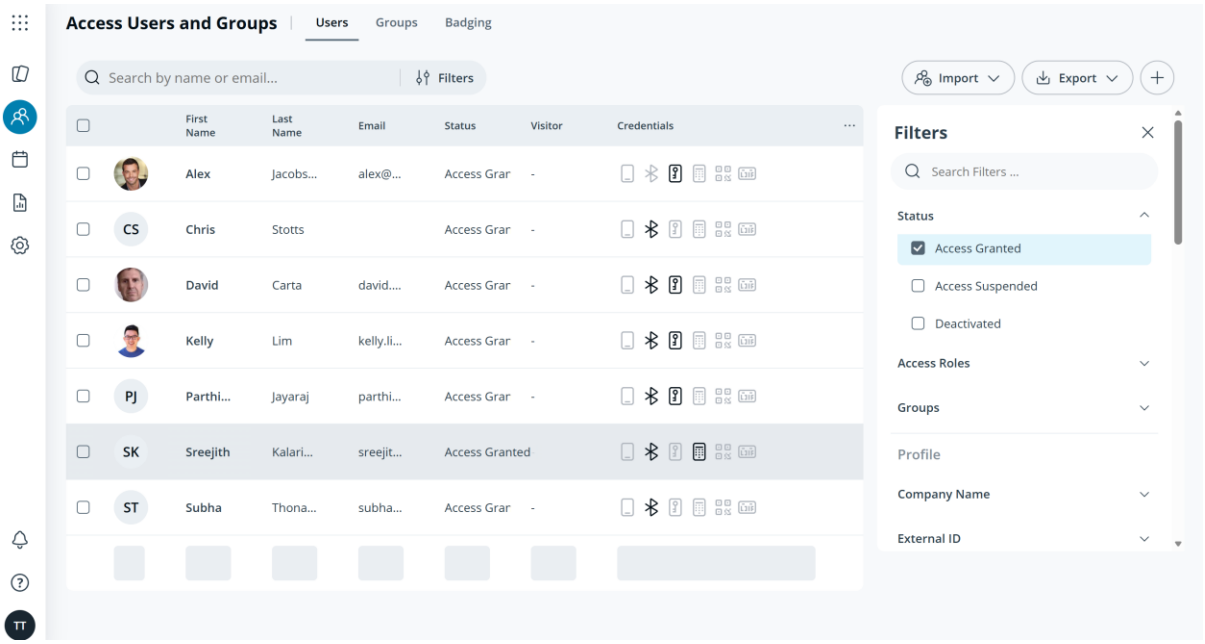


Users

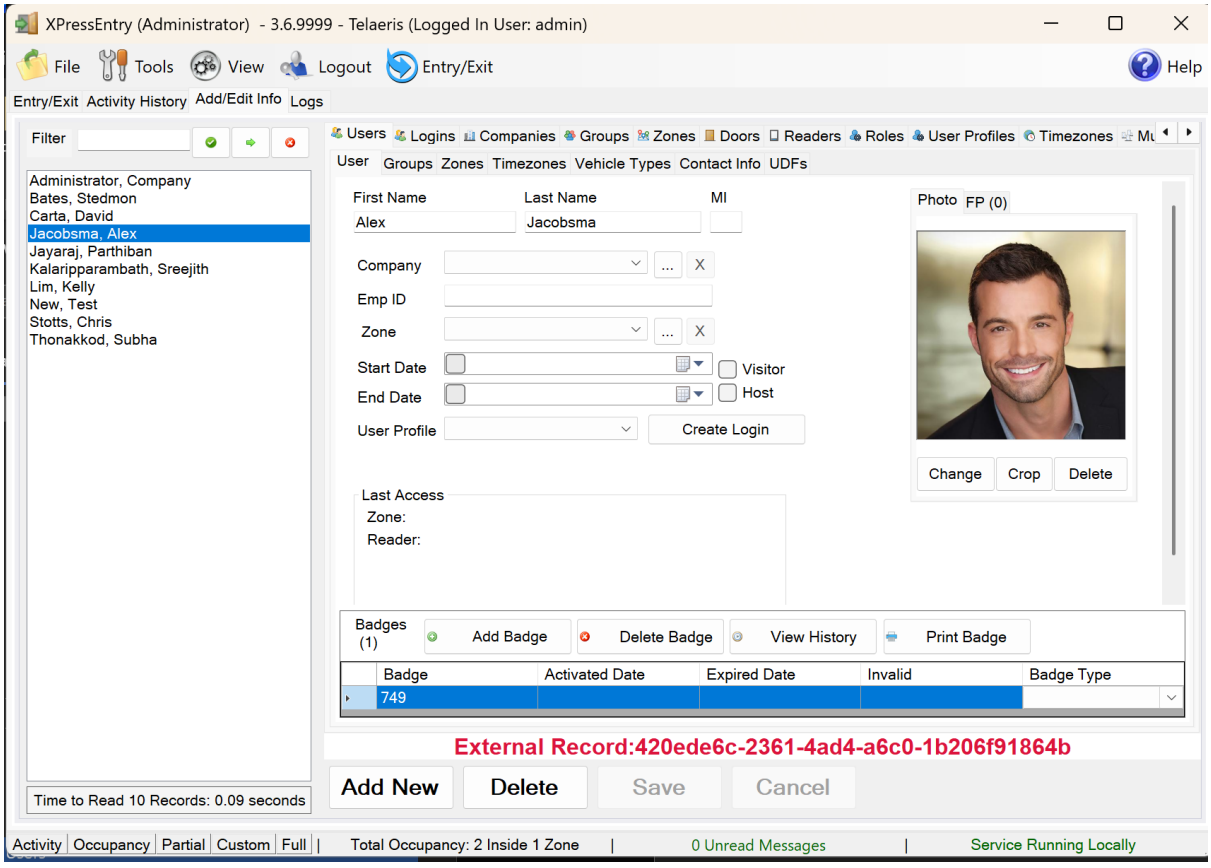
After a full sync, user profiles will be available in XPressEntry. XPressEntry pulls the following user information from Verkada:

