XPressEntry

Web Console User Guide

Revision 06/09/2026

TELAERIS

Table of Contents

Purpose

This document provides a comprehensive guide to the XPressEntry Web Console - the browser-based management interface for the XPressEntry system. It is intended for security administrators, IT staff, and operators who configure, monitor, and operate XPressEntry handheld and fixed readers.

The guide covers the full scope of Web Console functionality, including initial setup, user and device management, live occupancy monitoring, Entry/Exit Mode, Emergency Mustering, Events Mode, reporting, and system configuration.

For additional assistance, contact the Telaeris support team at (858) 627-9700 or helpdesk@telaeris.com.

Welcome to XPressEntry

Concept

XPressEntry is a credential-validation and occupancy-tracking platform. Using handheld readers (XPID series), fixed kiosk readers (XPIK), and tablet readers (XPIT series), security operators verify that personnel entering a facility are authorized, capture real-time entry and exit events, track zone occupancy, and run emergency mustering events.

The XPressEntry Web Console is the central management interface for the entire XPressEntry system. Unlike the legacy desktop application, the Web Console runs entirely in a modern web browser and requires no local software installation on operator workstations. Administrators and operators can use any device - desktop, laptop, tablet, or phone - to access the full system.

Common Use Cases

XPressEntry supports a wide range of security and safety applications:

- Entry/Exit Tracking
- Employee Credential Validation
- Emergency Mustering and Evacuation Tracking
- Confined Space Management
- Visitor Management
- Events and Training Attendance
- Remote Parking Validation
- Guard Tour
- Handheld Enrollment

XPressEntry operates as a fully stand-alone system or integrates with access control systems (Lenel OnGuard, Honeywell Pro-Watch, CCure 9000, Galaxy, and others), RTLS, time-and-attendance platforms, and other enterprise systems.

System Architecture

- XPressEntry Service - Background Windows service that manages the database, communicates with handheld readers, and syncs with integrated access control systems.
- XPressEntry Web Console - Browser-based administration and monitoring interface.
- Handheld / Fixed Readers - XPID, XPIK, and XPIT devices that scan badges and biometrics in the field and sync activity to the server.

Security and Access

For on-premises XPressEntry deployments, the Web Console is securely hosted within the corporate LAN behind the firewall and is accessed over HTTPS. It accesses the same SQL Server database as the XPressEntry Service.

Telearis hosted XPressEntry deployments are stored on Oracle Cloud. All data in transit is encrypted using TLS 1.3.

Solutions Overview

XPressEntry is a flexible platform that supports a wide range of physical security and workplace safety solutions. The Web Console is the central interface for configuring and monitoring all of them. The sections below describe each solution, its purpose, key capabilities, and how it is managed through the Web Console.

Emergency Mustering and Evacuation Tracking

XPressEntry Emergency Mustering is a premier solution for accelerated emergency evacuations and roll call. Using rugged handheld badge readers, security and safety teams can monitor facility occupancy in real time and ensure all personnel are accounted for during emergencies and drills.

In a real emergency, every second matters. Assembly areas are often located far from existing door readers, and personnel may not follow expected evacuation routes. XPressEntry solves this by mobilizing the access control system with handheld readers that work on-site, off-site, and in locations with no infrastructure at all.

Key Capabilities:

- Roll Call from Any Location - Verify who is safely accounted for at evacuation assembly areas or muster points, on-site or at remote locations.

- Live Personnel Tracking - Mobile roster lists instantly update across all connected devices, ensuring accurate tracking of personnel locations and status.
- Missing Persons List - Provide first responders with names, ID photos, and the last recorded location of any missing persons on-site.
- Multi-Modal Mustering - Account for employees via badge scanning, SMS text messages, RTLS, app self-mustering, and biometrics including facial recognition.
- Offline Mode - If connectivity is lost, handhelds continue to record all activities and re-sync automatically when connectivity is restored.
- Relocatable Muster Points - Adjust evacuation sites on the fly when assembly areas become unsafe due to fire, smoke, gas leaks, or structural hazards.

Web Console Role: Administrators configure muster zones, muster sites, alert notifications, and Reader Profiles from the Web Console. Real-time muster status is monitored live, and muster events are finished and reported from the Web Console.

Handheld Badge Verification

XPressEntry handheld badge readers extend access control beyond fixed door readers, enabling security personnel to verify credentials from anywhere - main entrances, secondary doors, restricted zones, remote gates, and outdoor areas where wired infrastructure is not available.

Handheld readers pull identity details directly from the access control system database, displaying the badge holder's photo for visual confirmation. Every scan is logged in real time and synced to the XPressEntry server and the integrated PACS.

Key Capabilities:

- Mobile Badge Authentication - Instantly verify employee and visitor credentials against the access control system from anywhere.
- Visual Identity Verification - Displays the badge holder's photo on the handheld to confirm the person presenting the credential matches the authorized identity.
- Access Control Anywhere - Control access at remote sites, temporary entrances, or locations where door readers are not practical or available.
- Entry/Exit Tracking - Logs all personnel and visitor activity in real time, maintaining accurate facility occupancy records.
- Real-Time Sync - All connected handhelds remain in sync with the access control system and with each other.
- Offline Mode - Continues recording activity if connectivity is lost and re-syncs automatically when restored.

Web Console Role: Reader Profiles control which badge technologies are enabled and how each handheld behaves. Live badge scan activity is visible in the Occupancy and Activity History tabs.

Entry/Exit Tracking

XPressEntry Entry/Exit Tracking provides real-time personnel movement tracking at any access point. Handheld badge and biometric readers validate credentials and record entries and exits wherever access control is needed - including locations where traditional wired door readers are not practical or available.

Key Capabilities:

- Access Control Anywhere - Authenticate credentials at workplace entrances, vehicle gates, remote sites, construction perimeters, and shuttle boarding points.
- Live Badge Verification - Validate badges instantly against the identity information on record in the access control system.
- Complete Audit Trail - Maintains a time-stamped record of all entry and exit activity across every reader.
- Confined Space Support - Track personnel entering and exiting restricted areas such as utility vaults, tunnels, and tanks where wired infrastructure is unavailable.
- Bus and Shuttle Boarding - Authenticate employees as they board and exit shared vehicles, ensuring workers board the correct routes and tracking movements between locations.
- Offline Mode - Continues recording if connectivity is lost; all activity syncs automatically when connection is restored.

Web Console Role: Doors, Zones, and Reader Profiles are configured in the Web Console to define where Entry/Exit tracking takes place and what behavior is applied. The Activity History tab and Occupancy dashboard provide live and historical visibility into all tracked movements.

Mobile Biometric Authentication

For high-security areas where absolute identity certainty is required, XPressEntry supports multi-factor biometric authentication on compatible handheld readers. Biometric modalities include facial recognition, iris scanning, and fingerprint verification, used alone or in combination with badge scanning and PIN.

XPressEntry biometric handhelds are designed for environments such as government facilities, airports, laboratories, and industrial sites where standard badge verification alone is not sufficient. They support both online and offline operation, authenticating from an offline database or from biometrics stored directly in the personnel badge when connectivity is unavailable.

Key Capabilities:

- Multi-Factor Authentication - Combine facial recognition, iris, fingerprint, badge, and PIN in any combination for layered identity assurance.
- Facial Recognition - Quickly authenticate personnel without requiring a physical badge - ideal for mustering, high-throughput entry points, and contactless workflows.

- Biometric Enrollment from Anywhere - Enroll new personnel and visitors into the access control database directly from the XpressEntry handheld reader.
- Offline Biometric Authentication - Authenticates from a locally cached database or badge-stored biometrics when connectivity is unavailable.
- Certified PACS Integrations - Natively certified with 30+ leading PACS platforms including LenelS2, Honeywell, Genetec, Software House, AMAG, RS2, Galaxy, and more.

Web Console Role: Biometric features are enabled per Reader Profile in the Web Console under Handheld Functionality and Scan Settings. User biometric data (photo, fingerprint) is managed in Users.

Employee Surveys

XPressEntry Surveys adds a survey and questionnaire capability to the handheld badge verification workflow. After scanning a badge to confirm identity, operators are presented with a customizable set of questions configured for that access point. Survey responses are recorded directly into XPressEntry and can be used to allow or deny access, update employee status in a backend system, or collect information for compliance and evaluation purposes.

Survey applications include health screenings, safety protocol acknowledgements, license or certification verification, consent to policies, COVID-19 symptom checks, and more. Different question sets can be deployed to different readers at different access points.

Key Capabilities:

- Custom Survey Questions - Create unlimited sets of survey questions tailored to specific business needs and access points.
- Access Denial Based on Responses - Deny entry when survey responses indicate a safety or compliance concern.
- Bluetooth Health Measurements - Capture measurements from compatible Bluetooth devices (e.g., temperature sensors) directly on the handheld during the survey.
- Secure, Role-Restricted Data Storage - Survey responses are encrypted and stored on the XPressEntry server. Visibility can be restricted by role, and sensitive data can be auto-purged after a defined period.
- Per-Location Survey Deployment - Assign different survey question sets to different readers for targeted screening at each access point.
- Offline Operation - Survey results are stored locally on the handheld and synced to the server when connectivity is restored.

Web Console Role: Survey question sets are created and managed in the Web Console and assigned to Reader Profiles. Survey response data and access decisions are visible in the Activity History tab.

Confined Space Management

XPressEntry provides a specialized entry / exit tracking and accountability solution for large, multi-entry confined spaces - areas such as heat exchangers, tanks, tunnels, vaults, and manholes where OSHA regulations require employers to control access, maintain accurate occupancy records, and ensure all workers have exited safely.

Traditional paper rosters at confined space entry points are slow and error prone. XPressEntry replaces them with real-time handheld badge scanning that maintains continuous occupancy and provides instant confirmation that all workers have exited at the end of each work period.

Key Capabilities:

- Real-Time Entry and Exit Tracking - Track workers entering and exiting large, multi-entry confined spaces with handheld readers that maintain live occupancy counts and time-in-space records.
- Restricted Access Enforcement - Cross-validate worker credentials against access control rules, training records, and safety certification requirements to deny unauthorized entry.
- Multi-Entry / Multi-Exit Support - Workers can enter through one access point and exit through a different one in spaces with multiple points of egress.
- Instant Clearance Verification - Confirm the confined space is clear in seconds rather than the 30+ minutes typically required to reconcile paper rosters.
- Audited Compliance Records - The XPressEntry server centralizes and securely stores all confined space event details, providing easily generated compliance reports.
- Cellular, Wi-Fi, and Offline Operation - Operates reliably at remote locations with limited or no connectivity, syncing all data when connection is available.

Web Console Role: Confined spaces are configured as Zones in the Web Console, with Doors defining each access point. Reader Profiles can enforce credential and certification checks. Zone occupancy and activity are monitored in real time.

Guard Tour

Guard Tour is built directly into XPressEntry, extending the platform security teams already use in the field to include scheduled patrol route management, GPS checkpoint tracking, incident reporting, and guard accountability - all from the same XPID series handheld badge and biometric readers, managed from the Web Console.

Guards authenticate at the start of each patrol by scanning their own badge, creating a verified record of who performed the patrol. Checkpoints throughout the facility are scanned using RFID tags, NFC tags, QR codes, or barcodes. All patrol activity is uploaded to the Web Console in real time.

Key Capabilities:

- Scheduled Guard Patrol Routes - Configure recurring patrol routes and schedules directly from the XPressEntry Web Console.

- GPS Guard Patrol Tracking - Visualize patrol routes and checkpoint scans on interactive maps in both the handheld reader and the Web Console.
- Incident Reporting During Patrols - Capture photos, video, audio recordings, and written notes on the handheld to document security incidents in real time.
- Flexible Checkpoint Technologies - Supports RFID tags, NFC tags, QR codes, and barcodes to accommodate different security levels and deployment environments.
- Patrol Alerts and Notifications - Automatic email alerts notify supervisors when patrol routes are overdue, checkpoints are missed, or incidents are reported.
- Guard Authentication - Guards scan their badge to log in to Guard Tour mode, creating a verified, auditable record of who performed each patrol.
- Offline Operation - Patrols continue without connectivity; checkpoint data syncs automatically when the device reconnects.

Web Console Role: Patrol routes, checkpoint locations, and schedules are configured and monitored from the Guard Tour section of the Web Console. Incident reports and patrol history are stored and accessible in the Web Console. GPS patrol maps and missed checkpoint alerts are reviewed by supervisors in the Guard Tour view.

Accessing the Web Console

Browser Requirements

The XPressEntry Web Console supports all modern web browsers. Recommended browsers include:

- Google Chrome (latest)
- Microsoft Edge (latest)
- Mozilla Firefox (latest)
- Apple Safari (latest)

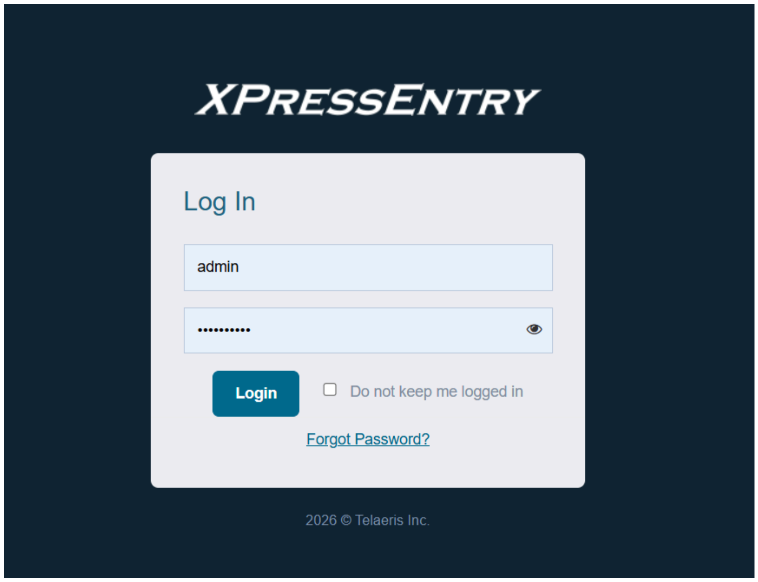
No plugins or local software installation is required. JavaScript must be enabled.

Connecting to the Console

Navigate to the Web Console URL provided by the administrator.

Logging In

The user enters their username and password on the login page and clicks Login.

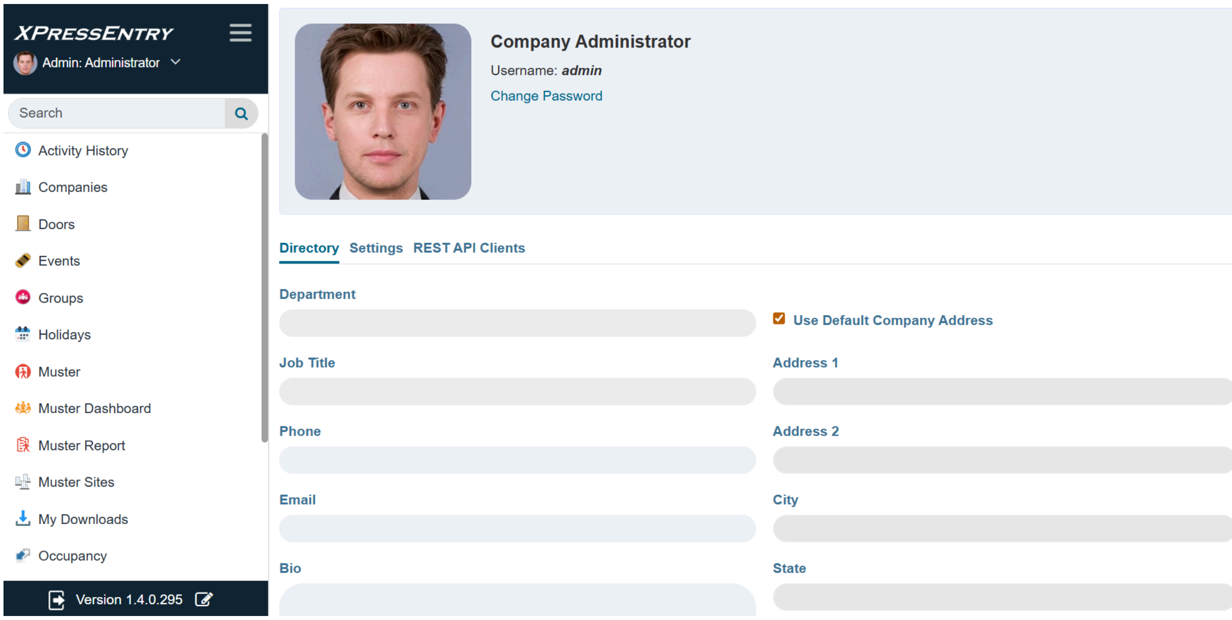


Web Console Interface Overview

Layout

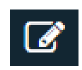
After logging in, the Web Console is organized into three primary areas:

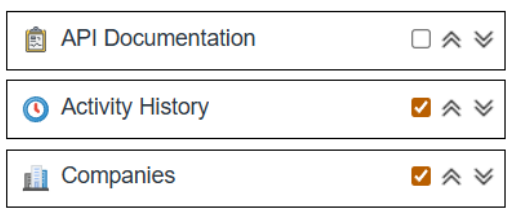
- Left Navigation Sidebar - List of available tabs/pages. Select any tab to view or edit its details. Use the search field to locate tabs quickly.
- Top Header Bar - Displays the current user's name and a user menu for Profile settings and Logout. Also contains the collapse icon.
- Main Content Area - Displays the active section - dashboards, data grids, forms, and configuration screens.



Navigation Tabs and Customization

The tabs displayed in the left navigation panel can be customized to show or hide sections relevant to a user's role:

1. Click the Edit icon in the bottom-left corner of the navigation panel. 
2. Check or uncheck the checkboxes for the pages to show or hide.



3. Rearrange tabs by dragging them, or sort alphabetically using the sort icons at the bottom.

4. Click **Save**.

Minimizing the Sidebar

The left navigation sidebar can collapse to give more screen space to the main content area. Click the collapse icon in the top right corner of the sidebar to minimize it. Click it again to expand. Tab icons remain visible in the collapsed state so you can still navigate quickly.

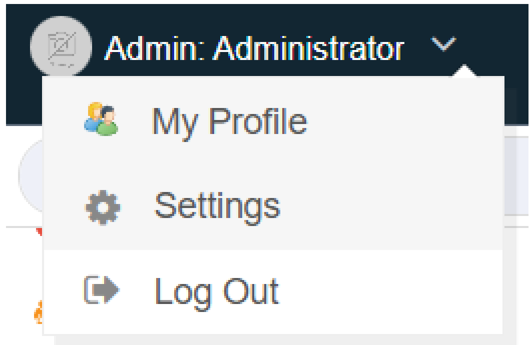
Available Tabs

Tab	Description	Tab Image
Activity History	Searchable log of all historical badge scan activity with date, user, door, zone, and reader filtering. Supports CSV and PDF export.	Activity History
Companies	Add and manage company records associated with badge holders in the system.	Companies
Doors	Define and configure physical access points, including their start and end zone assignments.	Doors
Events	Create and manage attendance events. Add attendees, run events on handhelds, and view or export attendee reports.	Events
Groups	Create access groups and assign users and authorized zones to control access privileges.	Groups
Holidays	Define holiday schedules that can be assigned to groups to restrict access on specified dates.	Holidays
Muster	Emergency mustering event management - Missing and Scanned lists, event controls, and real-time accountability status.	Muster
Muster Dashboard	Visual overview of active muster event status, showing occupancy and accountability across all muster zones at a glance.	Muster Dashboard
Muster Report	Review, filter, and export reports from completed muster events, including Scanned and Missing personnel lists.	Muster Report
Muster Sites	Configure muster site groupings that scope which zones and readers a handheld monitors during a muster event.	Muster Sites
My Downloads	Access reports and exports that have been queued for download or emailed to the user.	My Downloads

Tab	Description	Tab Image
Occupancy	Real-time zone occupancy counts. Click any zone for a detailed list of personnel currently inside.	Occupancy
Print Layouts	Configure and manage badge print layout templates for badge printing workflows.	Print Layouts
Reader Profile	Create and edit Reader Profiles that define the modes, scan types, and features available on handheld devices.	Reader Profile
Readers	Add, configure, and monitor all connected handheld and fixed reader devices.	Readers
Reports	Build and schedule Dynamic and Advanced reports. Export activity data for compliance, auditing, and operational review.	Reports
Roles	Define Web Console user roles and their associated permissions, controlling what each user can see and do.	Roles
Timezones	Create time zone schedules that define the days and hours during which access is permitted for users or groups.	Timezones
User Logins	View and manage Web Console login credentials for system users.	User Logins
User Profiles	Review and edit detailed user profile information including contact details, photos, and biometric data.	User Profiles
Users	Add and manage all badge holder records including credentials, group assignments, certificates, and activity history.	Users
Zones	Define physical areas in the facility and designate them as Hazard Areas, Muster Points, or Outside Areas.	Zones

User Profile and Permissions

Click the username in the top left corner to access the My Profile menu. From here, the user can:



- Change the password, Startup view, Contact Information, etc.
- Access additional Web Console Settings
- Log out

Access to specific tabs and functions is controlled by the Role assigned to each user. Roles are configured under the Roles tab. Only users with the Admin role have access to all settings and configuration functions by default.

Data Management

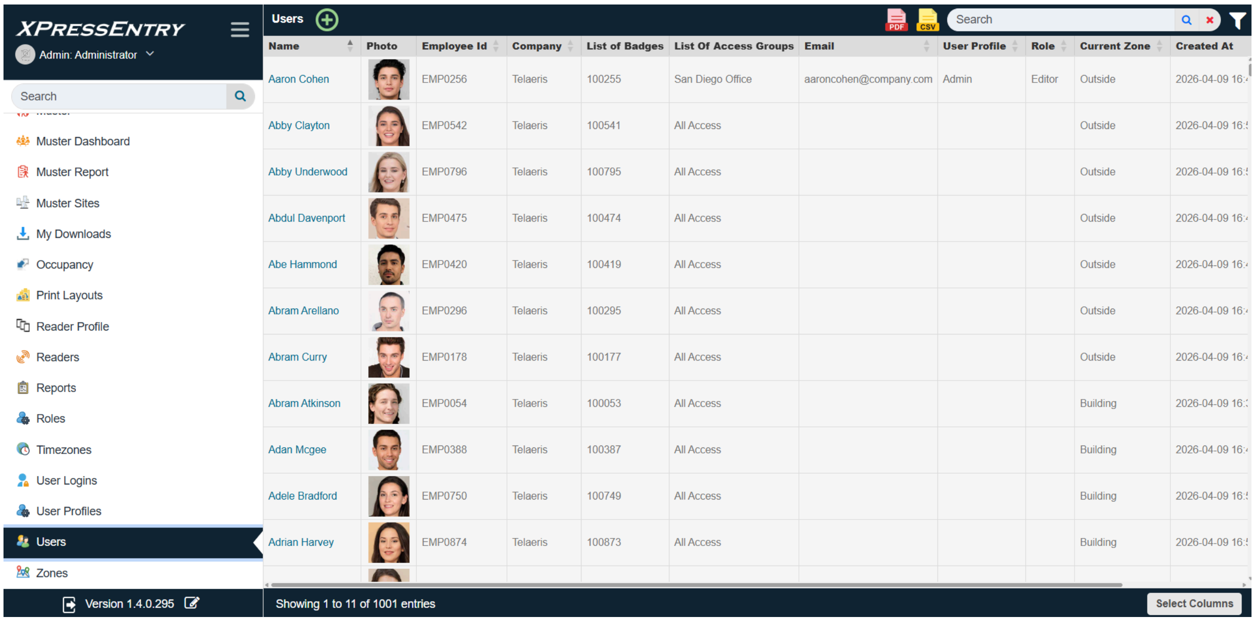
The data management tabs in the Web Console allow administrators to configure all the core records the system relies on - users, companies, groups, zones, doors, readers, roles, logins, and time zones. These tabs are accessible directly from the left navigation panel. The tabs available to any given user depend on their assigned role and permissions.