- User profile information: **Name**, **Photo**.
- **Badge number** and credentials.

Verkada User



XPressEntry User

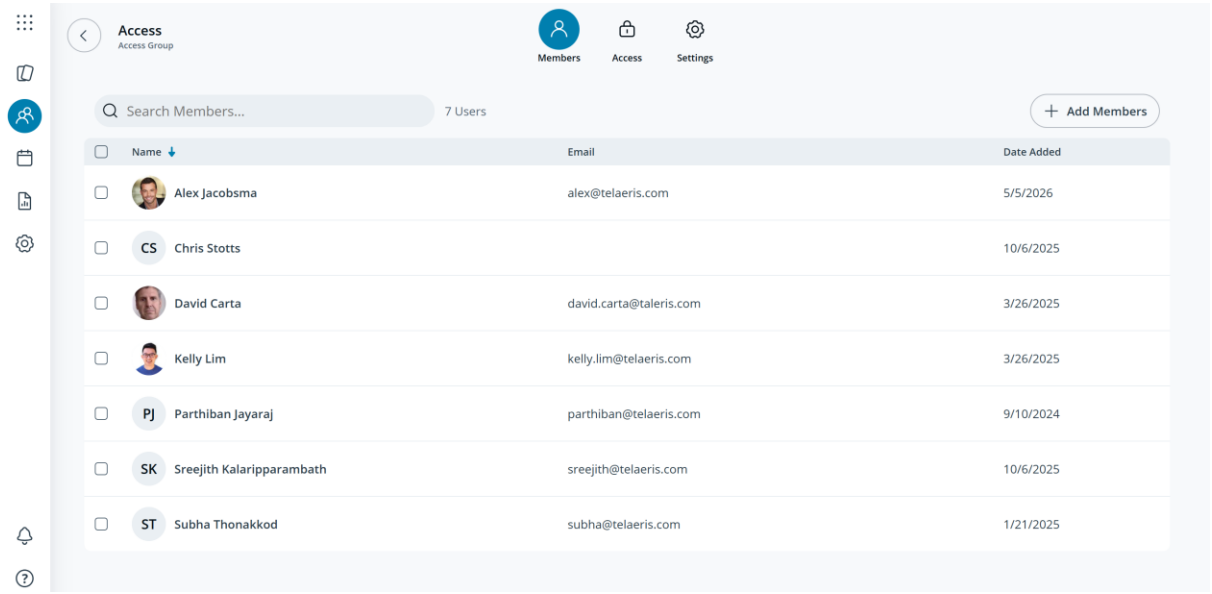


The badge number is displayed at the bottom of the user record screen.