All data management tabs follow a common layout:

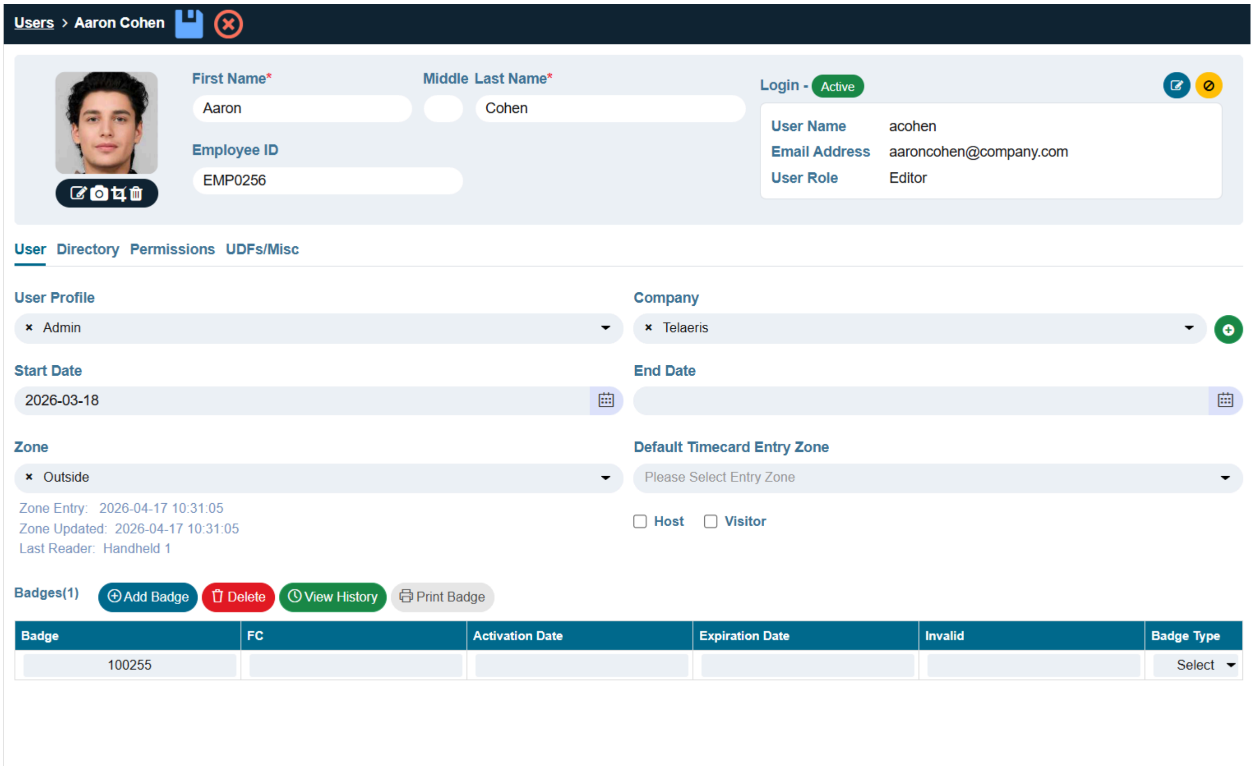
- Startup panel - List of existing records. Select any item to view or edit its details. Use the search field and filters to locate records quickly.
    - Note: Right-clicking any record in a data management list opens a context menu with quick options, such as Open or Delete.
- Detail view - Fields for the selected record. Edit values using text fields, dropdowns, or checkboxes.
- Add New / Save: Click the add icon to create a new record, fill in the details, and click the save icon.

Users

The Users sub-tab manages personnel records in the XPressEntry system - their credentials, group assignments, contact information, and activity history. Every badge holder who will be scanned by a handheld reader must have a record here.



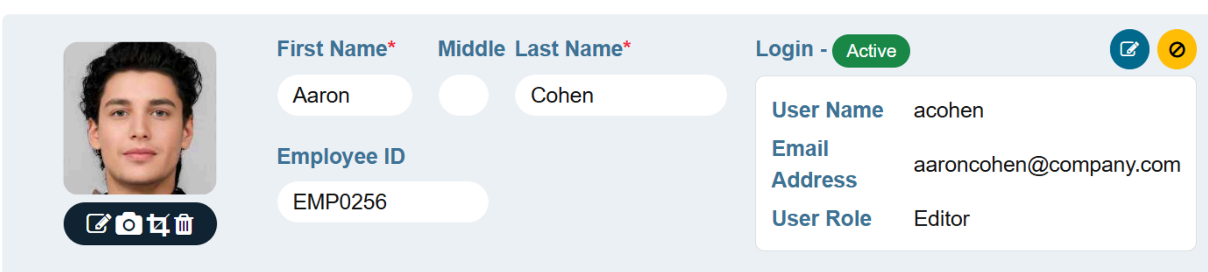
Each user record is organized into four tabs: User, Directory, Permissions, and UDFs/Misc. The header area at the top of the record is visible across all tabs and contains the user’s core identity information.



Header Area

The header is always visible when viewing a user record and displays the following:

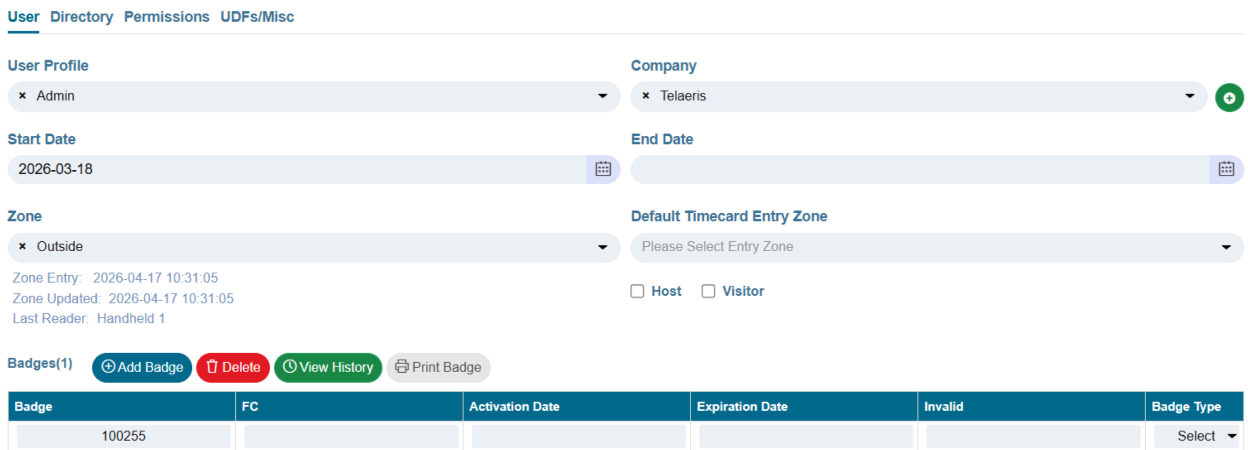
- Photo - The user's profile photo. Use the camera icon below the photo to add or update it. Additional icons allow editing, fingerprint management, and deletion.
- **First Name** / **Middle** / **Last Name** - The user's full name. First and last names are required fields.
- **Employee ID** - The user's employee ID number, if applicable.
- **Login** panel - Displays the user's associated login details - Username, Email Address, and User Role - along with an Active/Inactive status indicator. Use the edit icon to modify the linked login, or the deactivate icon to revoke it.



User Tab

The User tab contains primary access and badge configuration for the record.

Field	Description
User Profile	Assigns a User Profile to this record, which determines the badge print layout and handheld login permissions.
Company	The company this user belongs to. Select from existing companies or add a new one inline.
Start Date / End Date	Defines the date range during which the user's access is active. Leave blank for indefinite access.
Zone	Displays the user's current zone — where they were last recorded by the system. Also shows Zone Entry time, Zone Updated time, and Last Reader.
Default Timecard Entry Zone	The zone used as the default entry point for timecard tracking, if applicable.
Host	Marks the user as a host, typically used in visitor management workflows.
Visitor	Marks the user as a visitor rather than a regular employee.
Badges	Lists all badge credentials assigned to this user. Each badge entry shows the Badge number, FC (facility code), Activation Date, Expiration Date, Invalid Status, and Badge Type. Use Add Badge to assign a new credential, Delete to remove one, View History to see scan activity for that badge, and Print Badge to print a physical badge.



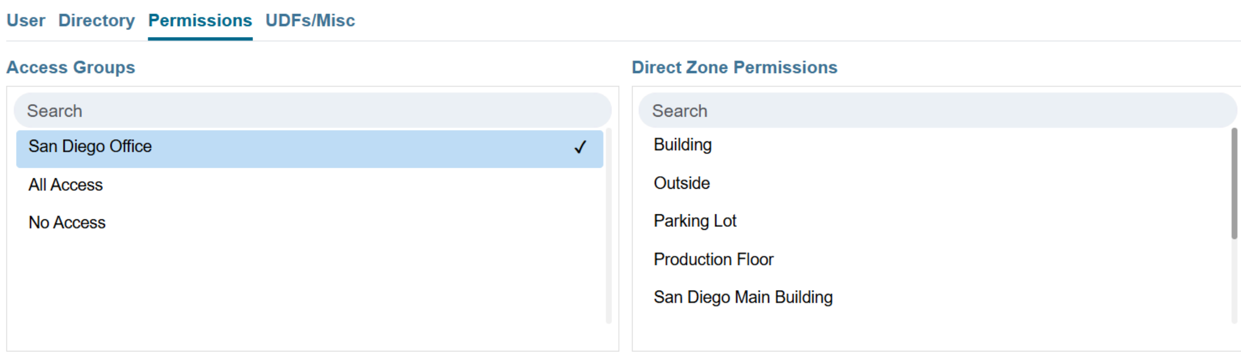
Directory Tab

The Directory tab stores additional contact and organizational details for the user.

Permissions Tab

The Permissions tab controls which zone(s) or reader(s) the user is permitted to access.

- **Access Groups** - Assigns the user to one or more access groups. The user inherits all zone permissions defined in the selected group(s). A checkmark indicates the currently assigned group.
- **Direct Zone Permissions** - Grants access to individual zones directly on the user record, independently of any group assignment. This allows exceptions to be made for specific users without modifying the group. This is an advanced option and is not commonly used in most deployments.



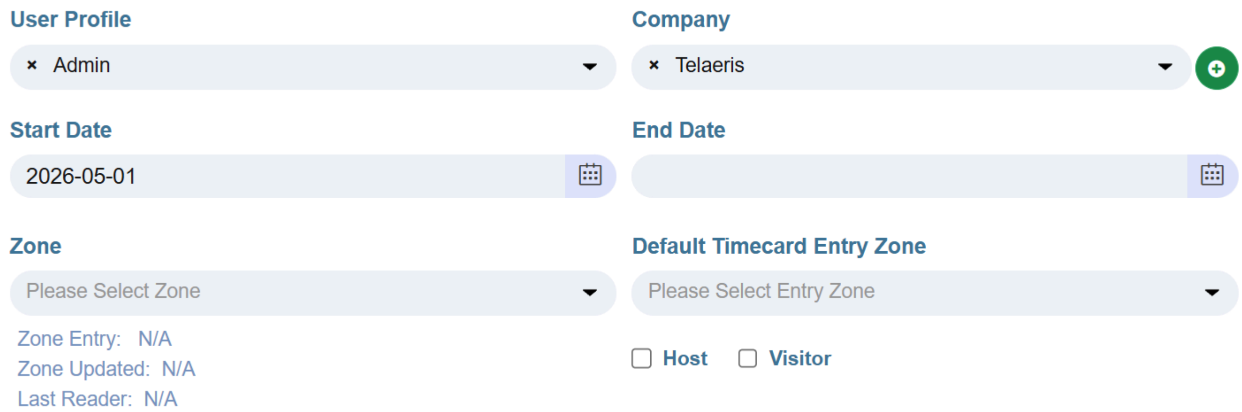
UDFs/Misc Tab

The UDFs/Misc tab contains User Defined Fields (UDFs) - custom data fields configured by the administrator to capture additional information specific to the organization's needs. The fields available here will vary by deployment.

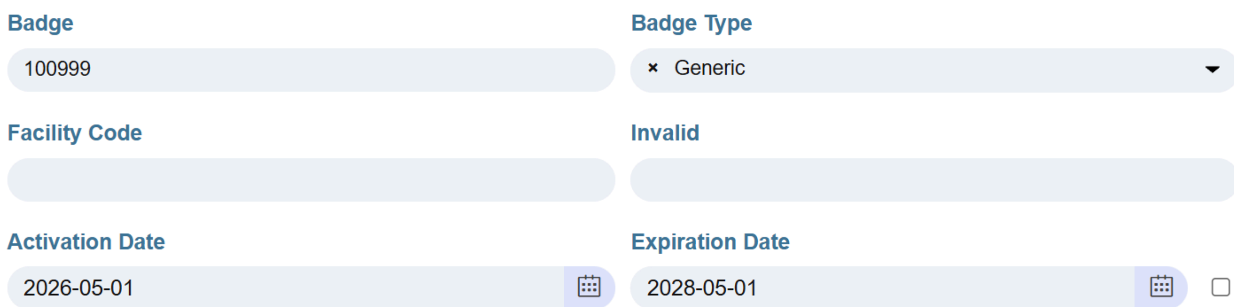
Creating a New User

1. Navigate to the **Users** tab in the left navigation panel.
2. Click the add icon at the top of the page to open a new blank user record.
3. Enter the user's **First Name**, **Middle initial**, and **Last Name**.
4. Enter the **Employee ID**, if applicable.

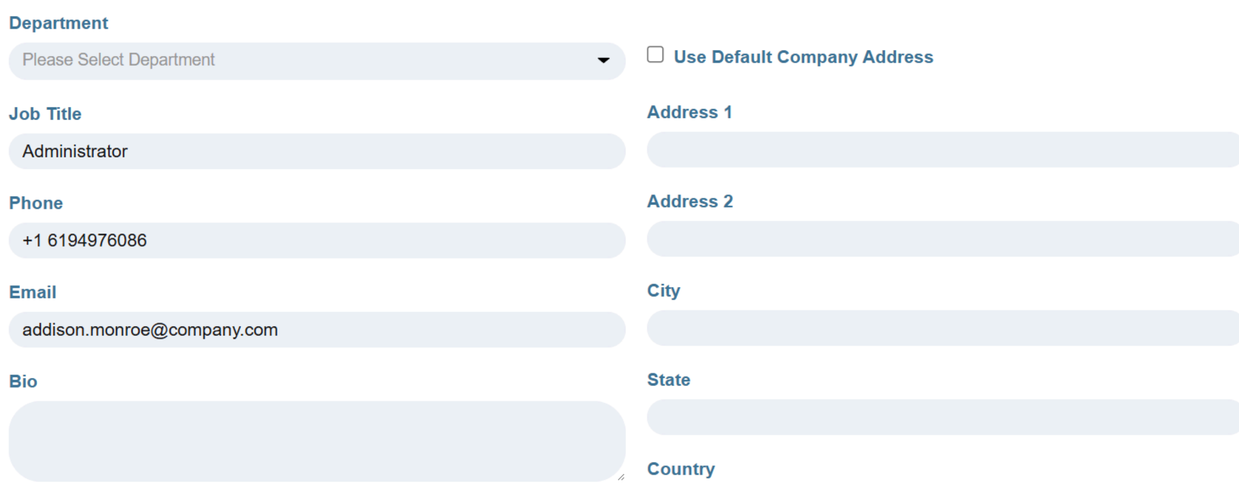
5. On the User tab, select a **User Profile** and **Company**.
6. Set a **Start Date** and **End Date** if the user's access should be time limited.



7. Under **Badge**, enter the badge number, select the badge type and enter any activation or expiration dates.



8. Optionally switch to the **Directory** tab and enter contact and organizational details.



9. Click the **Save** icon at the top of the page.

Note: A user record gives the person a badge identity in XPressEntry. It does not automatically create a Web Console login. To allow a user to log in to the Web Console, a separate login must be created under User Logins.

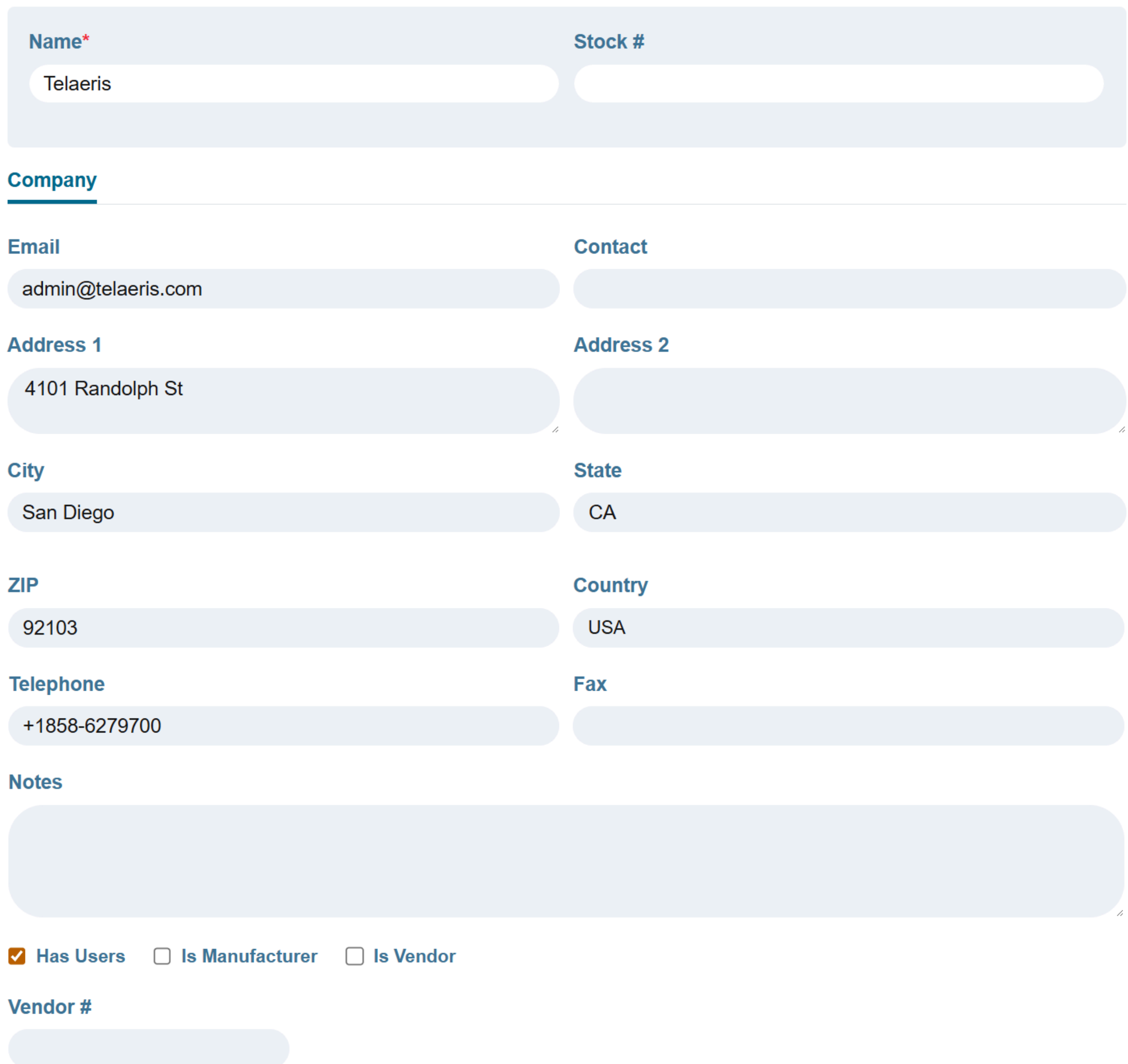
User Profiles

The User Profiles tab manages profiles that can be assigned to badge holders. A User Profile defines a badge print layout and controls whether users assigned to that profile are permitted to log in to a handheld device. Two default profiles are included - Admin and Entrant. The following fields can be edited:

- **Name** - The name of the profile.
- **Badge Layout** - The badge print layout template assigned to this profile. Select from available layouts configured under Print Layouts.
- **Can Log In To Handheld** - When checked, users assigned to this profile are permitted to log in to a handheld reader device.

Companies

The Companies tab manages company records associated with badge holders. Multiple companies can exist in the system - for example, the user's own organization plus manufacturers or vendors. When creating or editing a company, users can assign a company a name, stock number, email, contact, address, telephone number, fax number, additional notes or comments about the company, and whether the company has users, is a manufacturer, and/or is a vendor.



Groups

Groups define which zones a set of users is permitted to access. Every user assigned to a group inherits that group's permissions. When their badge is scanned at a door, XPressEntry checks whether their group grants access to that zone or reader before allowing or denying entry. Groups are most useful when an organization has distinct sets of personnel who would only access certain areas. For example:

- A San Diego Team group might have access to the San Diego Main Building and San Diego Parking Lot, but not any San Francisco zones.
- A San Francisco Team group would have access to San Francisco zones only.
- A contractor group might have access to a limited set of zones compared to full-time employees.

When a user belonging to the San Diego Team scans their badge at a San Francisco door, they will receive Access Denied, because their group does not include permissions for that location.

A default group is included:

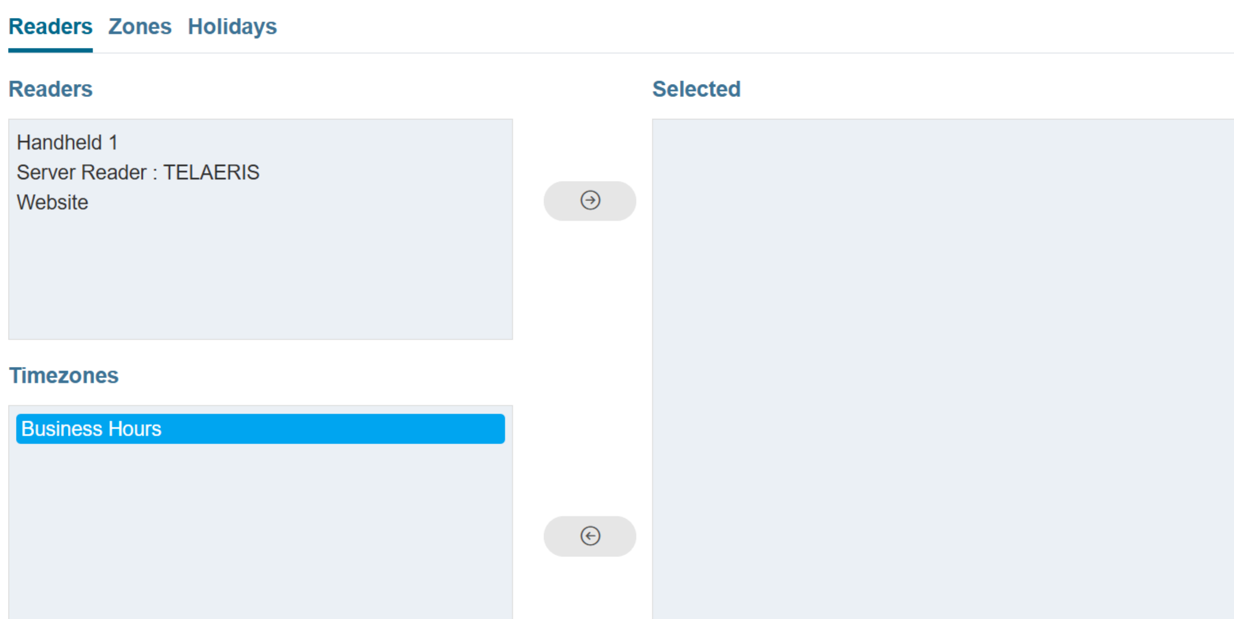
- All Access - Grants access to all zones and readers in the system. Suitable for administrators or security staff who need unrestricted movement.

Each group record contains a Name field, an Is Default Group checkbox, and three tabs: Readers, Zones, and Holidays.

Readers Tab

The Readers tab controls which handheld reader devices members of this group are permitted to use. This is used when Reader-based validation is enabled in the Reader Profile.

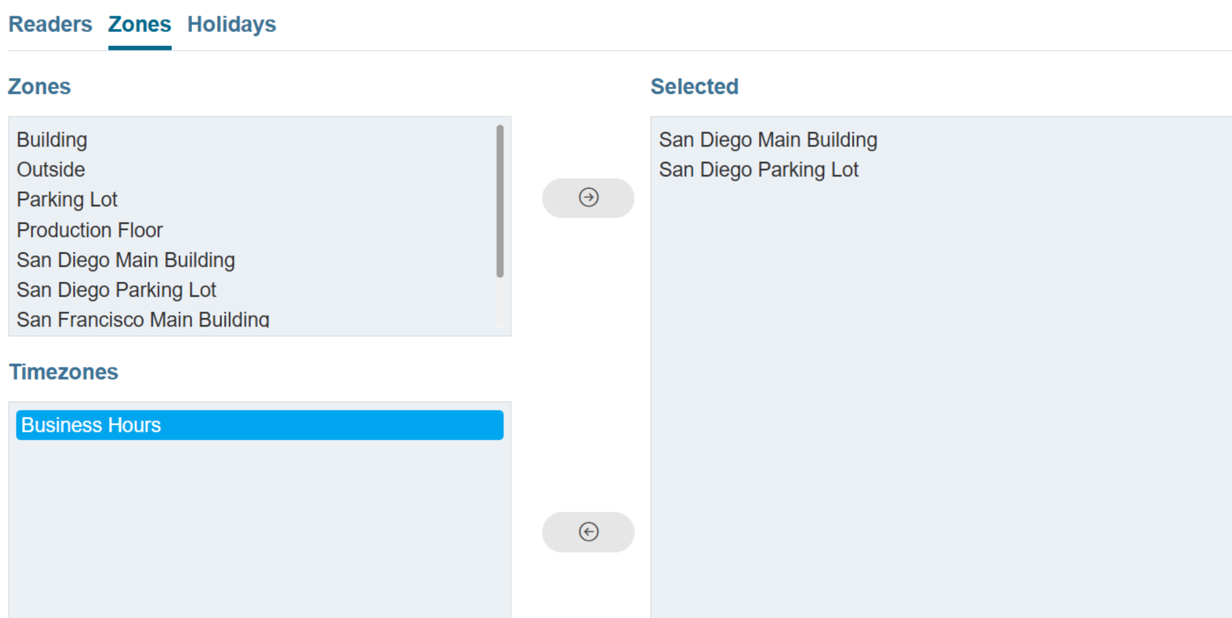
The left panel lists all available readers. Select a reader and click the arrow button to move it to the Selected panel on the right. Only readers in the Selected panel will grant access to group members. A Timezones section is also available on this tab to restrict reader access to specific days and hours.



Zones Tab

The Zones tab controls which physical areas members of this group are permitted to enter. This is used when Zone-based validation is enabled in the Reader Profile.

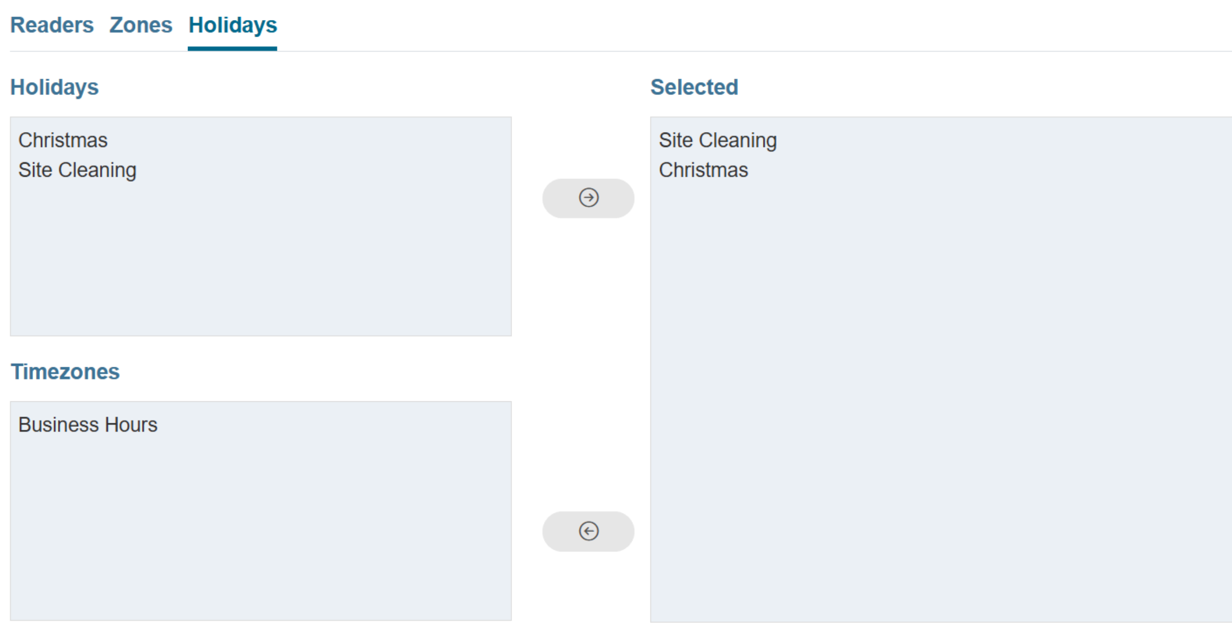
The left panel lists all zones configured in the system. Select a zone and click the arrow button to move it to the Selected panel on the right. Only zones in the Selected panel will grant access to group members when they scan at a door leading to that zone. A Timezones section is also available to restrict zone access to specific days and hours.



Example: The San Diego Office group has San Diego Main Building and San Diego Parking Lot in its Selected zones. All other zones - San Francisco Main Building and San Francisco Parking Lot - remain in the left panel and are not accessible to this group.

Holidays Tab

The Holidays tab assigns holiday schedules to the group, restricting access on specified dates. The left panel lists all holidays configured in the system. Select a holiday and click the arrow button to apply restrictions on those holiday dates.



Is Default Group

Checking Is Default Group at the top of the record designates this group as the one automatically assigned to new users when they are created, if no other group is explicitly selected.

Creating a New Group

1. Navigate to **Groups** in the left navigation panel.
2. Click the **Add** icon to create a new group.
3. Enter a **Name** for the group.
4. Switch to the **Zones** tab. Select the zones this group should have access to from the left panel and click the arrow to move them to **Selected**.
5. Optionally, switch to the **Readers** tab and assign specific readers if using reader-based validation.
6. Optionally, switch to the **Holidays** tab and assign any applicable holiday schedules.
7. Click **Save**.
8. Navigate to **Users** and assign members to this group via their **Permissions** tab.

Note: Groups in XPressEntry serve the same purpose as Access Levels in a traditional access control system. If XPressEntry is integrated with a PACS, access levels from that system can be synced and used in place of manually created groups.

Zones

A Zone represents a distinct physical area within a facility. Zones are the foundation for occupancy tracking, access control groups, and mustering. Every entry and exit event in XPressEntry is recorded in the context of a zone, and group permissions are defined at the zone level.

The Zones list displays all configured zones with the following columns: Name, Description, Parent, Zone Outside, Muster Point, Tracks Occupancy, Tracks Inventory, Map, Created At, and Updated At. The list can be exported as PDF or CSV, and columns can be toggled using the Select Columns button at the bottom right.

Zones   PDF CSV   Search

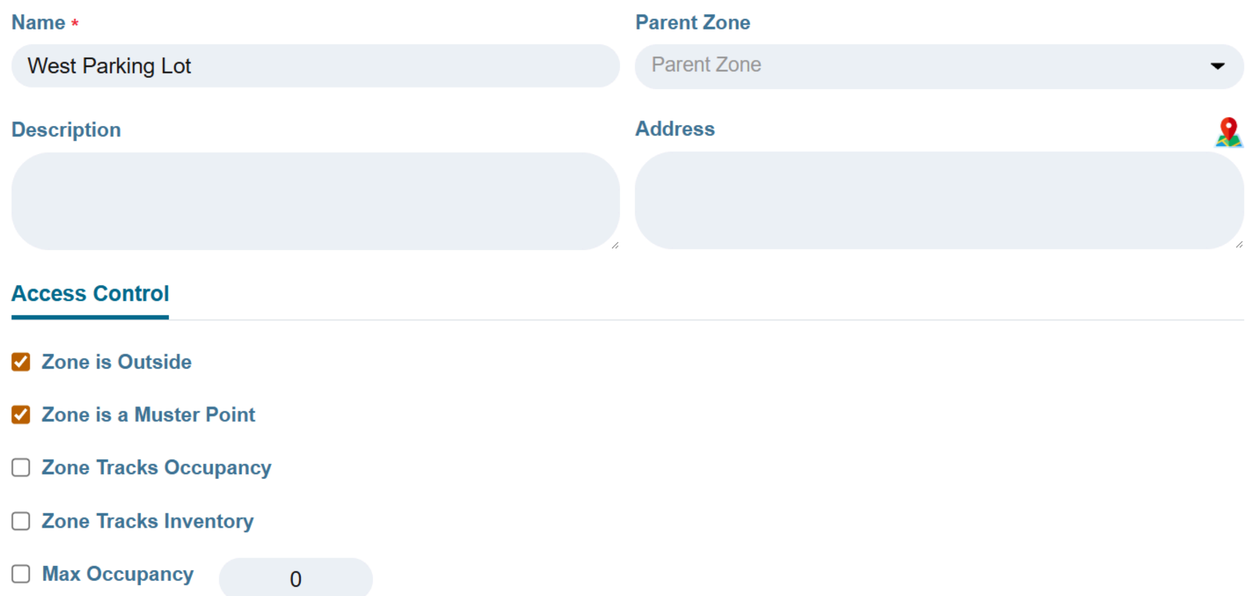
Name	Description	Parent	Zone Outside	Muster Point	Tracks Occupancy	Tracks Inventory	Map	Created At	Updated At
Building			No	No	Yes	No		2025-08-07 14:56:29	2025-08-07 14:56:29
Outside			Yes	Yes	No	No		2025-08-07 14:56:29	2026-04-17 16:19:03
Parking Lot			Yes	Yes	No	No		2026-04-14 12:18:35	2026-04-14 12:18:35
Production Floor			No	No	Yes	No		2026-04-14 12:18:03	2026-04-14 12:18:03
San Diego Main Building			No	No	Yes	No		2026-05-06 15:29:28	2026-05-06 15:29:28
San Diego Parking Lot			Yes	Yes	No	No		2026-05-06 15:29:45	2026-05-06 15:29:45
San Francisco Main Building			No	No	Yes	No		2026-05-06 15:30:01	2026-05-06 15:30:01
San Francisco Parking Lot			Yes	Yes	No	No		2026-05-06 15:30:17	2026-05-06 15:30:17
Telaeris San Diego Office			No	No	Yes	No		2026-05-11 10:42:41	2026-05-11 10:42:41

Zone Fields

The following fields are available when creating or editing a zone:

Field	Description
Name	The zone name (required). Should clearly identify the physical area (e.g., "San Diego Main Building", "San Diego Parking Lot").
Description	Optional free-text description of the zone.
Parent Zone	Assigns this zone as a sub-zone of a larger parent zone, useful for organizing zones in multi-building or multi-floor facilities.
Address	The physical address of the zone. Used for map-based features where applicable.
Zone is Outside	Marks the zone as an exterior area. Outside zones are not counted as part of the facility’s interior occupancy.
Zone is a Muster Point	Designates the zone as an emergency assembly location. Note: if a zone is a Muster Point, it must also be marked as Outside.

Zone Tracks Occupancy	When checked, XPressEntry maintains a live count of personnel currently inside this zone. Occupancy is updated with each entry and exit scan.
Zone Tracks Inventory	When checked, the zone participates in inventory tracking (used in XPTrack deployments).
Max Occupancy	Sets a maximum occupancy limit for the zone. When enabled, entry may be restricted once the limit is reached.



Door Associated with a Zone

The bottom of each zone record displays a table of all doors that are associated with that zone - either as a Start Zone or End Zone. Each row shows the Door name, Start Zone, End Zone, External Entry Reader, and External Exit Reader. This gives a quick reference for which access points connect to or from this zone without needing to navigate to the Doors tab.

Door	Start Zone	End Zone	External Entry Reader	External Exit Reader
San Diego Door 1	San Diego Parking Lot	San Diego Main Building		

Zone Types and How to Configure Them

The combination of checkboxes on a zone record determines how XPressEntry treats it. The table below summarizes the most common zone types:

Zone Type	Zone is Outside	Zone Tracks Occupancy	Zone is a Muster Point
Interior work area (e.g., Main Building, Production Floor)	No	Yes	No
Exterior area with no safety accountability (e.g., public parking)	Yes	No	No
Muster Point / Assembly Area (e.g., Parking Lot, Outside)	Yes	No	Yes. A zone cannot be a Muster Point without also being marked as Outside.

Creating a New Zone

1. Navigate to **Zones** in the left navigation panel.
2. Click the add icon to open a new zone record.
3. Enter a **Name** for the zone.
4. Optionally enter a **Description** and **Address**.
5. If this zone is a part of a larger area, select a **Parent Zone**.
6. Under **Access Control**, apply the applicable settings.
    a. Check **Zone Tracks Occupancy** if personnel counts should be maintained for this zone.
    b. Check **Zone is Outside** if this is an exterior area.
    c. Check **Zone is a Muster Point** if personnel should assemble here during an emergency. Note: Zone is Outside must also be checked for any Muster Point.
7. Optionally set a **Max Occupancy** limit.
8. Click **Save**.

Note: Zones must be created before Doors can be configured, since each Door requires a Start Zone and End Zone assignment.

Doors

A Door defines a physical entry/exit point in the facility and connects two zones (a Start Zone and an End Zone).

The following table includes all the fields available when creating or editing a door:

Field	Description
Door Name	Name identifying the doorway or access point.
Start Zone	The zone on the entry side of the door.
End Zone	The zone on the exit side of the door.
Door RFID Tag #	RFID tag data for the doorway (if applicable).
External Entry Reader	The reader used for entry scans. Populated from the physical access control system (PACS) only.
External Exit Reader	The reader used for exit scans. Populated from the physical access control system (PACS) only.

Readers

The Readers tab registers and configures each handheld device connected to the XPressEntry system. Each reader record links a physical device to a door assignment and a Reader Profile that controls its behavior.

The following table explains each field available when connecting or editing a reader:

Field	Description
Name	A descriptive name for the reader device (required). This name appears throughout the Web Console and on handheld screens (e.g., "Handheld 1").
Door	The door this reader is assigned to (required). Determines which Start and End zones are used when this reader records entry or exit events.
Profile	The Reader Profile assigned to this device (required). The profile controls which modes are enabled (Entry/Exit, Muster, Events, etc.), which badge types are accepted, and what validation rules apply.
GUID	The reader's unique identifier, automatically generated when the device first connects to the server. This value is used internally to identify the device and does not need to be edited manually.

The following table explains the available buttons once the Reader is created:

Button	Description
Clear Reader Credential	Clears the stored authentication credential for the reader device. Pressing this button will prevent the device from syncing and all data on the device will be deleted. Use this button if the reader needs to re-authenticate with the server after a credential change or system migration.
Show Setup QR Code	Displays a QR code that can be scanned by a new handheld device during initial setup to automatically configure the server connection. This is the recommended way to connect a new reader to the system.

Holidays

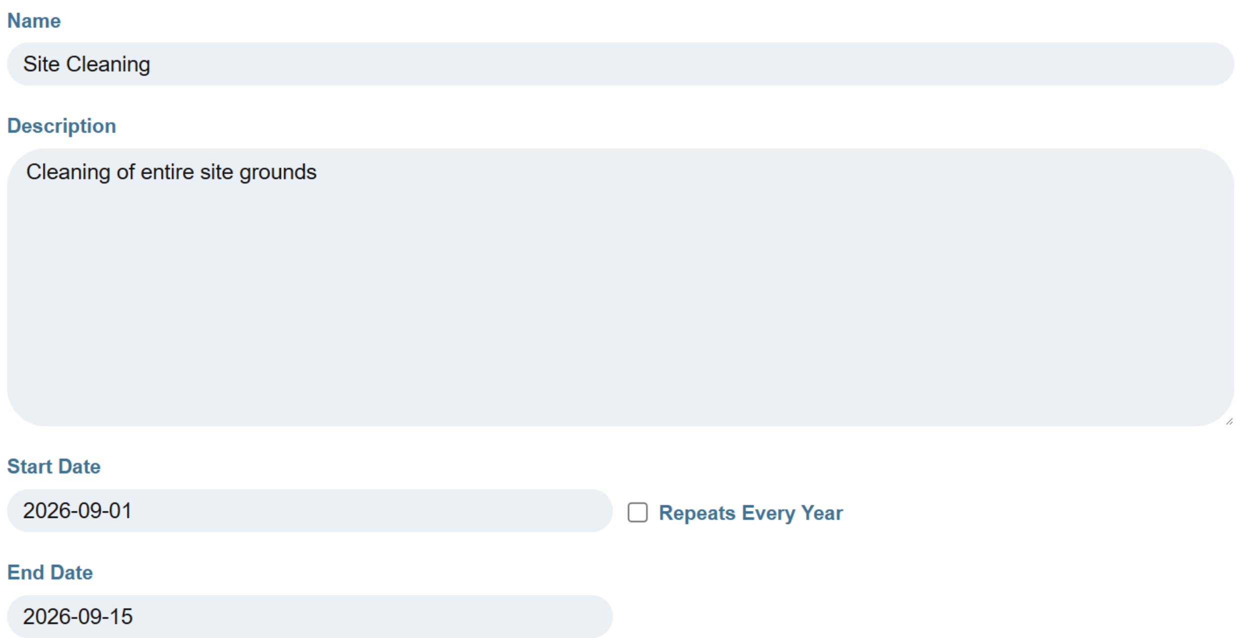
The Holidays tab defines holiday date ranges that can be assigned to Groups to restrict or modify access on specific dates. Once a holiday is created and assigned to a group, members of that group will have their access restricted according to the group's Timezones settings on those dates.

The following table explains each field available when creating or editing a Holiday:

Field	Description
Name	The name of the holiday (e.g., "Christmas", "Independence Day", "Company Shutdown").
Description	Optional notes or details about the holiday.
Start Date	The first date of the holiday period.
End Date	The last date of the holiday period.
Repeats Every Year	When checked, the holiday automatically recurs on the same date(s) each year without needing to be recreated.

Creating a Holiday

1. Navigate to **Holidays** in the left navigation panel.
2. Click the add icon to create a new holiday.
3. Enter a **Name** and optional **Description**.
4. Set the **Start Date** and **End Date**.
5. Check **Repeats Every Year** if this holiday should recur annually.
6. Click **Save**.
7. Navigate to **Groups**, open the relevant group, go to the **Holidays** tab, and move the holiday to the **Selected** panel.



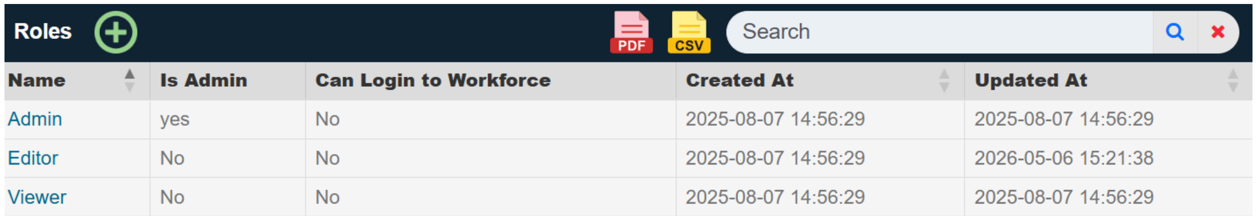
Roles

Roles define what a user can see and do in the Web Console and on handheld devices. Every Web Console login must be assigned a role. Roles are configured here and then linked to logins under the User Logins tab.

Default Roles

XPressEntry includes three pre-configured default roles:

Role	Description
Admin	Full access to all tabs, settings, and functions. Can create and manage all other users and roles.
Editor	Can view and edit data within the tabs and features permitted by the role's feature permissions. Cannot access system settings by default.
Viewer	Read-only access. Can view data but cannot add, update, or delete any records.



Roles

Name	Is Admin	Can Login to Workforce	Created At	Updated At
Admin	yes	No	2025-08-07 14:56:29	2025-08-07 14:56:29
Editor	No	No	2025-08-07 14:56:29	2026-05-06 15:21:38
Viewer	No	No	2025-08-07 14:56:29	2025-08-07 14:56:29

Custom roles can be created by clicking the add icon and configuring the options described below. Assign a Name when creating a new role.

Role Options

The following options are available when creating or editing a Role:

Option	Description
Is Admin	Grants full administrative access to the system. Use with care.
Can Sync A Handheld Device	When checked, users with this role can use their Web Console credentials to connect a handheld device to the XPressEntry server. When unchecked, that login will be rejected by the device.
Receives Registration Email	Controls whether users with this role receive a registration email when a new account is created.
Can Access All Timecard Groups	Grants access to all timecard group data regardless of individual group assignment.

Name *

Viewer

- ☐ Is Admin
- ☐ Can Sync A Handheld Device
- ☐ Receives Registration Email
- ☐ Receives Item Notification Email
- ☐ Can Access All Timecard Groups

Enabled Features (Permission Grid)

Below the role options is the Enabled Features grid. This controls exactly what a user with this role can do within each tab of the Web Console. The columns are View, Add, Update, Delete, and Advanced. Click any cell to toggle that permission on or off. Click All in a column header to toggle that permission for all features at once.

Where a permission is not applicable for a feature, the cell displays N/A and cannot be toggled. Some features also include an Advanced actions dropdown that exposes additional granular permissions specific to that feature.

The following is the Enabled Features grid:

Feature	View ☐ All	Add ☐ All	Update ☐ All	Delete ☐ All	Advanced ☐ All
API Documentation		N/A	N/A	N/A	N/A
Activity History		N/A	N/A	N/A	Advanced actions ⌄
Companies					N/A
Doors					N/A
Events					N/A
Groups					N/A
Holidays					N/A
Logins					Advanced actions ⌄
Muster		N/A	N/A	N/A	Advanced actions ⌄

Muster Dashboard		N/A	N/A	N/A	N/A
Muster Report		N/A	N/A	N/A	N/A
Muster Sites					N/A
My Downloads		N/A	N/A	N/A	N/A
Occupancy		N/A	N/A	N/A	Advanced actions ⌄
Print Layouts					N/A
Reader Profile					N/A
Readers					Advanced actions ⌄
Reports					Advanced actions ⌄
Roles					N/A
TimeZones					N/A
User Profiles					N/A
Users					Advanced actions ⌄
Zones					N/A

An empty cell represents the permission is available and can be toggled on or off for this role. N/A means that permission type does not apply to that feature and cannot be enabled. "Advanced actions" indicates additional granular options are available via a dropdown for that feature.

Editing a Role - Step-by-Step Example

The following example walks through editing the Editor role to grant access to Events, Muster, Occupancy, and Users:

1. Navigate to **Roles** in the left navigation panel.
2. Select **Editor** from the list.
3. Review the options at the top. Leave **Is Admin** unchecked. Check **Can Sync A Handheld Device** if this role should be able to connect handheld devices.
4. Scroll down to the **Enabled Features** grid.
5. Locate the **Events** row. Click **View**, **Add**, **Update**, and **Delete** to enable all four permissions.
6. Locate the **Muster** row. Click **View** only. **Add**, **Update**, and **Delete** are N/A for Muster.
7. Locate the **Occupancy** row. Click **View** only. **Add**, **Update**, and **Delete** are N/A for Occupancy.
8. Locate the **Users** row. Click **View**, **Add**, **Update**, and **Delete** to allow full user management.
9. Click **Save**.

Once saved, any login assigned to this role will see only the tabs permitted by these settings when they sign in.

Name *

Editor

- [ ] Is Admin
- [x] Can Sync A Handheld Device
- [ ] Receives Registration Email
- [ ] Receives Item Notification Email
- [ ] Can Access All Timecard Groups

Enabled Features

Feature	View ☐ All	Add ☑ All	Update ☑ All	Delete ☑ All	Advanced ☐ All
API Documentation		N/A	N/A	N/A	N/A
Activity History		N/A	N/A	N/A	Advanced actions ⌄
Companies					N/A
Doors					N/A
Events	X	X	X	X	N/A
Groups					N/A
Holidays					N/A
Logins					Advanced actions ⌄
Muster	X	N/A	N/A	N/A	Advanced actions ⌄
Muster Dashboard		N/A	N/A	N/A	N/A
Muster Report		N/A	N/A	N/A	N/A
Muster Sites					N/A
My Downloads		N/A	N/A	N/A	N/A
Occupancy	X	N/A	N/A	N/A	Advanced actions ⌄
Print Layouts					N/A
Reader Profile					N/A
Readers					Advanced actions ⌄
Reports					Advanced actions ⌄
Roles					N/A
TimeZones					N/A
User Profiles					N/A
Users	X	X	X	X	Advanced actions ⌄
Zones					N/A

User Logins

The User Logins tab manages Web Console login credentials. A login connects a username and password to a specific Role, controlling what that person can access after signing in. Badge holder records (in the Users tab) and Web Console logins are separate - a person can exist in the system as a badge holder without having a Web Console login.

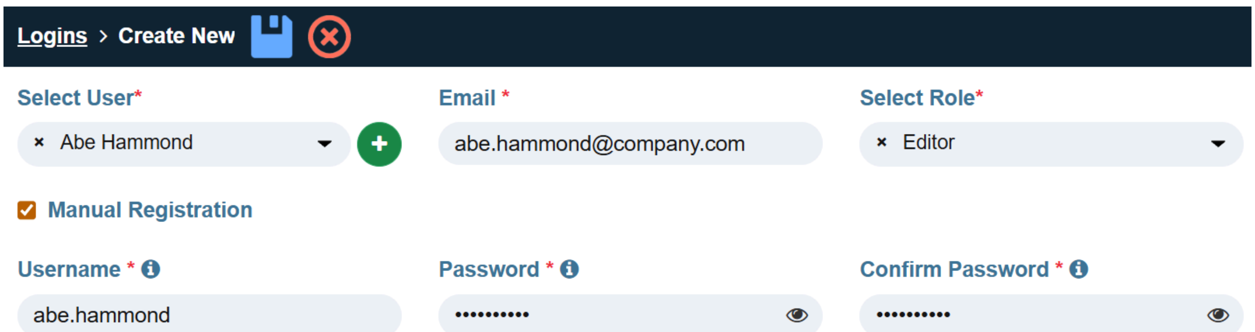
Creating a New Login

1. Navigate to **User Logins** in the left navigation panel.
2. Click the add icon to create a new login.
3. Select the **User**. There are two ways to select a user:

   a. Click the add icon to the right of the dropdown menu. Create a new User by entering their **First** and **Last Name** and selecting a **User Profile**. Click **Save User**.