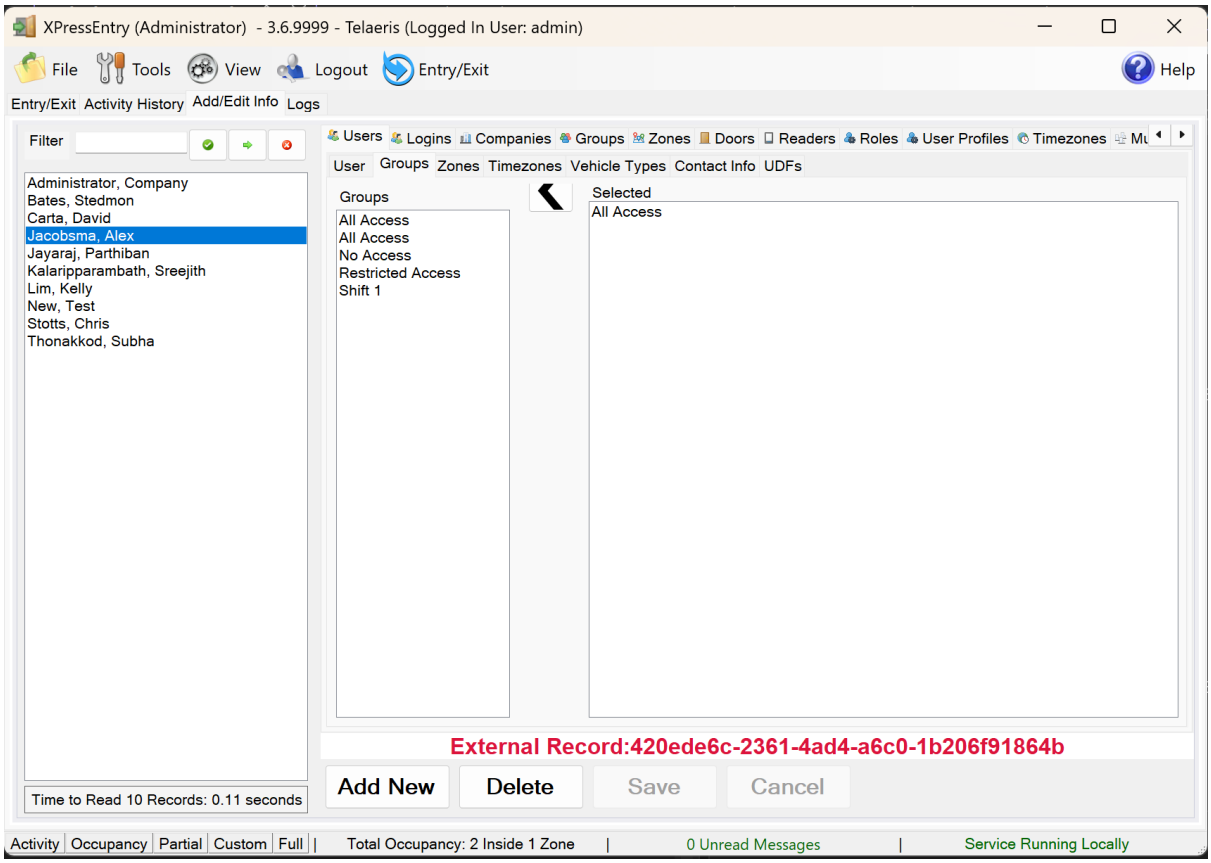
Direct Access Groups and Device Permissions / User Permissions

Direct Access Groups and **Device Permissions** assigned to a user in Verkada are combined and added to the **user's permissions** in the XPressEntry User tab.

Verkada User Access Rights



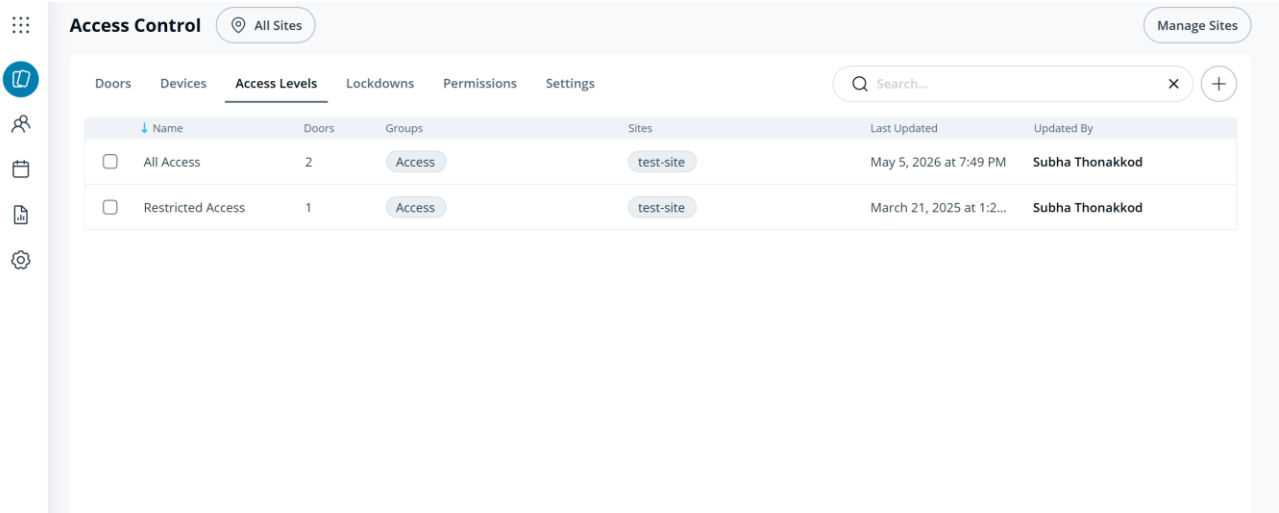
XPressEntry User Permissions



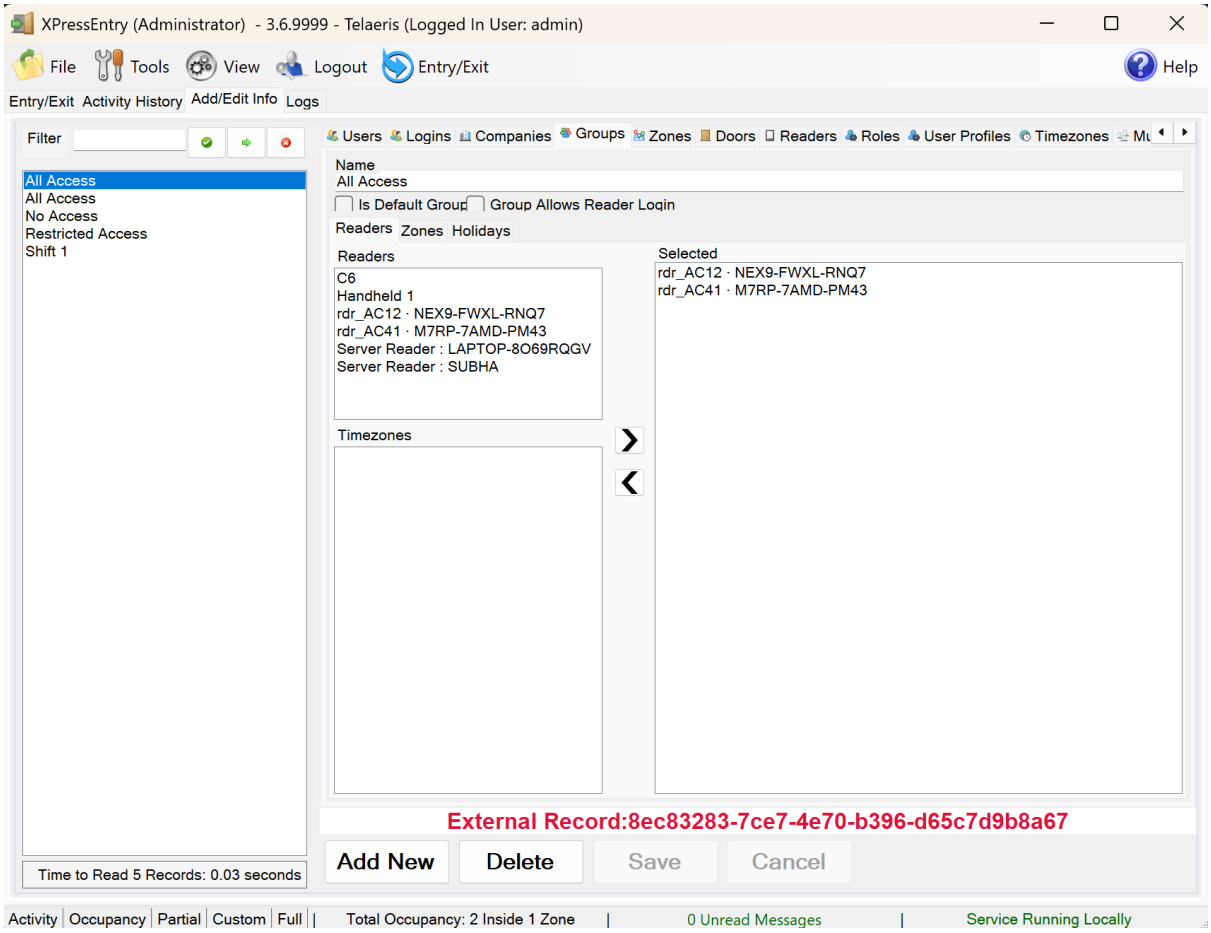
Access Groups / Groups

Access Groups from Verkada are mapped to **Groups** in XPressEntry. Each group includes the readers and schedules assigned to the corresponding **Access Level** in Verkada.