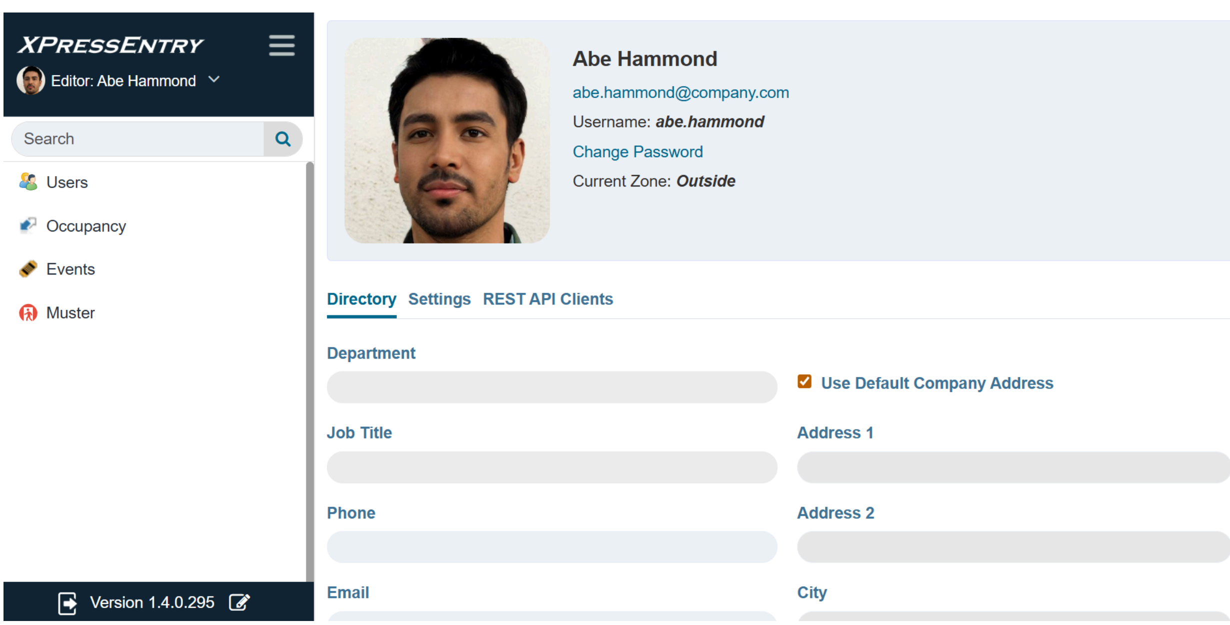
   b. Select a **User** from the dropdown menu. Use the Search field to find a User quickly.

4. Enter the user's email address.
5. Select a **Role** from the dropdown: Admin, Editor, Viewer, or any custom role.
6. Select **Manual Registration** as the registration method for immediate login creation.
7. Enter a username, password, and confirm the password.
8. Click **Save**.



Note: If Manual Registration is not checked and login is not assigned immediately, the User will receive an email to complete the registration.

Once a login is created and the user signs in, the Web Console displays only the tabs and functions permitted by their assigned role. This allows administrators to give security operators or supervisors access to live monitoring and reporting without exposing system configuration settings.



Timezones

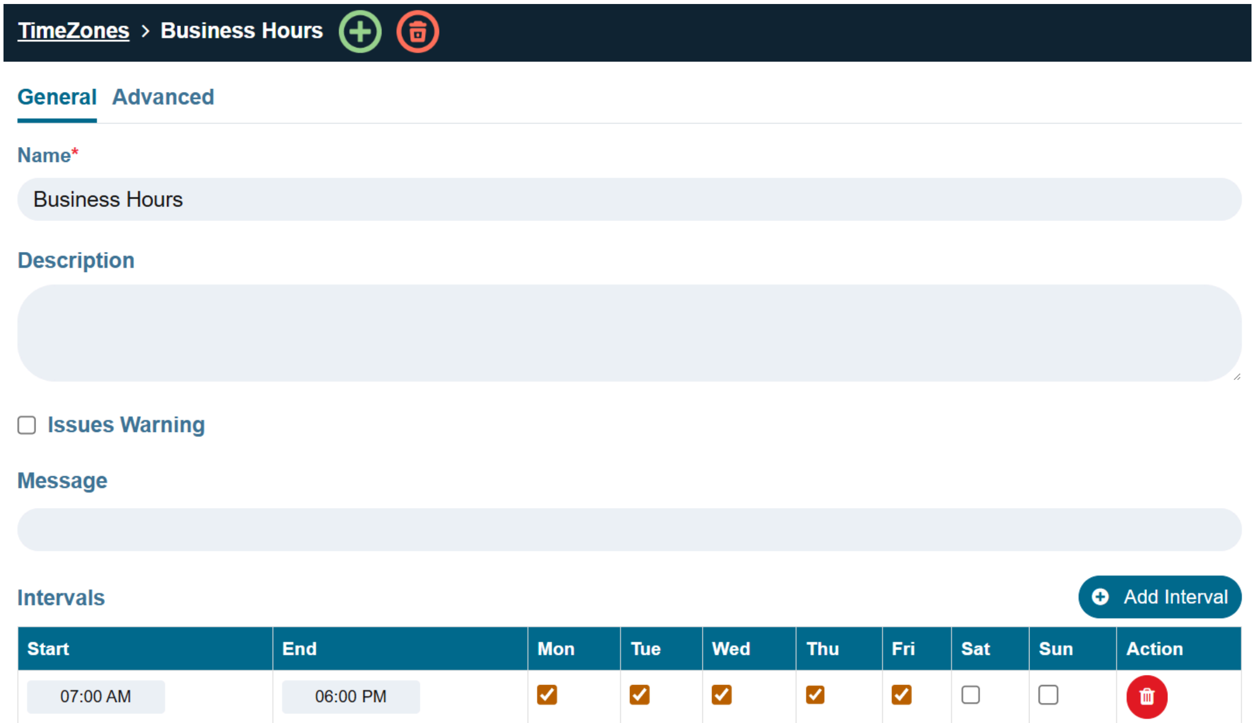
The Timezones tab defines scheduled access windows: the days and hours during which access is permitted. Timezones can be assigned to Groups (on their Readers, Zones, or Holidays tabs) to restrict when group members can enter, and to individual readers to control when a device is active.

Two tabs are available when creating or editing a Timezone, General or Advanced:

General Tab

The following fields are available when creating or editing a Timezone:

Field	Description
Name	The name of the Timezone schedule (required), e.g., "Weekdays 8am–6pm" or "Night Shift".
Description	Optional notes describing the schedule.
Issues Warning	When checked, scanning a badge outside of the permitted interval will issue a warning rather than a hard denial. The handheld displays the configured Message to the operator.
Message	The warning message displayed on the handheld when a scan occurs outside the permitted time window and Issues Warning is enabled
Intervals	Defines one or more time windows for this schedule. Click Add Interval to add a row. Each interval has a Start time, End time, and checkboxes for each day of the week - Mon, Tue, Wed, Thu, Fri, Sat, Sun. Multiple intervals can be added to create complex schedules (e.g., different hours on weekdays vs. weekends). Use the Action column to delete an interval.

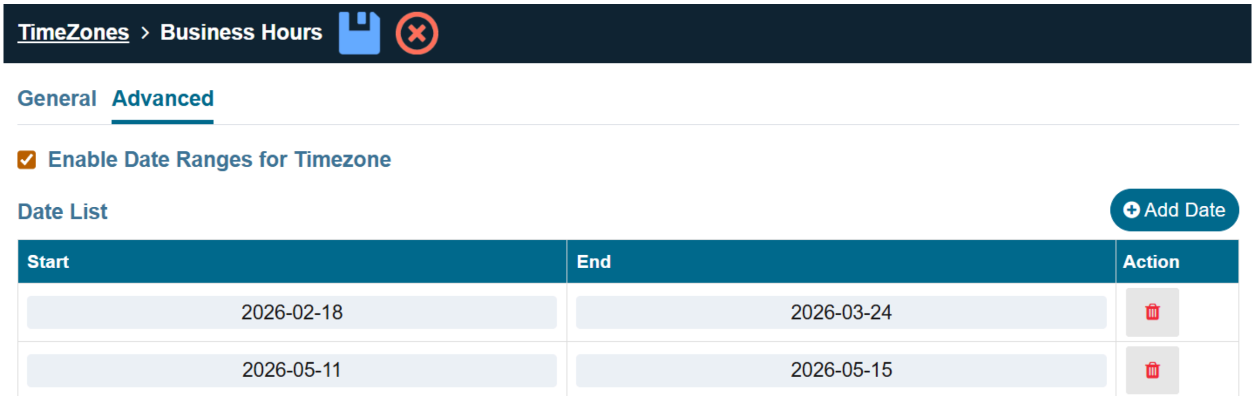


Advanced Tab

The Advanced tab allows a timezone to be further restricted to specific calendar date ranges, in addition to the day-of-week and time intervals defined on the General tab.

The following fields are available when creating or editing an Advanced Timezone:

Field	Description
Enable Date Ranges for Timezone	When checked, the Timezone will only be active within the date ranges defined in the Date List below. If unchecked, the Timezone applies on any date that matches the General tab intervals.
Date List	Defines one or more active date ranges for the Timezone. Click Add Date to add a row. Each row has a Start date, End date, and an Action column to delete the entry. The Timezone will only be enforced on dates that fall within at least one of these ranges.



Note: Use date ranges when access should be limited to a specific period - for example, a contractor whose access is valid only during a particular project window, or a schedule that applies only during a seasonal shutdown.

Creating a Timezone

1. Navigate to **Timezones** in the left navigation panel.
2. Click the add icon to create a new Timezone.
3. Enter a **Name** and optional **Description**.
4. If access outside this schedule should issue a warning rather than deny entry, check Issues Warning and enter a Message.
5. Click **Add** Interval to add a time window.
6. Set the **Start** and **End times** for the interval.
7. Check the days of the week this interval applies to.
8. **Add** additional intervals if needed for different days or shifts.
9. Click **Save**.
10. Navigate to the relevant **Group** and assign the **Timezone** on the **Readers**, **Zones**, or **Holidays** tab as appropriate.

Reader Profiles

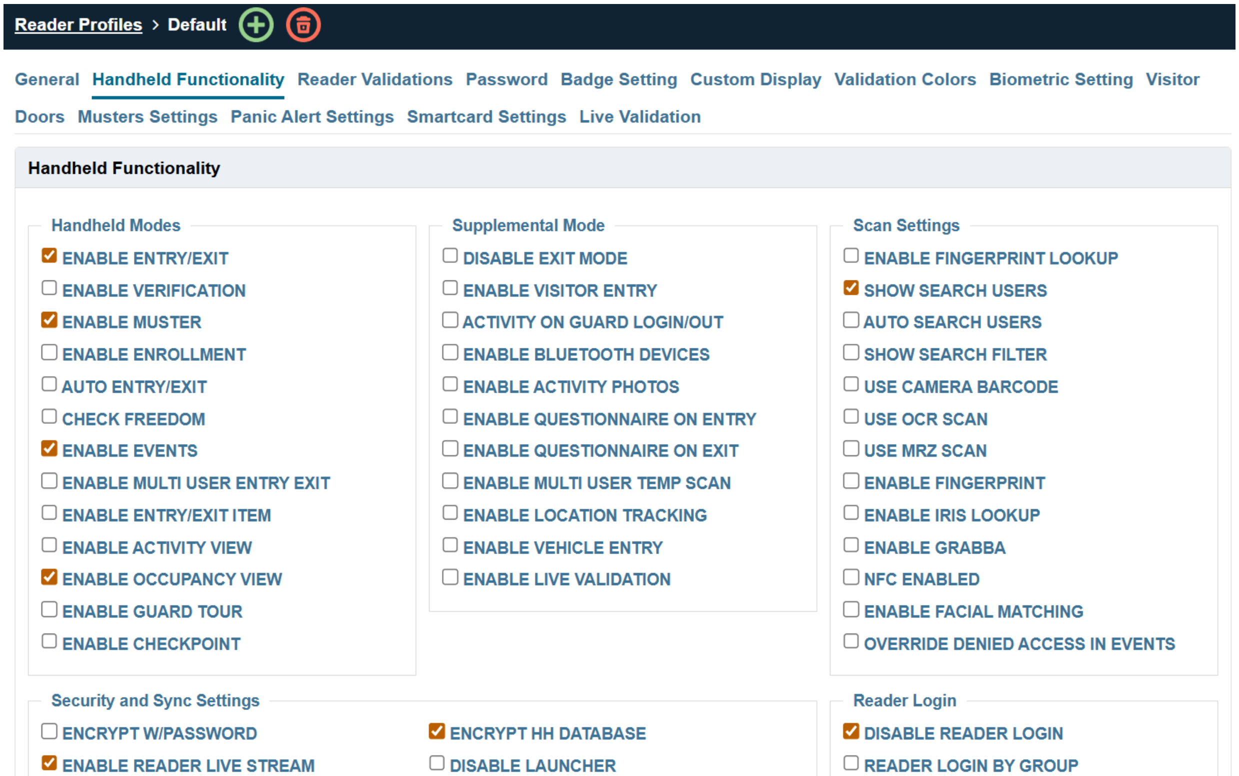
A Reader Profile is a configuration template assigned to one or more handheld reader devices. It controls which modes are available on the device, how badges are validated, and how the device communicates with the server. Every reader must have a profile assigned. One default profile is available.

Navigate to Reader Profile in the left navigation panel to view, create, and edit profiles. The list shows each profile's Name, Created At, and Updated At timestamps.

Each profile record contains multiple configuration tabs.

Handheld Functionality Tab

The Handheld Functionality tab controls which modes and features are active on devices assigned to this profile. It is organized into five sections: Handheld Modes, Supplemental Mode, Scan Settings, Security and Sync Settings, and Reader Login.

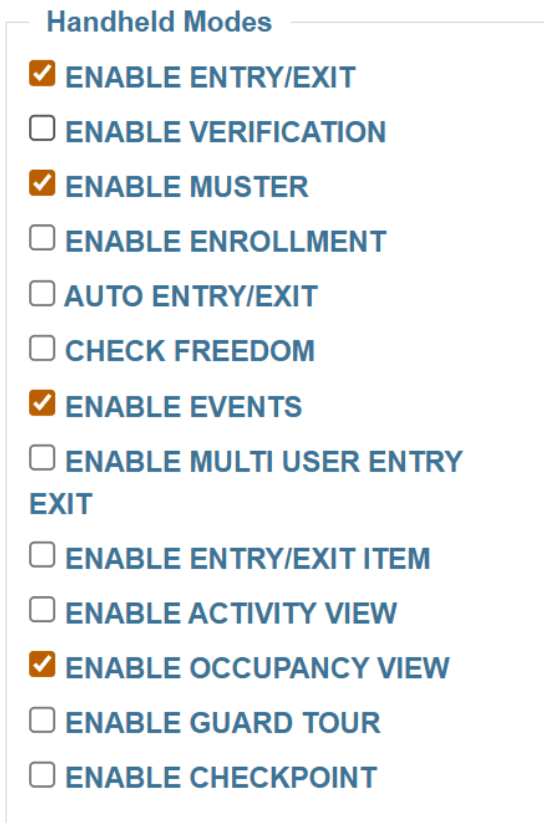


Handheld Modes

Handheld Modes determine which operational modes the device can run. Enable the feature by checking the box. The following are enabled in the Default profile and are the most commonly used:

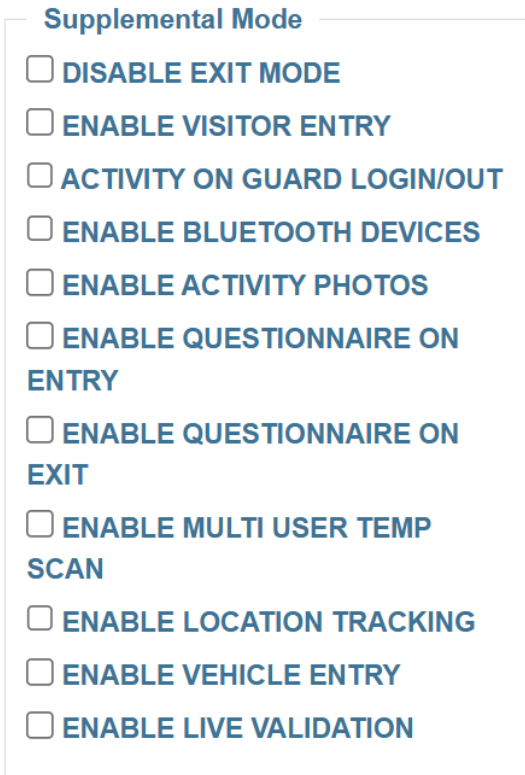
Setting	Description
Enable Entry/Exit	Enables Entry/Exit Mode on the handheld, allowing operators to record personnel entering and exiting through doors. This is the primary mode for day-to-day badge scanning.
Enable Muster	Enables Muster Mode on the handheld, allowing it to be used for emergency mustering and evacuation roll calls.
Enable Events	Enables Events Mode on the handheld, allowing operators to run

	attendance events and scan attendees.
Enable Occupancy View	Allows operators to view live zone occupancy counts directly on the handheld screen.



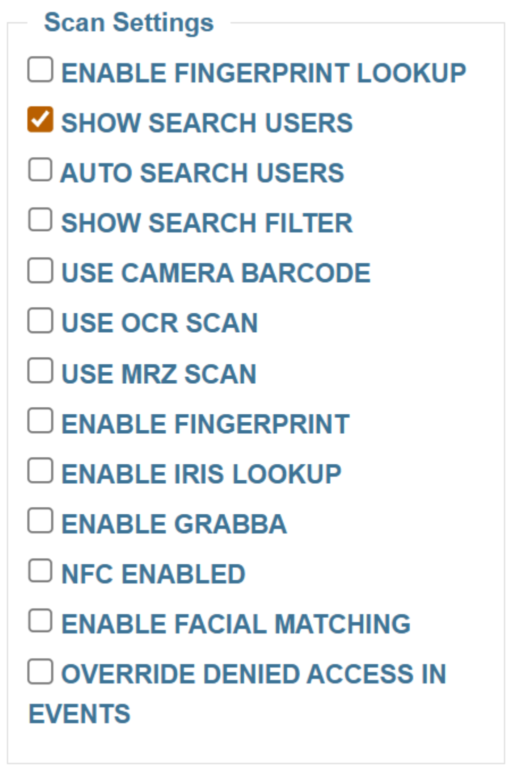
Supplemental Mode

Supplemental Mode settings add optional features to the scanning workflow. These are not enabled in the Default profile.



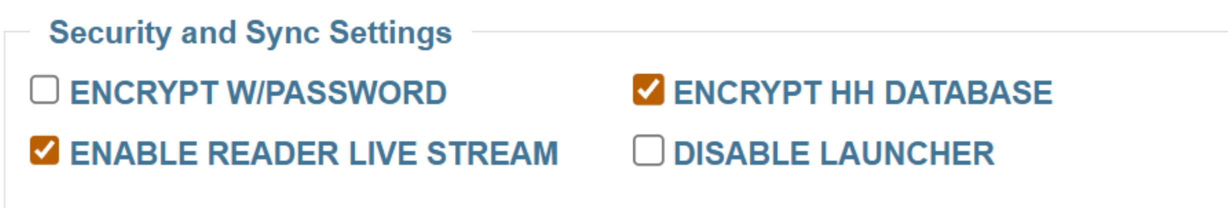
Scan Settings

Scan Settings control how the handheld reads and processes credentials. Show Search Users is enabled in the Default profile, allowing operators to manually search for a user when a badge cannot be scanned.



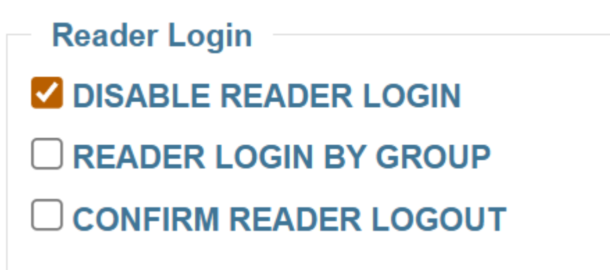
Security and Sync Settings

These settings control how the handheld communicates with the server and secures its local database.



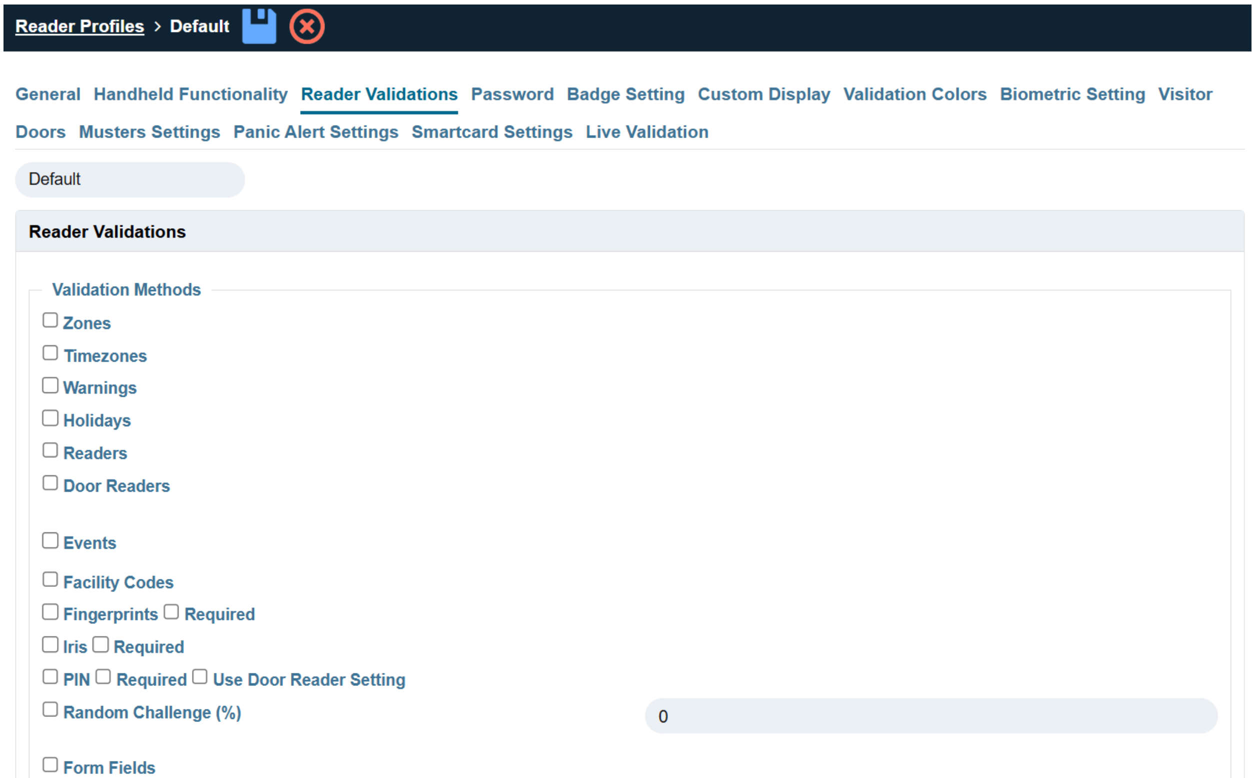
Reader Login

Reader Login settings control how operators authenticate to use the handheld device.



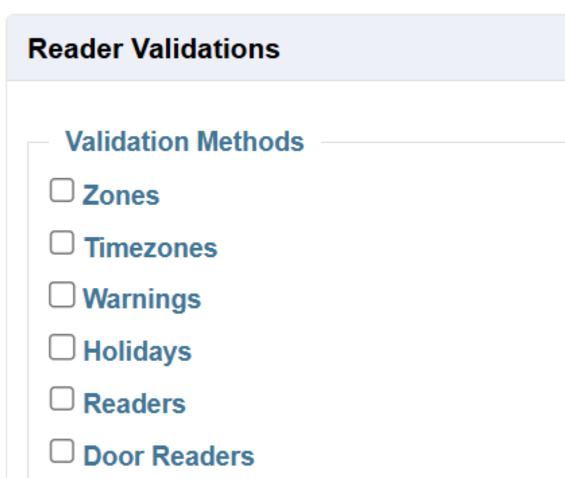
Reader Validations Tab

The Reader Validations tab determines how the handheld decides whether to grant or deny access when a badge is scanned. These settings apply to every scan made on a device assigned to this profile.