Verkada Access Groups



XPressEntry Groups

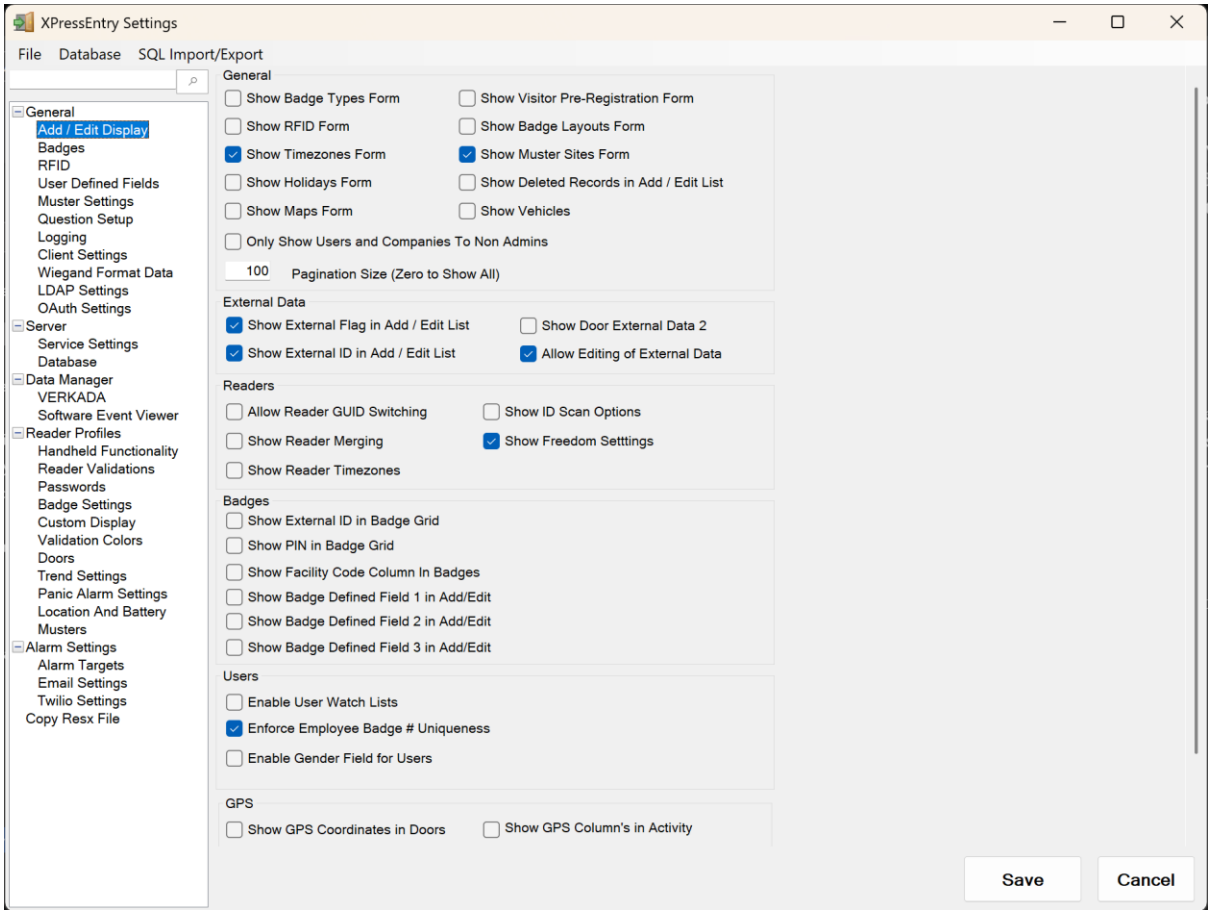


Configuring XPressEntry Using Verkada Data

Once XPressEntry has synced with Verkada, the system must be configured to use this data. The tabs that require configuration are **Doors**, **Readers**, and **Zones**.