Default Behavior (No Validation Checked)

When no validation options are checked, the handheld performs only a basic credential check: it confirms the badge exists in the XPressEntry database and is not marked as invalid. If the badge is recognized, the result is Access Granted - regardless of zones, groups, or any other access rules. This is appropriate when the goal is identity verification only.



Validation Methods

The following validation methods are available. Multiple options can be combined:

Validation Method	Description
Zones	Checks whether the user's group grants access to the zone associated with the door being scanned.
Timezones	Checks whether the current time falls within the Timezone schedule assigned to the user's group or reader. Denies access outside the permitted time window.
Warnings	Issues a warning rather than a hard denial when a validation condition is not met. The handheld displays a warning message to the operator but allows them to proceed.
Holidays	Checks whether a current holiday is assigned to the user's group. Access is restricted on matching holiday dates.
Readers	Checks whether the user's group grants access to the specific handheld reader being used, rather than the zone. Used in standalone deployments where access is tied to specific devices rather than locations.
Door Readers	Checks whether the badge holder has access to the External Entry or Exit Reader mapped to the door in the PACS. Used in PACS-integrated deployments to mirror access rules from the access control system.

Note: After changing any Reader Profile settings, the handheld must sync with the server to receive the updated configuration. On the handheld, tap the sync button (up/down arrows) to pull the latest profile.

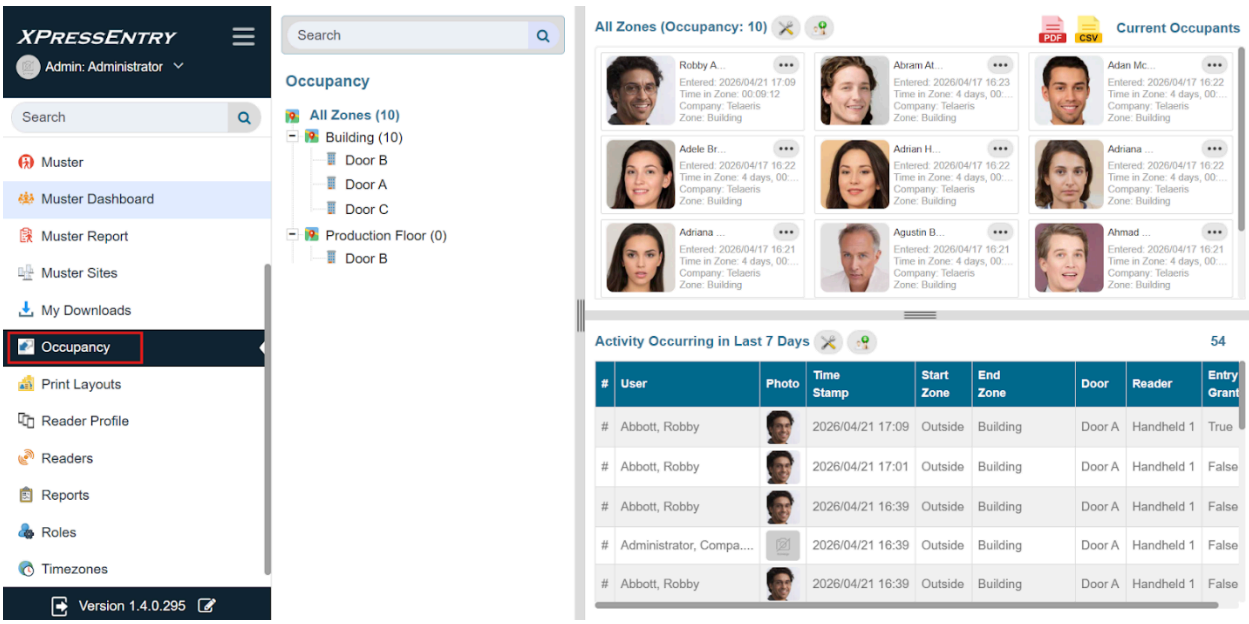
Entry/Exit Mode

Overview

Entry/Exit Mode enables handheld reader operators to record personnel movement between zones. Each successful badge scan is logged as an activity event in the Web Console's Activity History and Occupancy views and, where integrated, is passed to the physical access control system (PACS) as a standard card access event.

- Entry Mode - Records a user moving from the door's Start Zone into the End Zone.
- Exit Mode - Records a user moving from the door's End Zone back into the Start Zone.

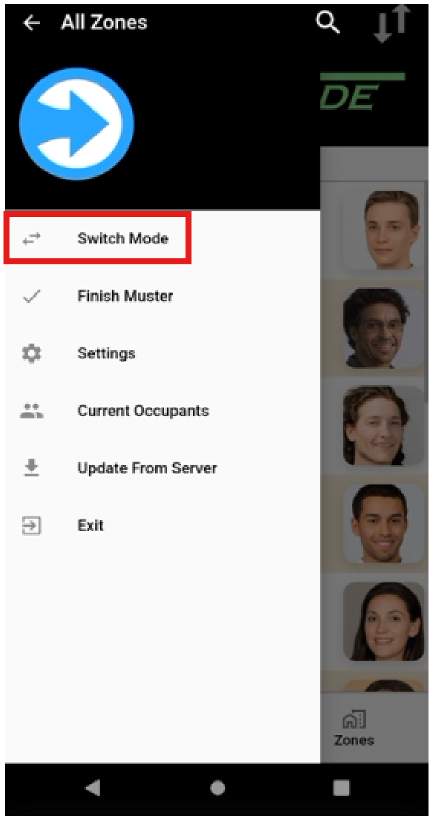
Before using Entry/Exit Mode, confirm that Enable Entry/Exit is checked in the Handheld Functionality tab of the Reader Profile assigned to the device, and that the handheld has been synced.

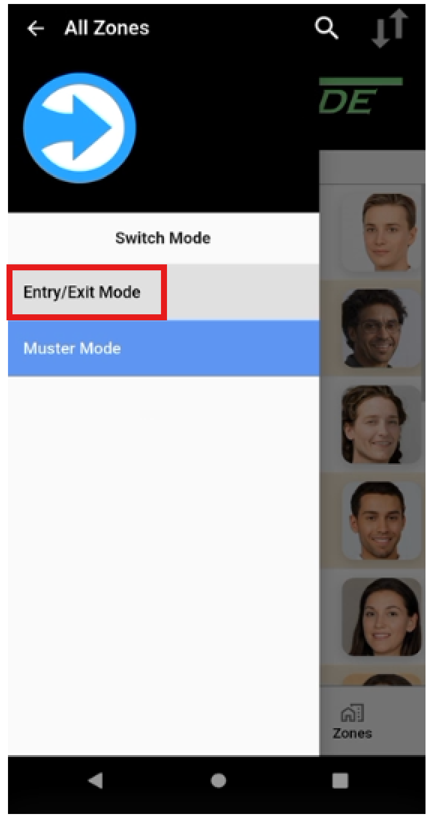


Using Entry/Exit Mode on the Handheld

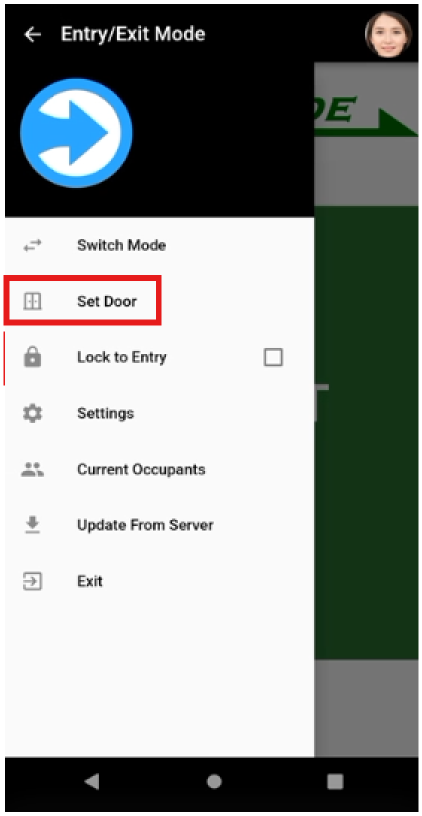
Switching to Entry/Exit Mode

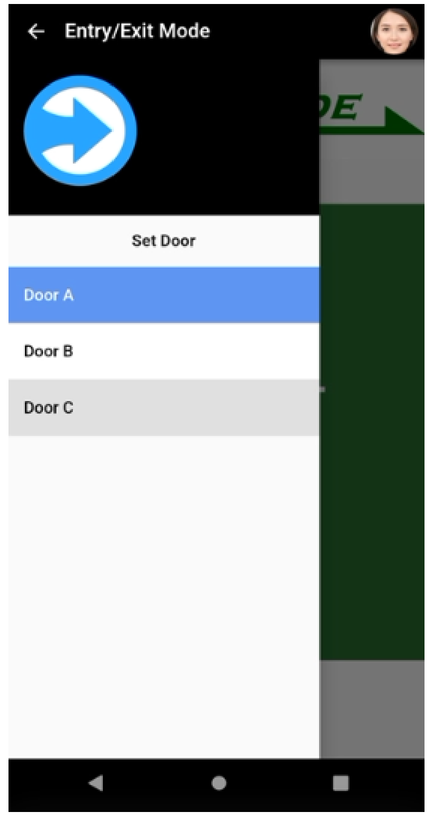
1. Tap the hamburger menu icon in the top-left corner.
2. Tap **Switch Mode** and select **Entry/Exit Mode**.





3. The active door name appears in the title bar. To change doors, tap the menu and select **Set Door**, then choose from the list.





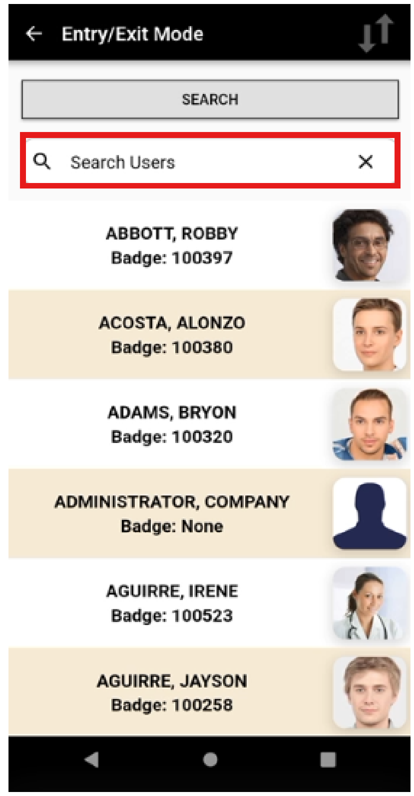
Scanning a Badge

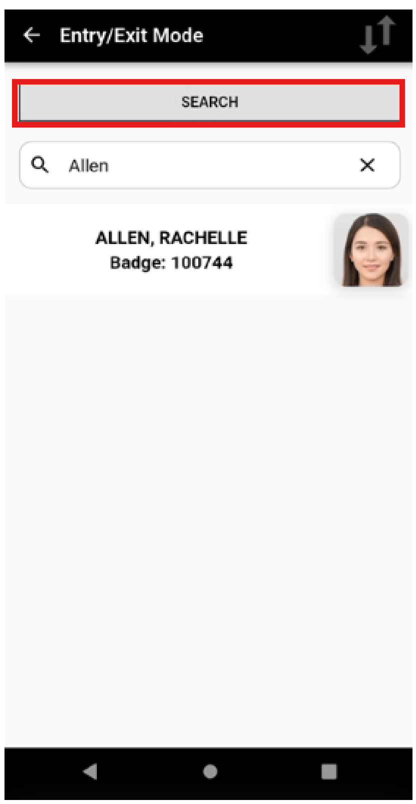
Present the badge to the reader. On a successful scan, the handheld displays the result (Access Granted or Denied), the employee's name, ID number, and photo. The event is logged instantly to the Web Console.

Manual Lookup

If a badge cannot be scanned, tap the search icon, enter the user's name or badge number, select them from the results, and tap Submit to record the entry or exit.


Entry/Exit Mode
ENTRY MODE
Door: Door A
PRESENT BADGE

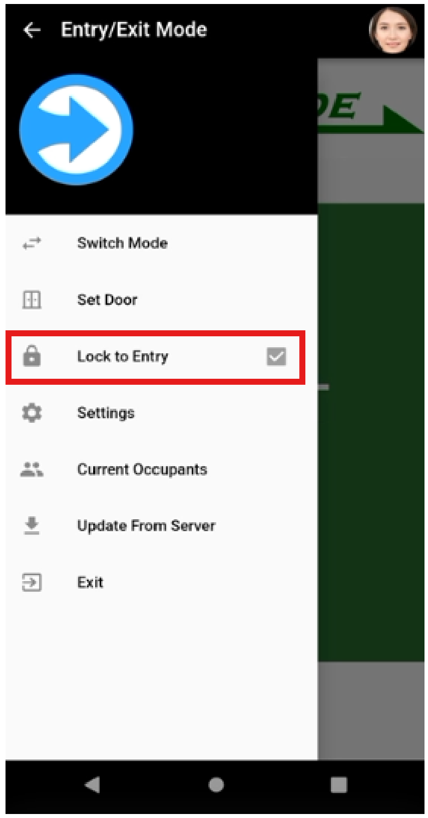

Entry/Exit Mode
SEARCH
Search Users
ABBOTT, ROBBY
Badge: 100397
ACOSTA, ALONZO
Badge: 100380
ADAMS, BRYON
Badge: 100320
ADMINISTRATOR, COMPANY
Badge: None
AGUIRRE, IRENE
Badge: 100523
AGUIRRE, JAYSON
Badge: 100258


Entry/Exit Mode
SEARCH
Allen
ALLEN, RACHELLE
Badge: 100744


Entry/Exit Mode
VALIDATING BADGE
Allen
Rachelle
ID #100744
SUBMIT

Toggling Entry/Exit Direction

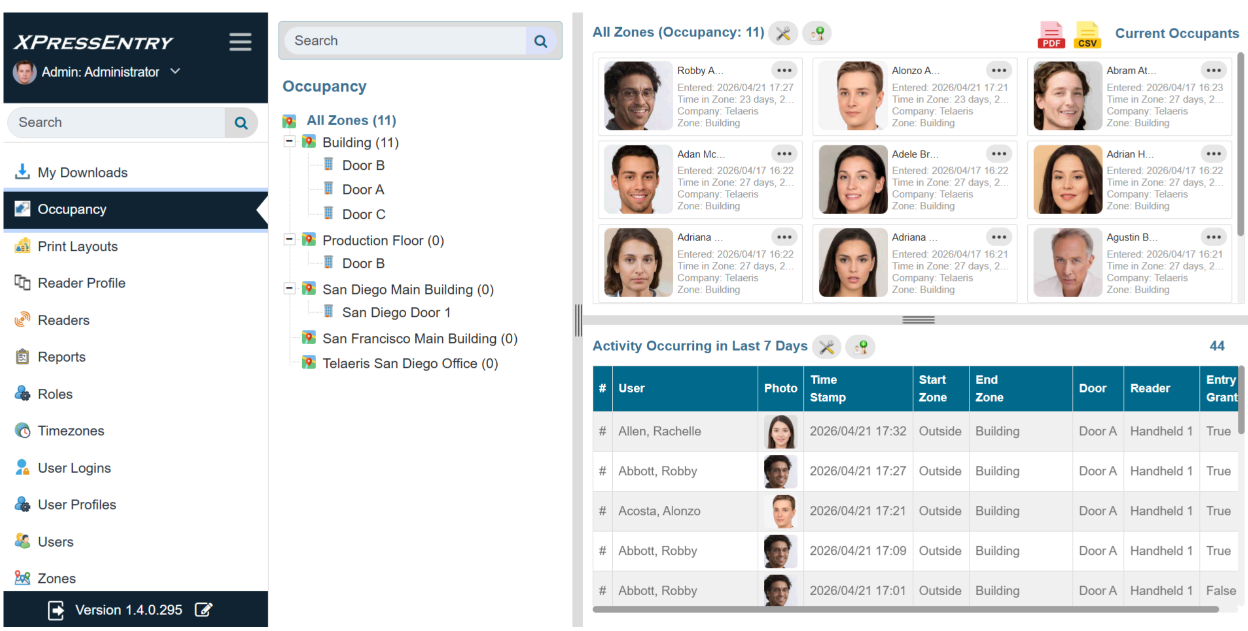
Tap the screen to toggle between Entry and Exit modes. To lock the device to one direction (e.g., at a turnstile), open the menu and select Lock to Entry. Uncheck the same option to unlock.



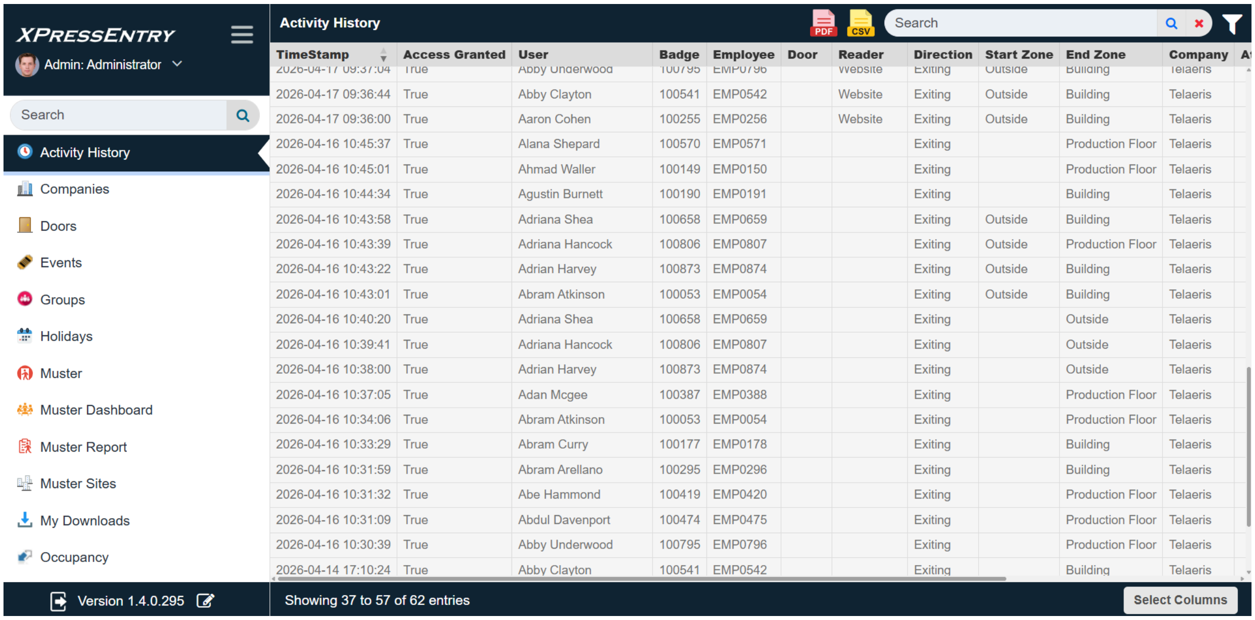
Monitoring Activity on the Web Console

All badge scan activity is visible in real time on the Web Console:

- Occupancy - Live zone occupancy counts. Click any zone to see who is currently inside.



- Activity History - Searchable log of all entry and exit events - date, user, badge, door, zone, and result.



Reader Validations

Validation methods determine how the handheld decides whether to grant or deny access on each scan. These are configured in the Reader Profile under the Reader Validations tab. See the [Reader Profile](#) section above.

Troubleshooting - Entry/Exit

Badge Scan Not Recognized

- Confirm the badge credential type matches the reader's configured format (proximity, UHF RFID, barcode/QR, or OCR).
- Verify the badge holder is enrolled in XPressEntry and has an active credential.
- Use Manual Entry as a fallback to record the event by badge number.

Entry/Exit Activity Not Appearing on the Web Console

- Ensure the handheld has network connectivity and has synced with the XPressEntry server.
- Check that the Reader Profile has Enable Entry/Exit enabled under Handheld Modes.
- Verify the correct door is selected via Set Door; scans are logged against the currently assigned door.

Cannot Change Door Assignment

- Verify that the Reader Profile is not locked to a fixed door assignment.
- Confirm the operator account has sufficient permissions to reassign the door.

Access granted when it should be denied (or vice versa)

- Review the Reader Validations tab in the Reader Profile. Confirm the correct validation methods are checked and the user's group has the correct zone or reader permissions.

Emergency Mustering

Overview

Emergency Mustering uses XPressEntry's handheld readers to account for all on-site personnel during an emergency or drill. When a muster event is active, everyone currently on-site appears in the Missing list on both the Web Console and connected handhelds. As each person is scanned or manually confirmed, they move to the Scanned list. A single handheld reader can process 250 check-ins in under 5 minutes - always prioritize badge scanning before manually processing anyone without a credential.

Setup Checklist

Complete these steps before conducting a muster event:

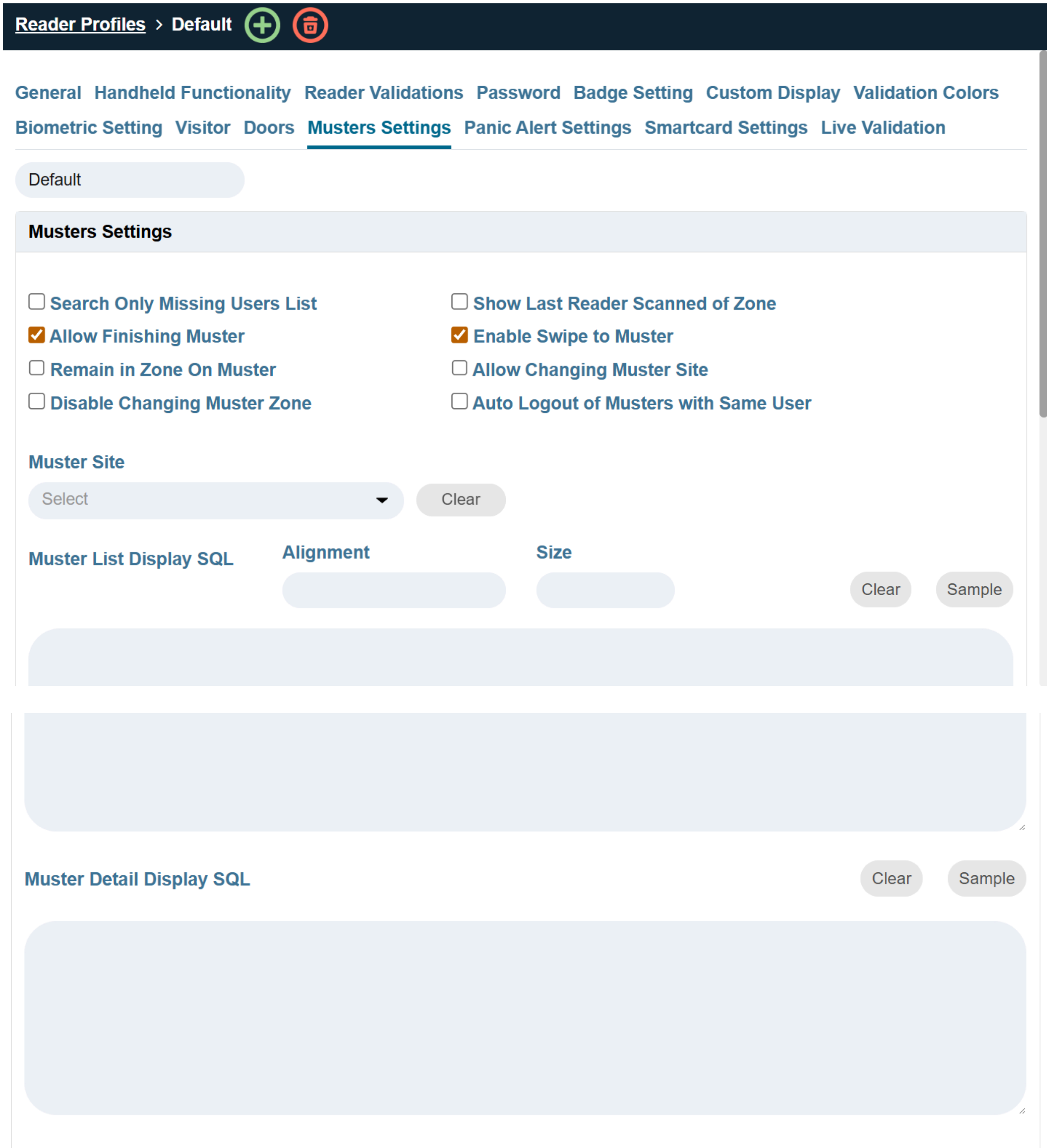
1. In the **Reader Profile** assigned to your handheld, confirm **Enable Muster** is checked under **Handheld Modes**, and configure **Muster Settings** options as needed.
2. Configure **Zones**: designate tracked work areas with **Zone Tracks Occupancy**, and assembly areas with both **Zone is Outside** and **Zone is a Muster Point**.
3. Create **Muster Sites** if the facility has multiple buildings or locations.
4. Configure Muster Settings and Alert Settings if SMS or email notifications are required.
5. Sync the handheld and deploy it to the assembly point.