Note: In XPressEntry, editing of external data is disabled by default. To enable editing, navigate to **Settings** > **General** > **Add/Edit Display** and check **Allow Editing of External Data** in the External Data section.

XPressEntry External Data Settings



Configuring Doors

Entry and exit permissions in XPressEntry are managed through doors. Each door contains two readers: an entry reader and an exit reader. Door access is determined by the user's access to the door's associated readers.

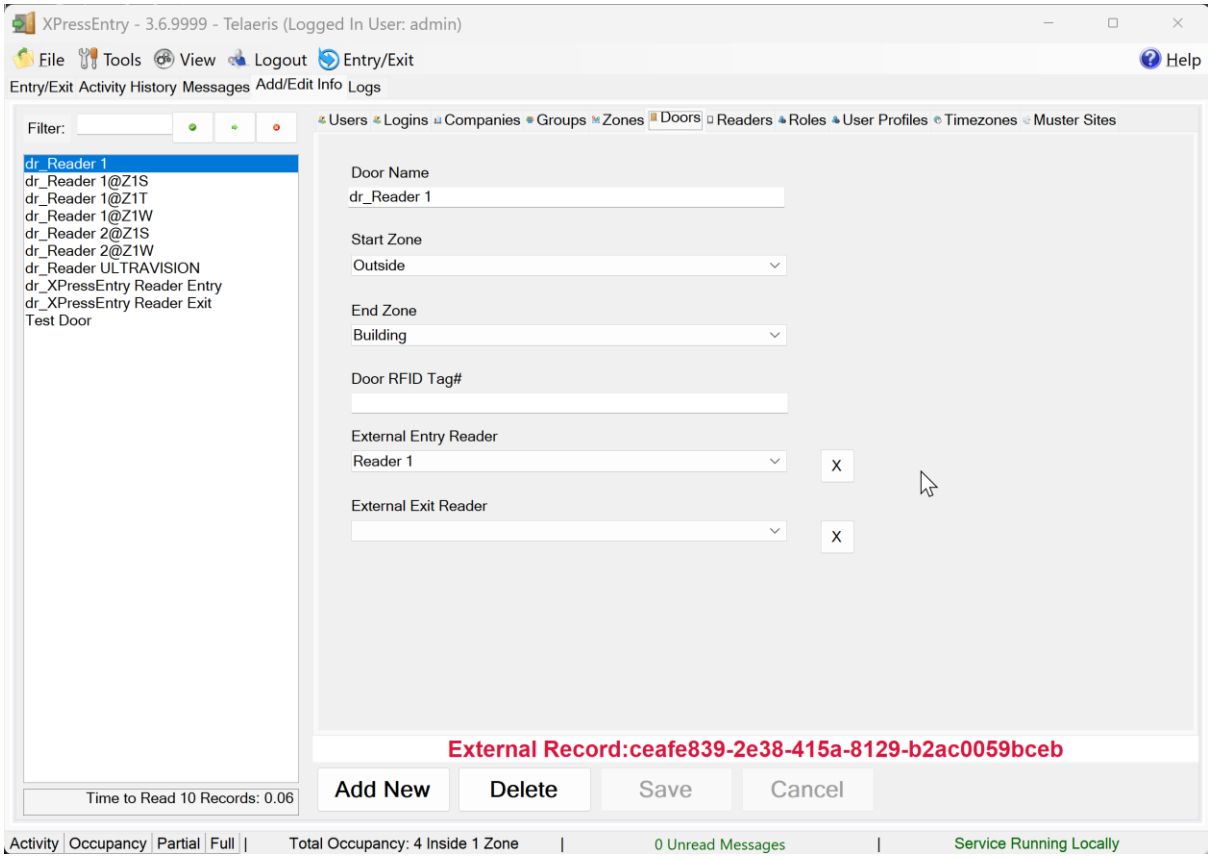
For entry, permission is based on the user's access to the door's external entry reader. For exit, permission is based on the user's access to the door's external exit reader.

There should be one door in XPressEntry for each physical station where a handheld device will be deployed.

For each door, configure the following after the first full sync:

- **Start Zone** and **End Zone** – Set manually so that user occupancy can be tracked. This will move a user into the specified zone when they enter or exit through the door.
- **External Entry Reader** – Automatically set to the reader created from the door. Verify this is correctly mapped.

XPressEntry Doors



Doors can also be added for each physical Verkada reader. If XPressEntry is configured to pull activities, it will move users within the system based on the reader they scanned at and the zones attached to that door.

Configuring Readers

In XPressEntry's Verkada integration, it is not necessary to pre-associate a reader in the system with a specific handheld device. This association can be made on the handheld itself at the time of scanning.

A handheld unit can logically represent any reader in the building. When a handheld is issued to an employee at a specific door, the employee sets the door on the handheld. The XPressEntry reader that the handheld represents is determined by whether it is in entry or exit mode.

Example Scenario:

> A handheld stationed at Door A (which has Reader A-Entry and Reader A-Exit) is set to Door A in entry mode. When a cardholder scans, the handheld identifies itself as Reader A-Entry and sends the activity to the server.

If that same handheld is moved to Door B and switched to exit mode, it identifies itself as Reader B-Exit and sends each outgoing scan accordingly.

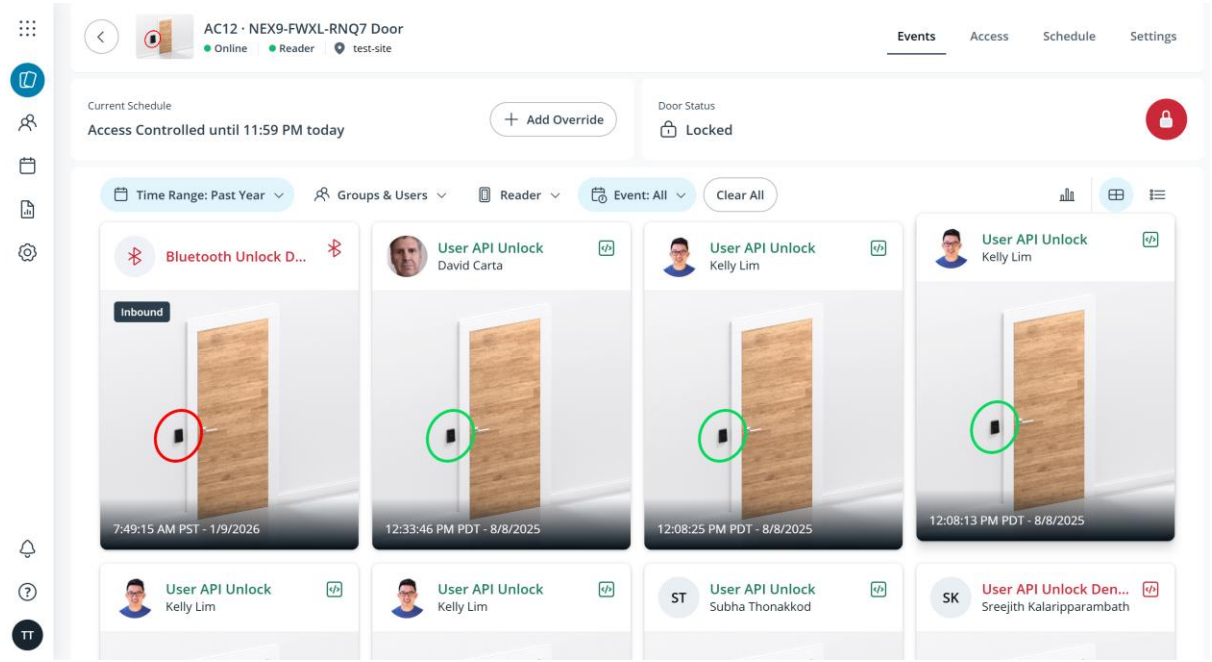
Activity Logging

XPressEntry can retrieve badge activities from Verkada and push XPressEntry handheld activities to the Verkada server. Both directions of activity flow support user occupancy tracking and allow viewing of handheld scan events within the Verkada event history.