Reader Profile - Musters Settings Tab

Each Reader profile includes a Musters Settings tab that controls how the handheld behaves specifically during a muster event. Navigate to Reader Profile, open the assigned profile, and click the Musters Settings tab. Configure settings as needed:

Setting	Description

Search Only Missing Users List	Restricts the handheld search to the Missing list only. Recommended for large sites.
Allow Finishing Muster	Permits handheld operators to finish a muster event from the device. Enabled by default.
Remain in Zone on Muster	Prevents XPressEntry from updating the user's zone when scanned at a muster point. Preserves last-known work location data.
Disable Changing Muster Zone	Locks the handheld to its assigned muster zone and prevents operators from switching during the event.
Show Last Reader Scanned of Zone	Displays the last reader's name rather than the zone name in the user list.
Enable Swipe to Muster	Allows operators to muster a user by swiping left or right on their record. Enabled by default.
Allow Changing Muster Site	Permits the operator to switch the active Muster Site from the handheld during an event.
Auto Logout of Musters with Same User	Automatically logs out a muster session if the same credential is scanned again.
Muster Site	Assigns a specific Muster Site to this Reader Profile. The handheld will only display data for that site. Leave blank to show all zones.
Muster List Display / Muster Detail Display SQL	Advanced fields for customizing how user data appears in the muster list. Contact Telaeris support for guidance.



Muster Sites

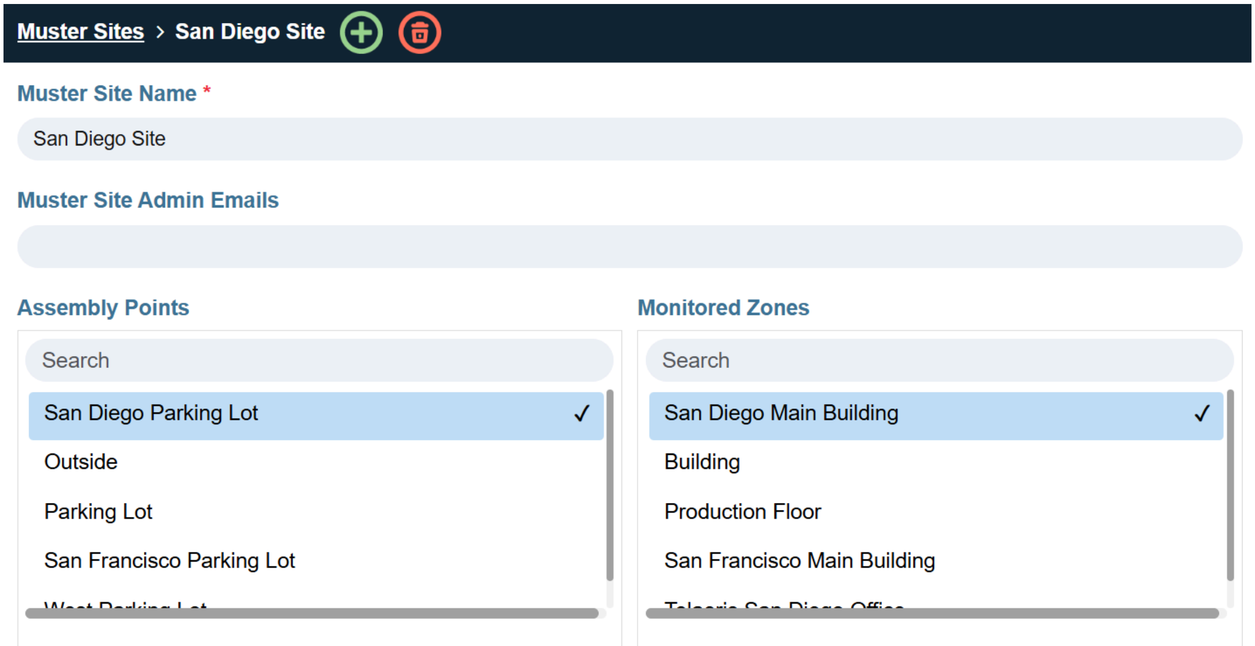
What are Muster Sites?

A Muster Site represents a grouped list of monitored zones at a specific facility location. Without Muster Sites, a handheld shows all on-site personnel across the entire system. With Muster Sites, each handheld displays only the zones and personnel relevant to its assigned location.

This is essential for multi-building or enterprise deployments. For example, if a company runs one XPressEntry system across facilities in San Diego and San Francisco, a muster event in San Diego should only show San Diego personnel — not employees at the San Francisco facility. Creating a Muster Site for each location keeps each handheld focused on the right people and the right assembly points.

When creating a Muster Site under the Muster Sites page, the following fields are available:

Field	Description
Muster Site Name	The name of the site (required), e.g., "San Diego Site" or "Building A".
Muster Site Admin Emails	Email addresses of Muster Site administrators.
Assembly Points	The zones where mustered personnel check in. Click a zone to select it (a checkmark appears). Personnel scanned in these zones are marked as Scanned.
Monitored Zones	The zones whose occupancy is tracked during the event. Personnel in these zones appear on the Missing list when a muster begins.



Creating a Muster Site

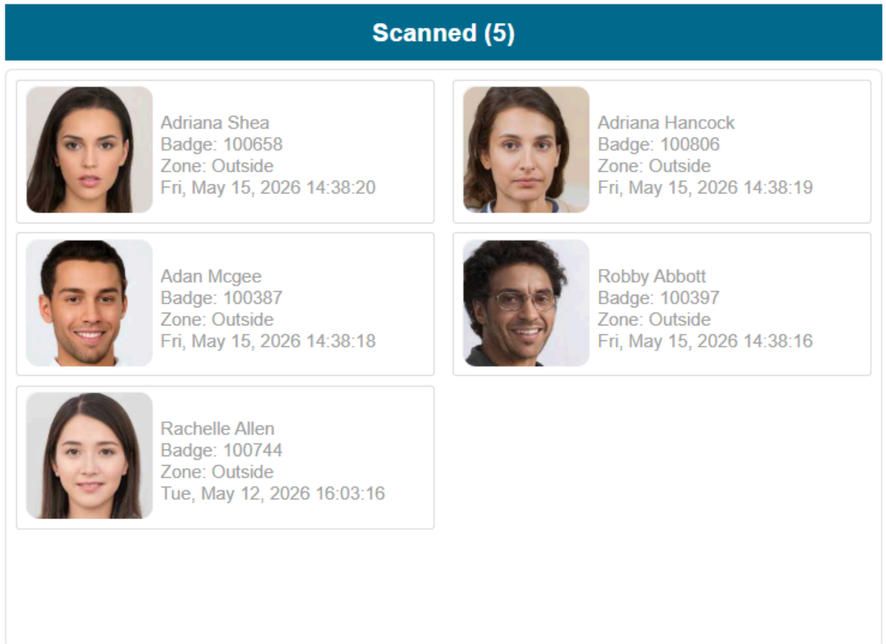
1. Navigate to **Muster Sites** in the left navigation panel.
2. Click the **Add** icon to create a new site.
3. Enter a Muster Site **Name**.
4. Optionally enter admin email addresses.
5. Under **Assembly Points**, click the zone(s) where mustered personnel will assemble. A checkmark appears next to selected zones.
6. Under **Monitored Zones**, click the zone(s) whose occupancy will be tracked during the muster event.
7. Click **Save**.

Web Console Muster Views

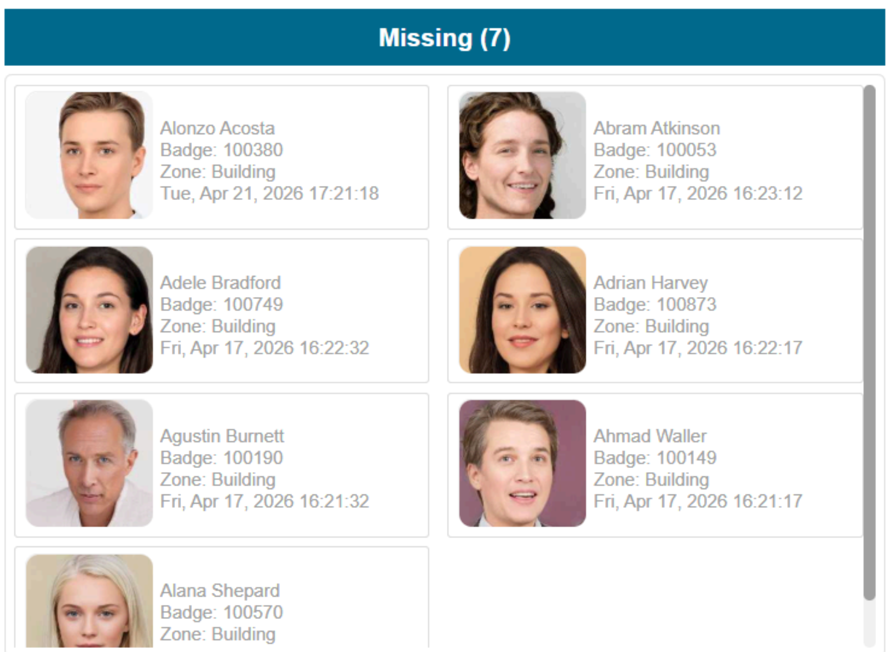
Muster Page

The Muster page is the primary interface for monitoring and managing an active event. It shows:

- Scanned panel (left):



- Missing panel (right):

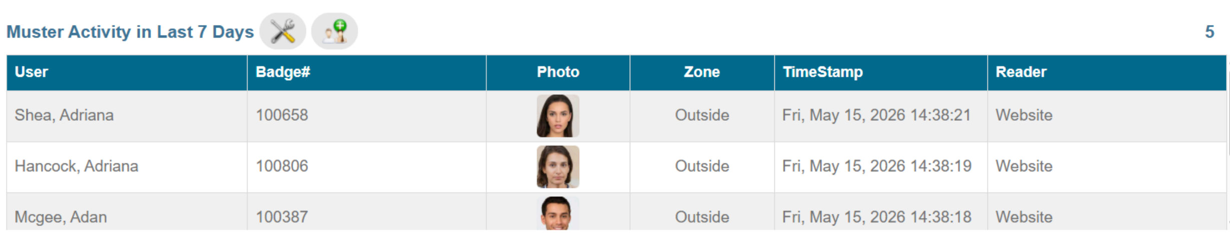


- Site label: Displayed above the panels (e.g., "Mustering Site: All Zones"), indicating whether a site filter is active.

Mustering Site : All Zones

Toolbar Control	Description	Icon
Wrench icon	Opens the site filter. Select a Muster Site to scope the view, or All Zones to show all personnel.	
Finish button	Ends the active muster event. Prompts for an event name.	Finish
X button	Cancels the active muster event without saving.	
Refresh button	Manually refreshes the Missing and Scanned lists.	
User Filter / Search User	Filters the Missing list by name to quickly locate a specific person.	User Filter Search User
PDF/CSV icons	Exports the current muster data.	PDF CSV

Below the panels, the Muster Activity in Last 7 Days table shows recent scan history: User, Badge #, Photo, Zone, Timestamp, and Reader.


Muster Activity in Last 7 Days 5

User	Badge#	Photo	Zone	TimeStamp	Reader
Shea, Adriana	100658		Outside	Fri, May 15, 2026 14:38:21	Website
Hancock, Adriana	100806		Outside	Fri, May 15, 2026 14:38:19	Website
Mcgee, Adan	100387		Outside	Fri, May 15, 2026 14:38:18	Website

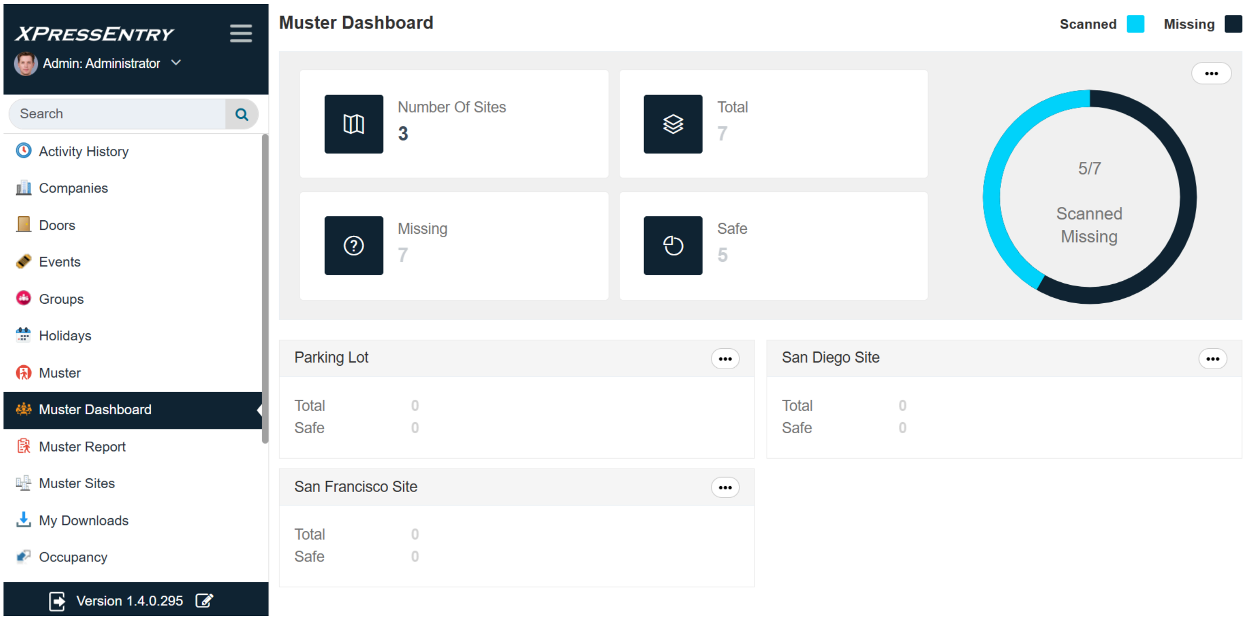
Badge holders can be moved from Missing to Scanned on the Web Console by dragging their card. This cannot be reversed from the console.

Muster Dashboard Page

The Muster Dashboard provides a high-level summary of an active or recent muster event, including:

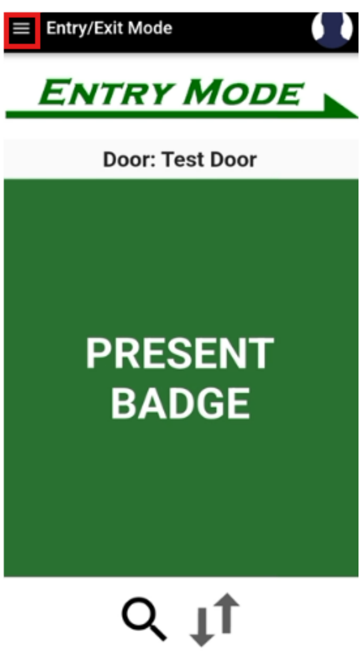
- Summary tiles: Number of Sites, Total personnel, Missing count, and Safe (Scanned) count.
- Chart: Visual proportion of Scanned vs. Missing out of the total.

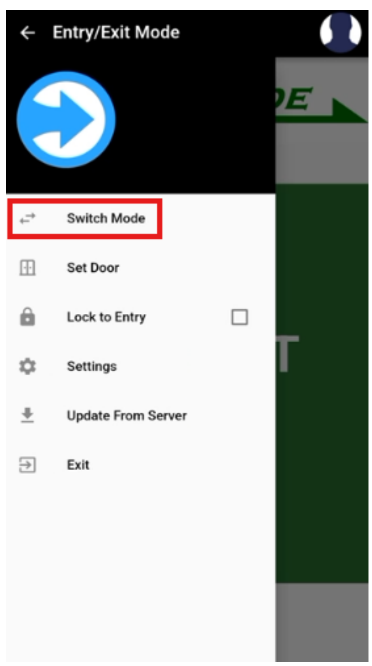
- Per-site cards: Each Muster Site shown with its own Total and Safe counts, so supervisors can see accountability by location at a glance.

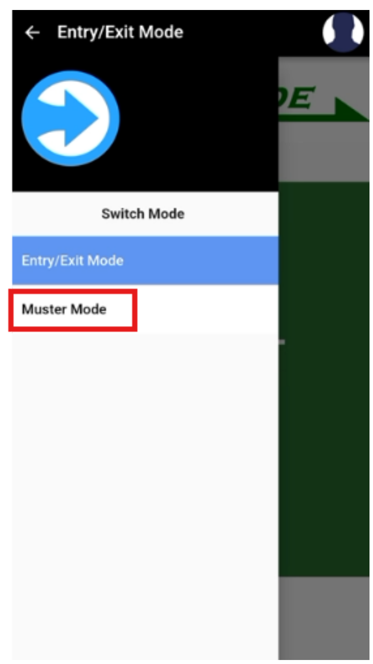


Mustering on the Handheld

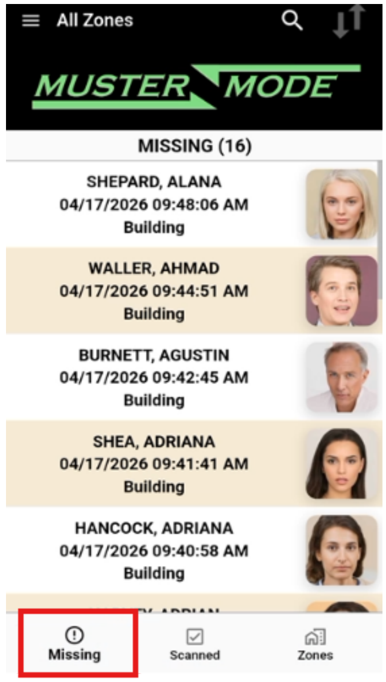
1. Tap the hamburger menu icon and select **Switch Mode** > **Muster Mode**.



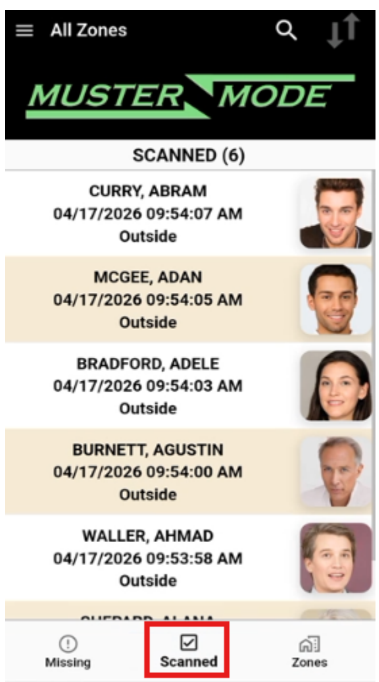


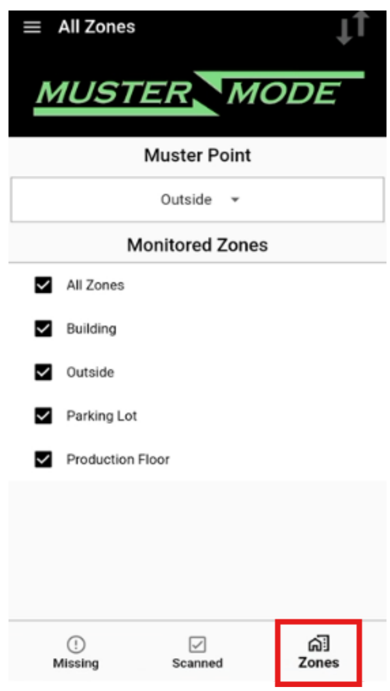


2. The Missing list appears, showing all unaccounted personnel with their photo, name, badge, zone, and last scan time.

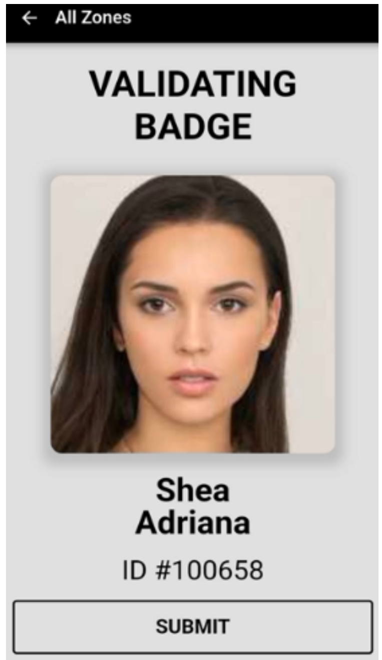


3. An additional page is available for Scanned User entries and Monitored Zones.

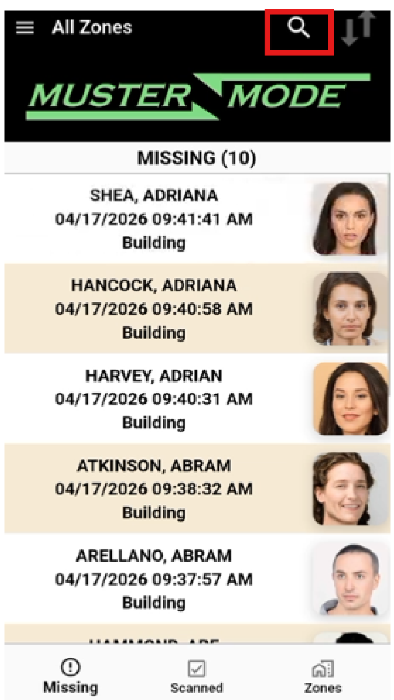


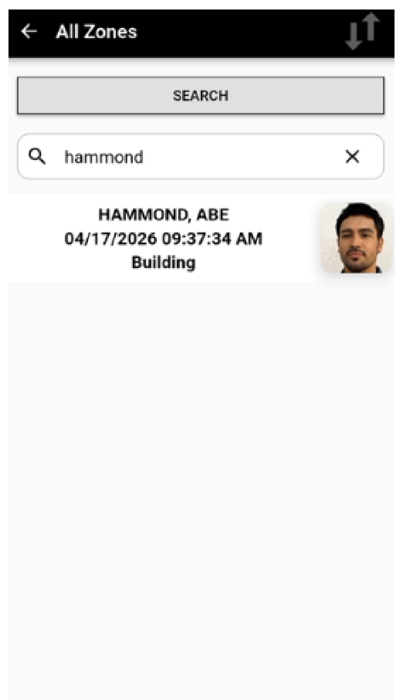


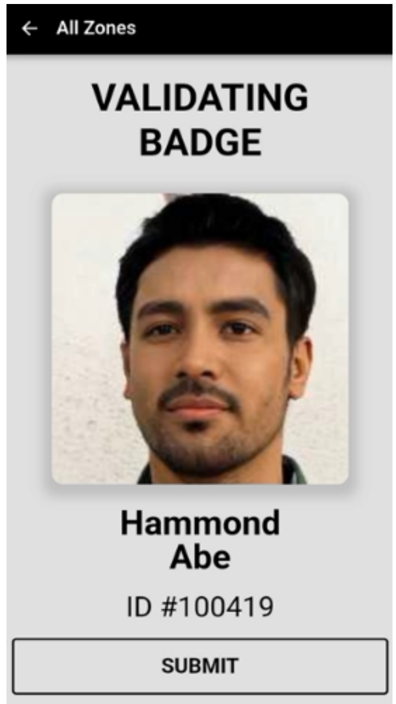
4. Scan each person's badge as they arrive at the assembly point. Their card moves from **Missing** to **Scanned**.



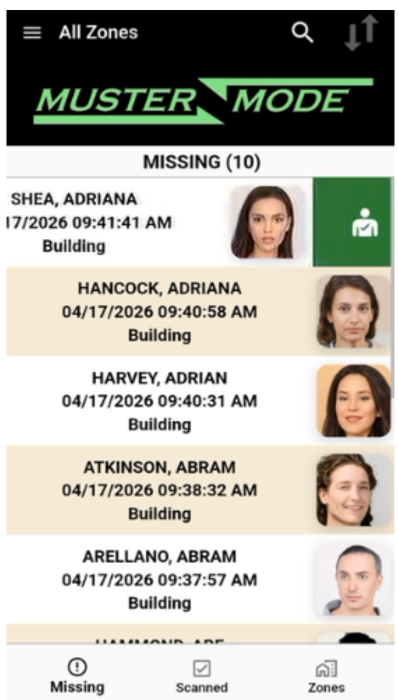
5. If a badge cannot be scanned, tap the search icon, enter the person's name or badge ID, select them from the results, and tap **Submit**.