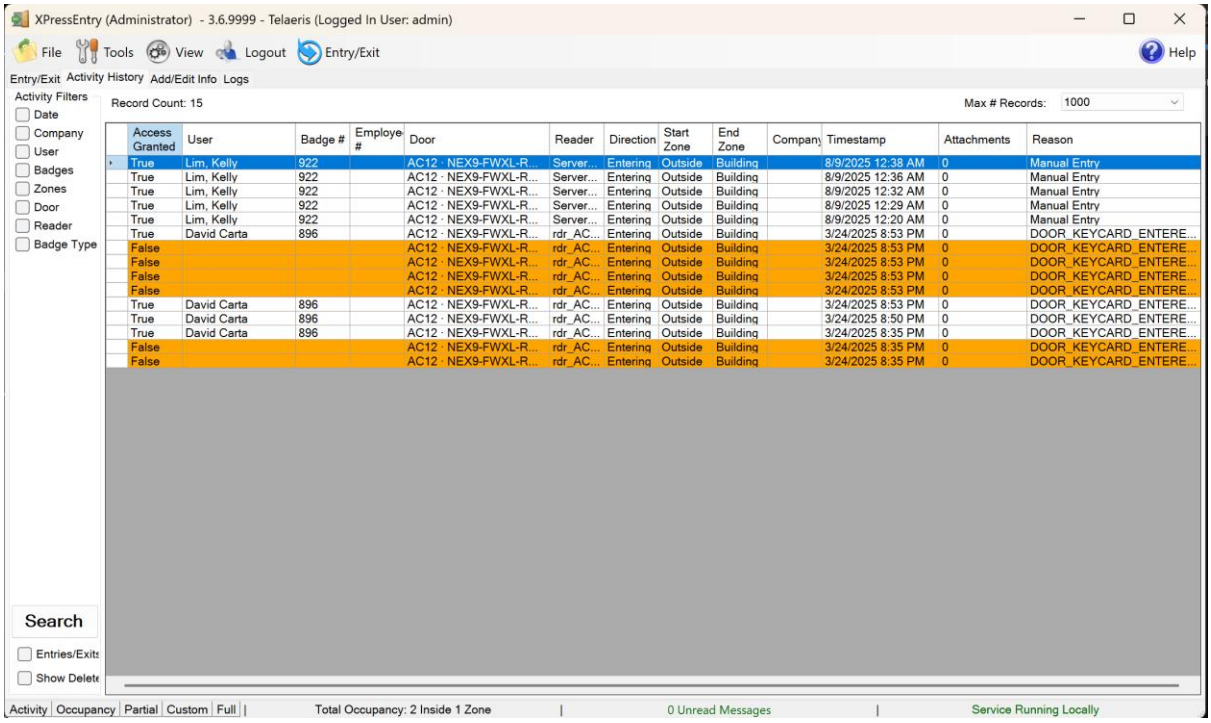
Activity records include the following fields:

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

Verkada Activity Reporting



XPressEntry Activity Reporting



Best Practices

Follow these recommendations to ensure a stable connection and ongoing success:

- **Daily Full Sync**
  - Schedule a full sync daily (e.g., 2:00 AM) to ensure data consistency, since Verkada does not support real-time or partial user updates.
- **Handheld Reader Mapping**
  - Map each handheld device to the physical Verkada controller it represents so that handheld activities are routed to the correct doors.
- **Zone Configuration**
  - Set Start and End Zones on each door so user occupancy is tracked accurately as people scan in and out.
- **API Logging**
  - Enable verbose API logging during initial setup and troubleshooting to capture detailed request and response data.
- **Connection Monitoring**
  - After saving settings, run Test Connect and confirm a "Connection Success!" message before relying on the sync.
- **Port Availability**

- Confirm that ports 30000 and 30001 remain open between the XPressEntry server and handhelds to avoid intermittent communication failures.

Troubleshooting

Connectivity Issues

- Verify the Verkada API host URL is correct and reachable from the XPressEntry server.
- Confirm the API user account has the required administrator permissions in Verkada Command.
- Check that the Organization ID and API Key are valid and entered without extra whitespace.
- Enable verbose API logging to capture detailed error messages from the Verkada API.

Sync Problems

- Run a manual Full Sync Now to re-synchronize the XPressEntry system with Verkada.
- Verify the Page Size setting is within Verkada's supported range; lower the value if large syncs time out.
- Check network connectivity and firewall rules between the XPressEntry server and command.verkada.com.
- Confirm that only one update is running at a time – if the Update Frequency is set too low, syncs may overlap and appear stuck.

Activity and Mapping Failures

- Confirm that handheld activities are reaching Verkada by reviewing the Verkada event history after a test scan.
- Verify that each XPressEntry door's External Entry Reader and External Exit Reader are mapped to the correct Verkada devices.
- Check that Access Levels in Verkada are assigned to the readers used by the integration.

Summary

The XPressEntry integration with Verkada provides a reliable solution for mobile access control management, supporting entry, exit, and mustering use cases. Proper configuration of handheld-to-reader mapping, zones, and sync options ensures accurate occupancy tracking and complete handheld activity history within Verkada Command.