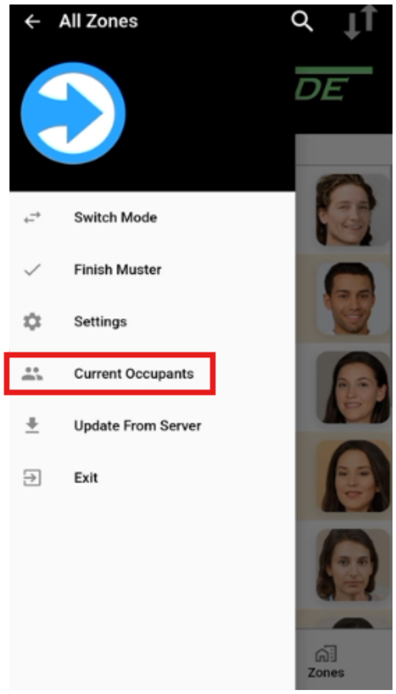


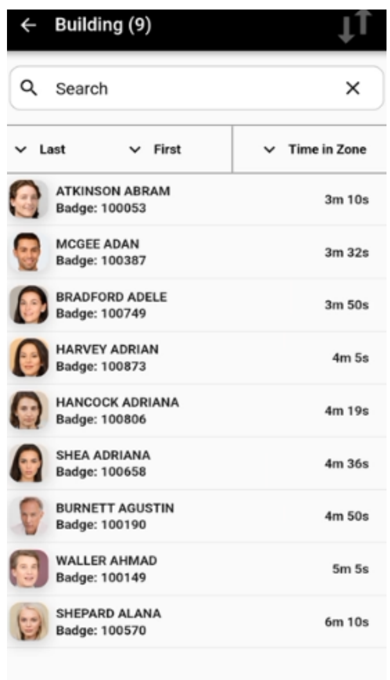


6. Swipe left or right on a card to muster without tapping Submit (if Enable Swipe to Muster is on).



7. To view Current Occupants, tap the hamburger menu icon and select Current Occupants and a specific zone.



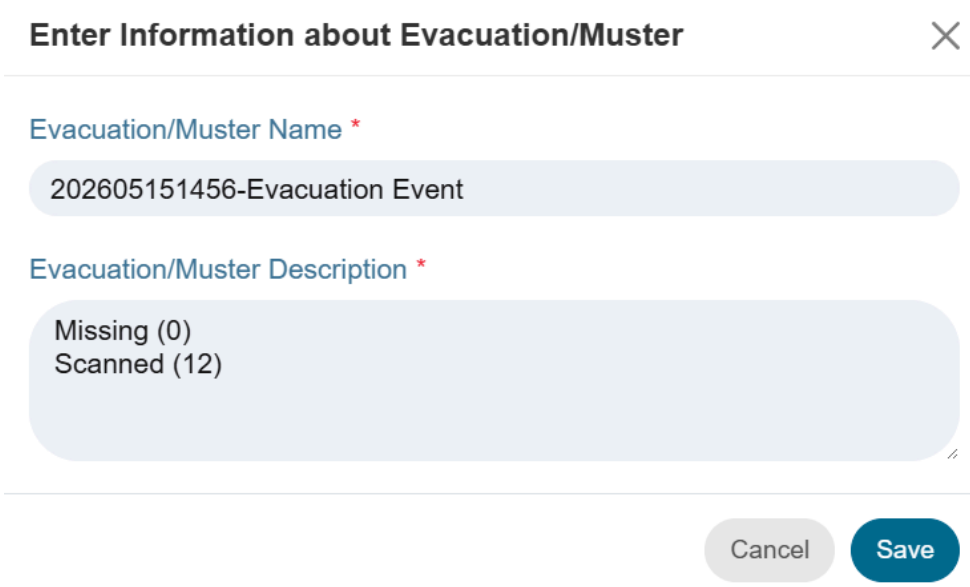


Finishing a Muster Event

From the Web Console:

1. Click the **Finish** button in the Muster page toolbar.

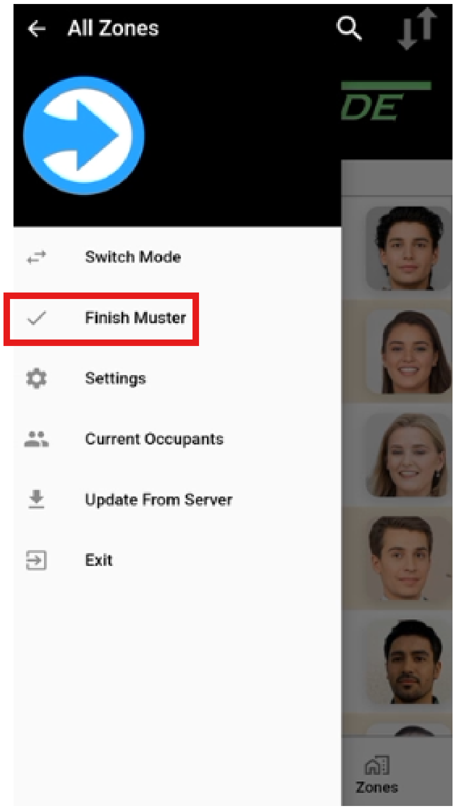
2. Enter an event name (e.g., "April Evacuation Drill"). The description is optional.

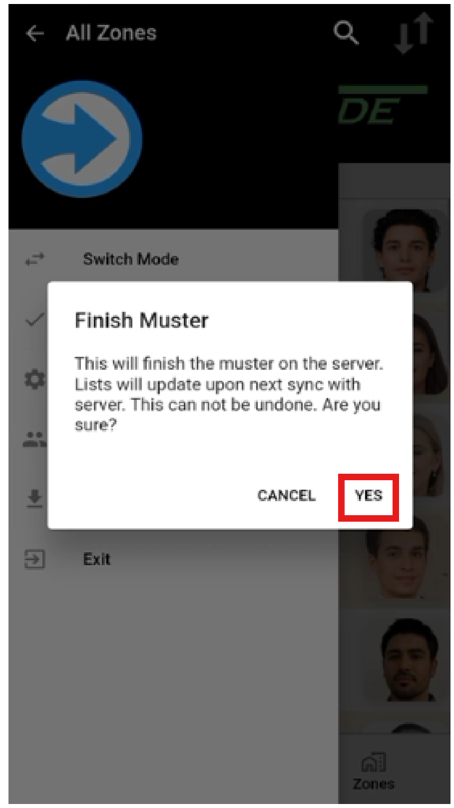


3. Click **Save**.

From the Handheld:

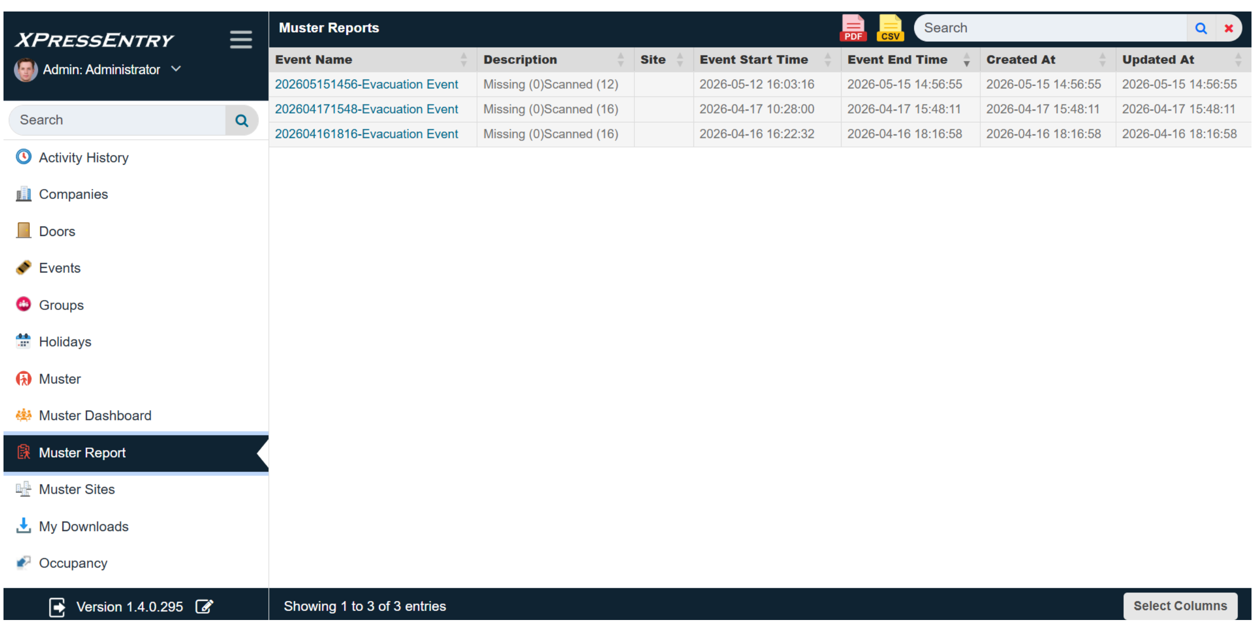
1. Tap the hamburger menu icon and select Finish Muster.
2. Confirm when prompted. This action cannot be undone.





Muster Reports

The Muster Report tab lists all completed events. Each row shows the Event Name, Description, Site, Event Start Time, Event End Time, Created At, and Updated At. Click any event to view detailed results including all Scanned and Missing personnel. Export using the PDF or CSV icons at the top right.



Mustering Best Practices

- Configure Zones correctly first: Tracked work areas need Zone Tracks Occupancy. Assembly areas need Zone is Outside and Zone is a Muster Point.
- Use Muster Sites for multi-location facilities: Scope each handheld to only the zones it needs to monitor so operators are not overwhelmed by unrelated personnel.
- Enable Allow Finishing Muster in the Reader Profile: This lets operators close the event from the handheld without needing Web Console access.
- Scan badges first: Scanning is dramatically faster than manual check-ins. Reserve manual processing for personnel without a badge.
- Run regular drills and save reports: Muster reports allow the user to track response times and accountability rates across events to identify and address gaps.

Troubleshooting - Mustering

Handheld Not Showing Occupancy

- Confirm the Reader Profile has Enable Muster checked
- Verify the Muster Site is configured correctly and the handheld's profile is associated with it
- Ensure the handheld has synced with the server recently

Occupancy Data is Stale or Inaccurate

- Set the Auto Exit User # Hours value to automatically clear personnel who have not badged out
- Confirm the PACS integration is actively syncing badge activity to XPressEntry
- Check that exit readers are properly mapped as doors with Start and End zones

Cannot Finish Muster from Handheld

- Verify that Allow Finishing Muster is enabled in the Reader Profile for that device

Events Mode

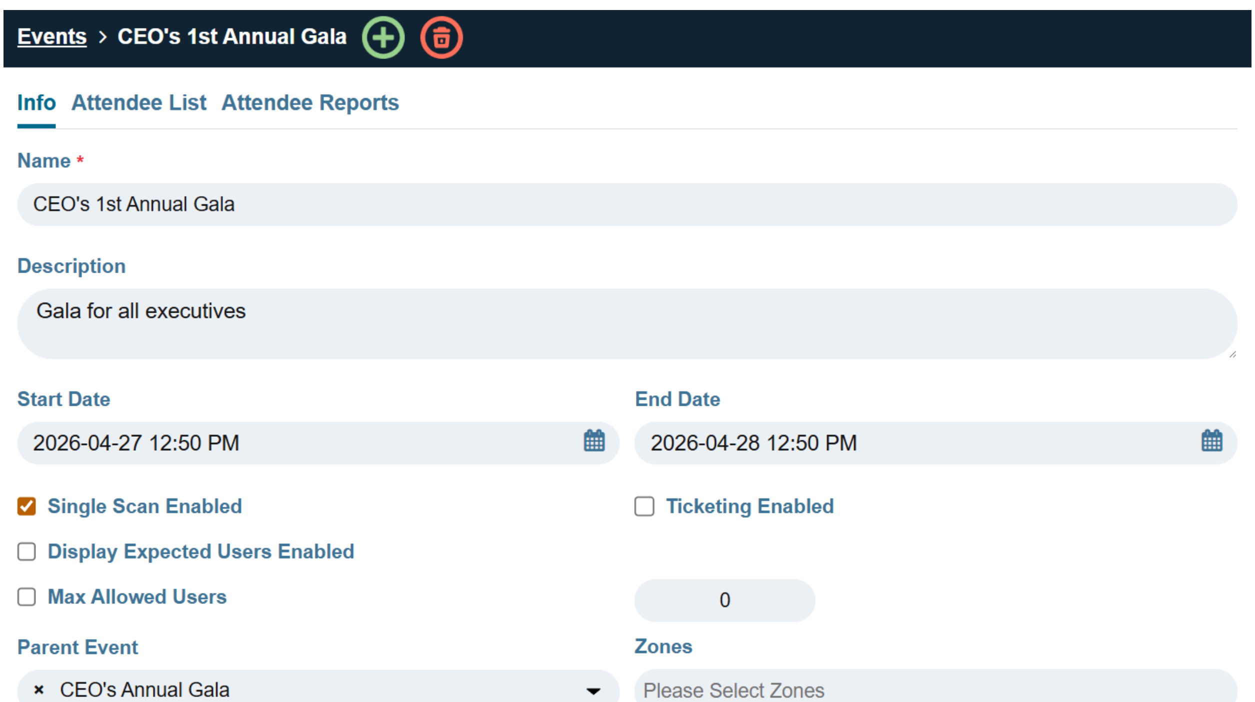
XPressEntry Events Mode allows administrators to use their existing personnel list, whether sourced from an integrated access control system database or a standalone XPressEntry database, to manage and track attendance at any closed event. The feature is particularly powerful because the handheld device does not require a live connection to the database in order to authenticate attendees. Once synced, it can operate independently, making it suitable for off-site venues or locations with limited connectivity.

Key capabilities include:

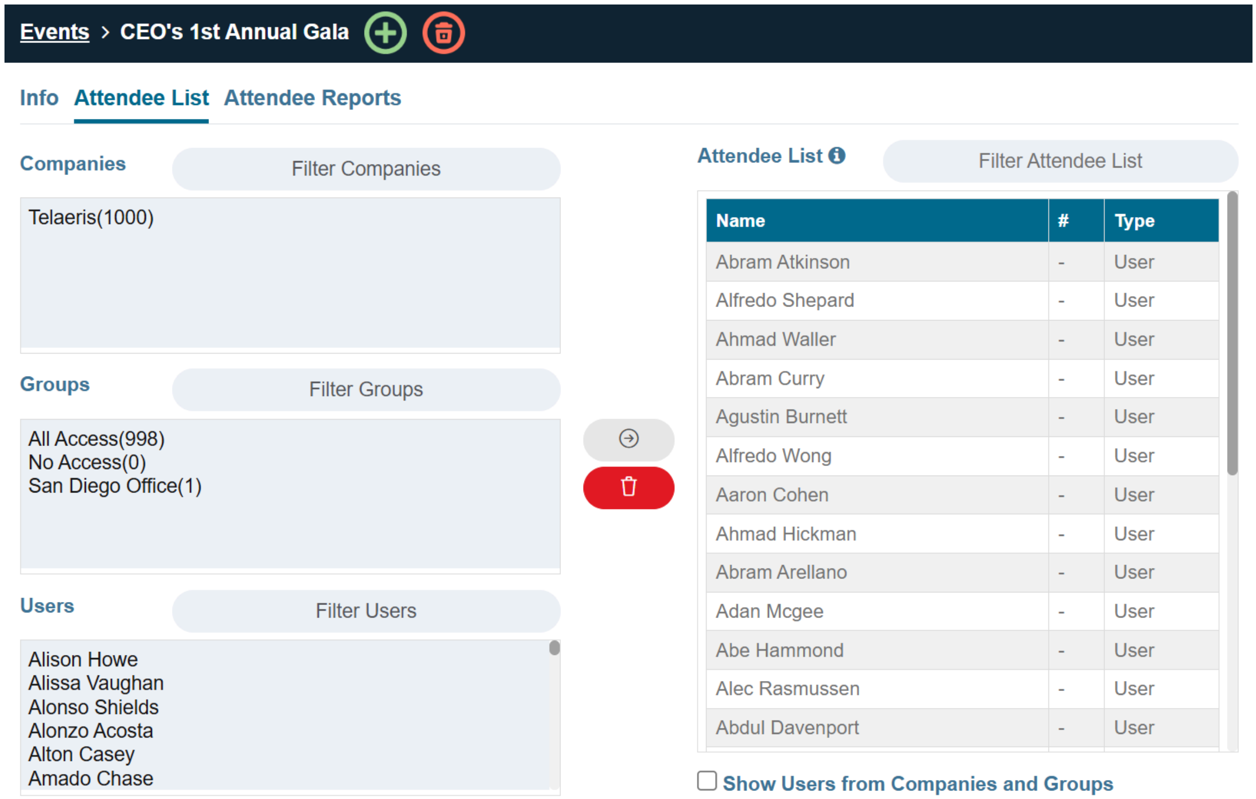
- Instant event setup - Create events in minutes using personnel already in the XPressEntry database.
- Flexible attendee selection - Invite an entire company, specific access groups, or hand-picked individual users.
- Single scan control - Prevent card pass-back and duplicate entries by limiting each badge to one check-in.
- Real-time tracking - Monitor check-ins as they happen from the server when the handheld is connected.
- Comprehensive reporting - Generate attendee reports showing who came in, who was denied, and who attempted multiple entries. Export as a CSV for payroll, compliance, or records.
- Event organization - Archive completed events to keep the interface clean, and group recurring events under a parent event for easy access.

Creating an Event

1. Navigate to **Events** in the left navigation panel.
2. Click the **Add** icon at the top of the list.
3. Fill in the event details (see Event Info Fields below).
4. Click **Save**.



5. Switch to the **Attendees** tab and add the attendee list.



6. Click **Save** again. The event is now ready and will appear on synced handhelds.

Event Info Fields

The following fields are available on the Info tab when creating or editing an event.

- **Event Name** - A descriptive name for the event (e.g., "CEO's Annual Gala"). This name is displayed on the handheld when operators select an event to begin.
- **Description** - Optional notes about the event (e.g., "Gala for all executives").
- **Start Date** / **Start Time** - The date and time the event is expected to begin. Handheld devices show only events that fall within their active window.
- **End Date** / **End Time** - The date and time the event is expected to end.
- **Single Scan** Enabled - Optional. When checked, each badge holder is permitted only one entry into the event. See Single Scan Enabled for details.
- **Display Expected Users** Enabled - Displays the list of expected attendees on the handheld.
- **Max Allowed Users** - Sets a hard cap on the number of people who can check into the event; once the limit is reached, further scans are denied.
- **Ticketing Enabled** - When enabled, attendees must present a valid ticket credential in addition to their badge to check in to the event. Contact Telaeris support for details on ticketing configuration.

- **Parent Event** - Optional. Assign this event to a parent event to group recurring events together (e.g., monthly training sessions under an annual series). See Grouping Events with Parent Events for details.
- **Zones** - The zone(s) where the event will take place.

Adding Attendees

After saving the event's basic information, switch to the Attendees tab to define who is permitted to attend. XPressEntry offers three methods for building the attendee list, which can be used in any combination.

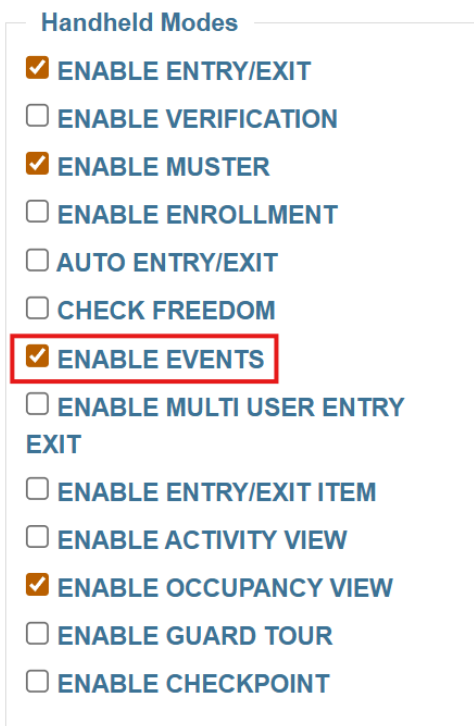
- By Company - The company selector appears at the top of the Attendees tab. Click the company name, then click the arrow to the right to add all members of that company to the event. This is the fastest option when an entire organization or contractor company is invited.
- By Group - Select a specific access control group from the list. These can be groups already configured in your integrated access control system, or groups created within XPressEntry for standalone installations. Click the arrow to move the group into the attendee list.
- By Individual - Use the user filter/search to find specific people by name. Select them individually to add them to the list.

Note: For large events, using company or group selection is faster than selecting individuals. Individual selection is best suited for small, invitation-only gatherings.

Once the attendee list is complete, click Save.

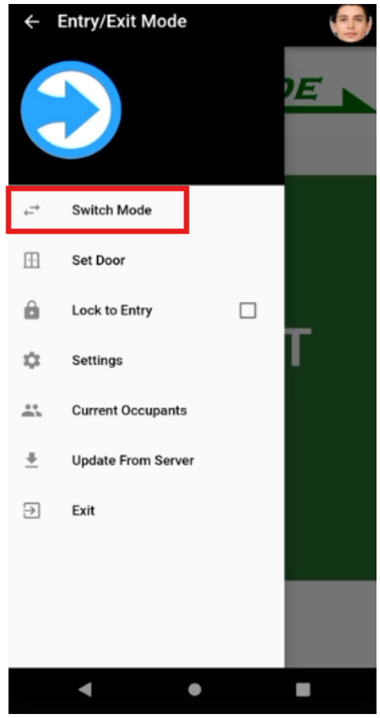
Running an Event on the Handheld

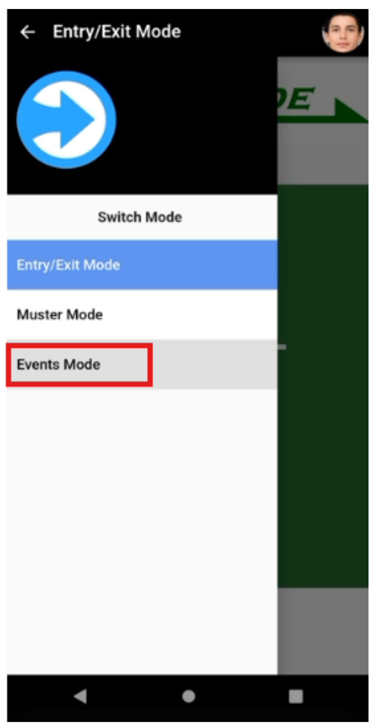
Before running an event, ensure Enable Events is checked in the Handheld Functionality tab of the Reader Profile assigned to the device.



Switching to Events Mode

1. Tap the hamburger menu icon in the top-left corner.
2. Tap **Switch Mode**.
3. Select **Events Mode**.



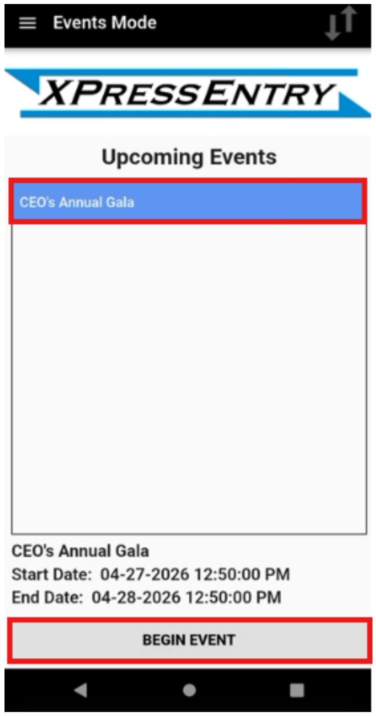


Selecting and Beginning an Event

Once in **Events Mode**, all active events that fall within the current date / time window and have been synced to the device will be displayed.

1. Review the list of available events on the screen.

2. Tap the event to activate (e.g., "CEO's Annual Gala").
3. Tap **Begin Event**.



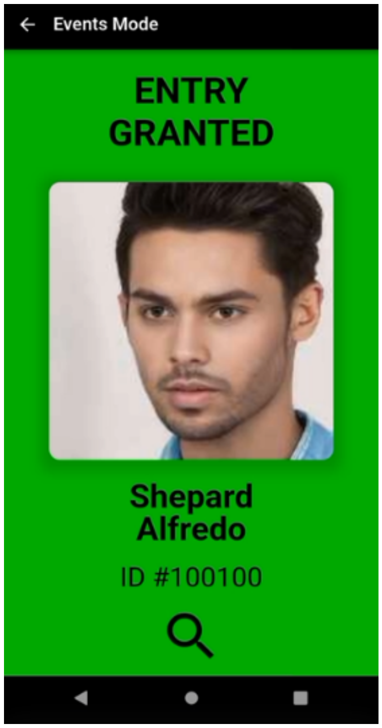
The event is now active. Attendees can immediately begin presenting their badges.

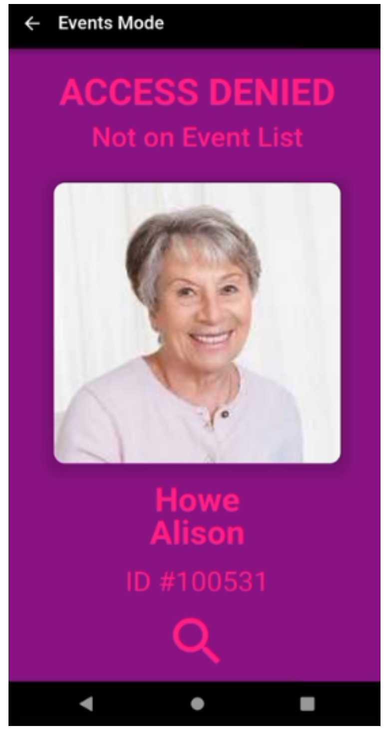
Note: If the expected event does not appear on the handheld, tap the sync button (up/down arrows) to update from the server and pull down the latest event list.

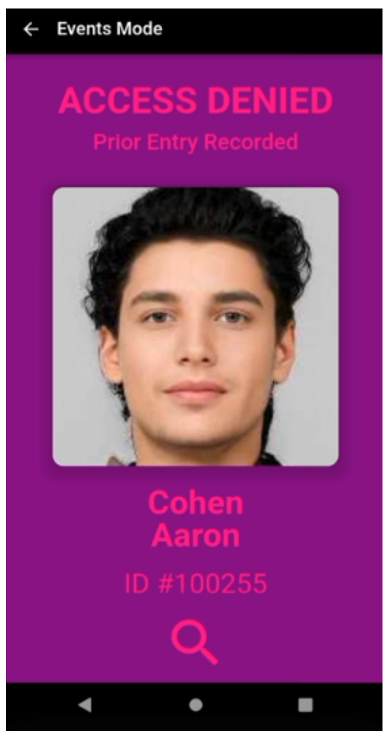
Scan Results

Each badge scan produces one of the following results on the handheld screen:

- Entry Granted - The badge holder is on the event's attendee list and has been successfully checked in.
- Not on Event List - The badge holder is not included in the event's attendee list and is denied entry.
- Prior Entry Recorded - The badge holder has already been scanned into this event. Only shown when Single Scan Enabled is active. Entry is denied to prevent card pass-back.







Attendee Reports

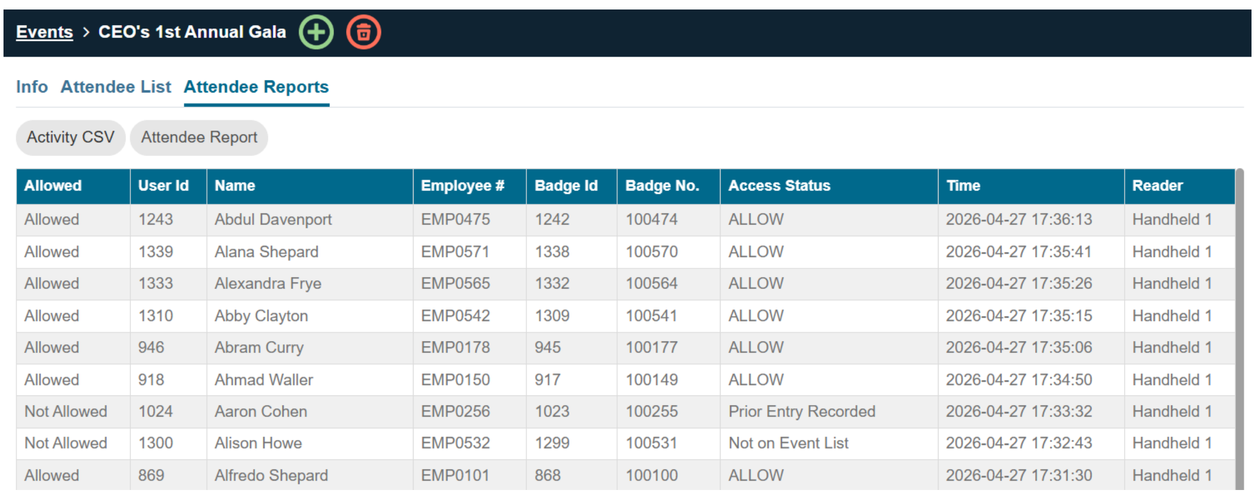
After an event concludes, attendance reports are available directly from the XPressEntry Web Console. From the Events tab, select the event to save a report on and navigate to its Attendee Report section.

Two CSV reports are available for export:

- **Activity CSV** - A chronological log of every badge scan attempt during the event. Each row represents a single scan, so an attendee may appear multiple times. This report is useful for auditing access activity in detail and includes the outcome of each scan attempt, such as:
    - Access granted
    - Not on event list
    - Prior entry recorded
    - Maximum users entered
- **Attendee Report** - A one-row-per-person summary of everyone on the event's invite list, regardless of whether they attended. Use this report to quickly see overall attendance, confirm check-in times, and identify no-shows.

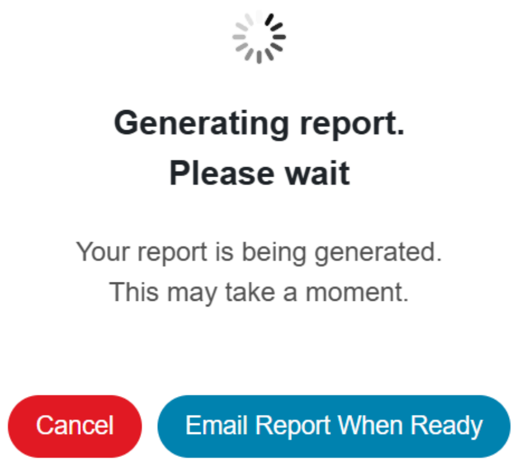
To export either report:

1. From the **Events** tab on the Web Console, select the event to run a report on.
2. Navigate to the **Attendee Report** section for that event.
3. Review the results on screen.
4. Click **Activity CSV** or **Attendee Report** to download the file.
5. Open the CSV on a PC and use it for payroll, compliance records, management reporting, or any other purpose.



Allowed	User Id	Name	Employee #	Badge Id	Badge No.	Access Status	Time	Reader
Allowed	1243	Abdul Davenport	EMP0475	1242	100474	ALLOW	2026-04-27 17:36:13	Handheld 1
Allowed	1339	Alana Shepard	EMP0571	1338	100570	ALLOW	2026-04-27 17:35:41	Handheld 1
Allowed	1333	Alexandra Frye	EMP0565	1332	100564	ALLOW	2026-04-27 17:35:26	Handheld 1
Allowed	1310	Abby Clayton	EMP0542	1309	100541	ALLOW	2026-04-27 17:35:15	Handheld 1
Allowed	946	Abram Curry	EMP0178	945	100177	ALLOW	2026-04-27 17:35:06	Handheld 1
Allowed	918	Ahmad Waller	EMP0150	917	100149	ALLOW	2026-04-27 17:34:50	Handheld 1
Not Allowed	1024	Aaron Cohen	EMP0256	1023	100255	Prior Entry Recorded	2026-04-27 17:33:32	Handheld 1
Not Allowed	1300	Alison Howe	EMP0532	1299	100531	Not on Event List	2026-04-27 17:32:43	Handheld 1
Allowed	869	Alfredo Shepard	EMP0101	868	100100	ALLOW	2026-04-27 17:31:30	Handheld 1

Note: If the report takes a while to generate, users can select Email Report When Ready instead of waiting for the download to complete. The report will be emailed to the designated email once it is ready.



Reports are stored on the Web Console and remain accessible for historical review at any time, even after the event has ended.

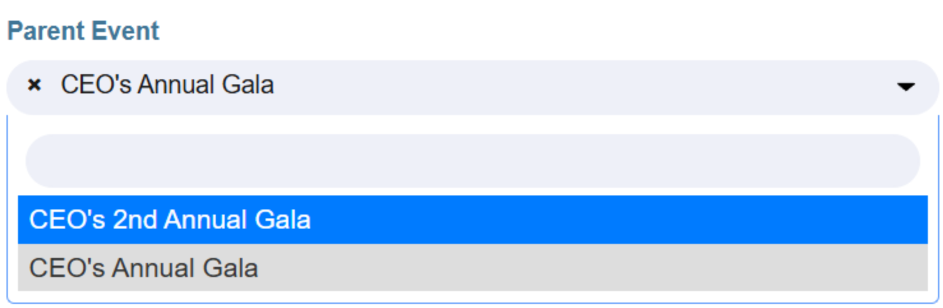
Grouping Events with Parent Events

For recurring events - such as monthly mandatory training that runs throughout the year - XPressEntry allows individual event instances to be grouped under a single Parent Event. This keeps the Events list organized and makes it easy to find related events and their collective attendee reports in one place.

For example, if an organization runs "HSC Mandatory Training" every month, it might create individual events called HSC January, HSC February, HSC March, and so on, and then assign them all the same parent event ("HSC Mandatory Training Annual").

To assign a parent event:

1. Open the child event (e.g., "HSC February") and go to the Info tab.
2. Use the Parent Event dropdown to select the parent event to group it under.
3. Click Save.



Events Best Practices

1. Create events before the day of the activity - This gives handheld devices time to sync the event details from the server.
2. Sync the handheld immediately before the event - Tap the sync button on the handheld to ensure the latest attendee list and event settings are loaded.
3. Use company or group selection for large events - This is faster to set up than adding users individually and automatically includes newly added members.
4. Enable Single Scan for secure events - Prevents card pass-back and ensures each physical attendee is individually verified.
5. Export reports promptly after each event - Particularly important for mandatory training with compliance requirements.
6. Use Parent Events for recurring series - Grouping monthly or quarterly events keeps the list clean and reporting organized.

Troubleshooting - Events

Event Does Not Appear on the Handheld

- Confirm Events Mode is enabled under Reader Profiles > Handheld Functionality > check Enable Events and that Save was clicked.
- Tap the sync button (up/down arrows) on the handheld to update from the server.
- Check that the event's Start Date and End Date fall within the current date/time window.

Attendee Scan Shows "Not on Events List"

- Confirm the badge holder has been added to the event's attendee list (by company, group, or individually).
- If the attendee was added after the handheld last synced, re-sync the device to pull the updated list.

"Prior Entry Recorded" Appears Unexpectedly

- This message only appears when Single Scan Enabled is active for the event.
- Verify whether Single Scan Enabled is intentionally checked for this event on the Info tab.

Scans Not Appearing in the Attendee Report

- Check the handheld's network connectivity. Scans made offline are stored locally and will sync automatically once connectivity is restored.

- Confirm the correct event was selected on the handheld before scanning began.

Reports and Activity History

The XPressEntry Web Console provides real-time visibility into facility access activity and handheld reader status. Its reporting capabilities allow administrators to monitor, analyze, and export data captured from all connected XPressEntry handheld readers and integrated access control systems.

Key reporting capabilities include:

- Real-time activity monitoring - View entry and exit events as they happen, including scan results, door assignments, and user identity.
- Scheduled email reports - Configure SMTP-based reports that are automatically delivered to designated recipients on a defined schedule.
- Activity History log - Search and filter all historical scan activity across every reader, date range, and user.
- CSV report - Download raw activity data for use in payroll, compliance records, or security audits.

The Reports tab is accessible from the main navigation panel of the XPressEntry Web Console.

1. Log in to the XPressEntry Web Console using administrator credentials.
2. In the left-hand navigation panel, click **Reports**.
    a. If the **Reports** tab is not visible, click the edit icon at the bottom of the navigation panel and check **Reports**. Click **Save**.
3. The **Reports** list will display all configured reports. Click any report name to view or edit it.

Note: If the Reports tab is not visible, confirm that the user role has permission to access Reports. Contact the system administrator to adjust role permissions if needed.

Creating a Report

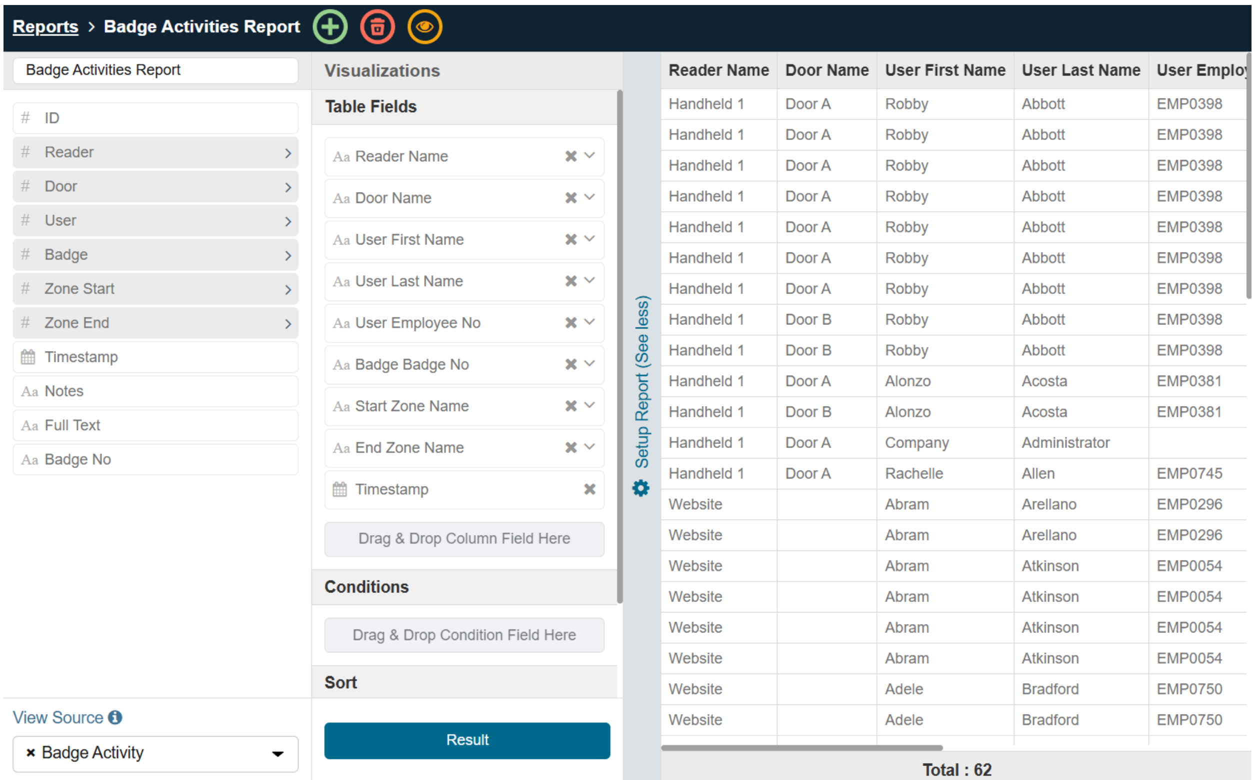
To create a new report:

1. Click the **Reports** tab in the left navigation panel.
2. Click the **Add** (+) icon at the top of the **Reports** list.
3. Select the Report type (see Report Types below).
4. Fill in the report details (see Report Fields below).
5. Click **Save**.

Report Fields - Dynamic Reports

The following fields are available when creating or editing a dynamic report:

- **Report Title** - A descriptive name for the report (e.g., "Daily Entry Activity"). This name appears in the Reports list.
- **View Source** - The source/category of data the report covers. Options include Badge Activity, Muster Activity, Event Activity, and more depending on what features are enabled.
- **Table Fields**
- **Conditions**
- **Sort** - Users can sort the report by a specific field. Select a field and choose to sort by ascending or descending order.

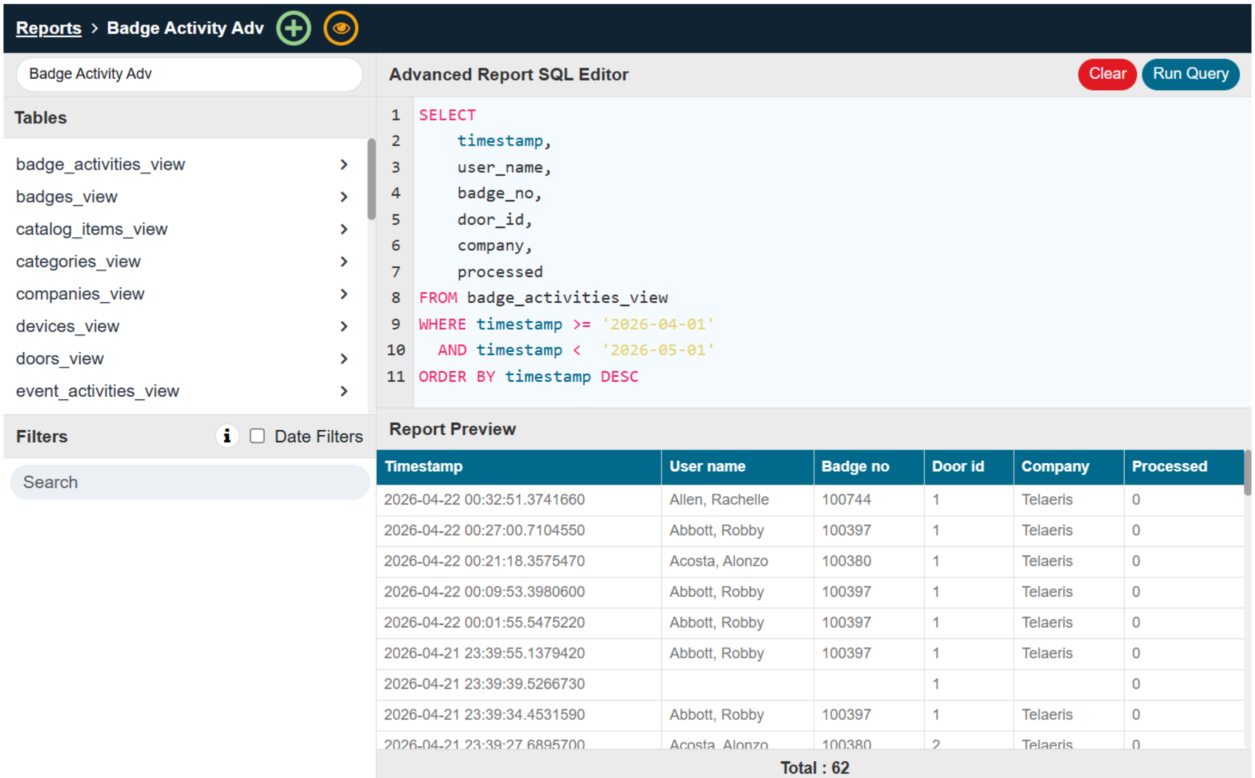


Report Fields - Advanced Reports

The following fields are available when creating or editing an advanced report:

- **Report Title** — A descriptive name for the report. Appears in the Reports list and in the subject line of scheduled report emails.
- **Tables** — Lists all available database views for reference. Expand any view to inspect its column names before writing a query.
- **Filters** — Optional user-facing filter parameters, such as a date range selector. Enable Date Filters to automatically inject a standard date range condition into the query at run time.

- **Advanced Report SQL Editor** — A syntax-highlighted code editor for entering custom SELECT statements. Only SELECT statements are permitted; INSERT, UPDATE, DELETE, and DDL commands are blocked.



SMTP Email Configuration

Before scheduled reports can be delivered, an SMTP server must be configured in the XPressEntry Web Console. SMTP settings are defined at the system level and apply to all reports.

To configure SMTP:

1. Navigate to **Settings** in the Web Console.
2. Locate the Email / SMTP section.
3. Enter the organization's SMTP server address, port, authentication credentials, and sender address.
4. Click **Save** and use the Test Email function to confirm delivery is working.

Note: Contact the IT team for SMTP server details. Common configurations use port 587 (TLS) or 465 (SSL). If test emails are not received, verify that the XPressEntry server IP is allowed to relay through the mail server.

Report Types: Dynamic and Advanced

XPressEntry offers two report types for querying and exporting data from the Web Console: Dynamic Reports and Advanced Reports. Both produce exportable output, but they differ significantly in how the query is constructed and who they are intended for.

Dynamic Reports

A Dynamic Report is a drag-and-drop visual report builder designed for administrators who want to extract and filter data without writing any code. The user chooses a data source, then drags fields from the left panel directly into the report layout. The Web Console assembles the underlying query automatically - no SQL knowledge is required.

Dynamic Reports are best suited for routine operational reporting tasks - such as reviewing badge scan activity, checking occupancy counts, or producing attendance summaries - that need to be run regularly by security or HR staff without technical assistance.

Dynamic Report Interface

The Dynamic Report editor is divided into three areas:

- Left panel - Field browser. Lists all available fields for the selected data source, grouped by related entities. For example, for the Badge Activity source, fields are grouped under Reader, Door, User, Badge, Zone Start, and Zone End. Use the View Source dropdown at the bottom of this panel to switch between data sources such as Badge Activity, Events, or Muster.
- Center Panel - Visualizations. Contains three drop zones: Table Fields (drag the columns to appear in the output here), Conditions (drag fields here to add filter logic), and Sort (a dropdown to choose how results are ordered). Click the Result button at the bottom to run the report.
- Right panel - Results. Displays the report output as a table once Result is clicked. Results can be exported from here as a CSV file.

Advanced Reports

An Advanced Report gives technically proficient users direct access to the XPressEntry database through a custom SQL query editor. Rather than dragging and dropping fields, the user writes a SELECT statement directly against the available database views. This makes Advanced Reports significantly more flexible - they can join multiple views, perform aggregations, apply complex conditional logic, and return precisely the columns and structure needed for a specific use case.

Advanced Reports are best suited for custom integrations, compliance exports with specific formatting requirements, or any scenario where the drag-and-drop approach of a Dynamic Report cannot produce the exact output needed.

Advanced Report Interface

The Advanced Report editor is divided into two panels:

- Left panel - Tables and Filters. Lists all the available database views for reference (e.g., badge_activities_view, badges_view, doors_view, event_activities_view). Click the arrow next to any view name to expand it and see its column names. Below the Tables list is a Filters section with a Search field and a Date Filters checkbox, which can inject a standard date range filter into the query automatically.
- Right panel - SQL editor. A multi-line code editor where the user types a SQL query. The editor supports syntax highlighting. Use the Clear button to reset the editor, and Run Query to execute the statement. Results appear below the editor, and any errors are displayed in an Error panel directly beneath the query.

Creating an Advanced Report

1. Click the **Reports** tab in the left navigation panel, then click the **Add** (+) icon and select **Advanced Report**.
2. Enter a report title in the **Add** Report Title field at the top left.
3. Use the Tables panel on the left to browse available views and their column names. Click the arrow next to a view to expand it and confirm the exact column names before writing the query.
4. Type the SELECT statement into the SQL Editor on the right. Only SELECT statements are permitted - INSERT, UPDATE, DELETE, and DDL commands are blocked. See Example Queries below for working examples using the badge_activities_view.
5. Optionally, check the **Date Filters** checkbox in the Filters panel to enable a date range input that will be applied to the query automatically when it is run.
6. Click **Run Query** to execute the statement. Results appear below the editor. If there is an error in the query, such as an invalid column name, an Error panel will appear beneath the editor with the full SQL Server error message to help diagnose the issue.
7. Once the query runs successfully, click the save icon to store the report for future use.

Example Queries

The following queries use the actual column names from the badge_activities_view:

Example 1 - All badge activity for a date range

```
SELECT
    timestamp,
    user_name,
    badge_no,
    door_id,
    company,
    processed
FROM badge_activities_view
WHERE timestamp >= '2026-04-01'
```

```
  AND timestamp <  '2026-05-01'
ORDER BY timestamp DESC
```

Example 2 - Denied entries grouped by person

```
SELECT
    user_name,
    badge_no,
    company,
    COUNT(*) AS denied_count
FROM badge_activities_view
WHERE processed = 0
  AND timestamp >= '2026-04-01'
  AND timestamp <  '2026-05-01'
GROUP BY user_name, badge_no, company
ORDER BY denied_count DESC
```

Example 3 - Daily scan count per door, joined with door names

```
SELECT
    CAST(b.timestamp AS DATE) AS scan_date,
    d.name                 AS door_name,
    COUNT(DISTINCT b.badge_no) AS unique_badges,
    COUNT(*)                AS total_scans
FROM badge_activities_view b
JOIN doors_view d ON d.id = b.door_id
WHERE b.processed = 1
  AND b.timestamp >= '2026-04-01'
  AND b.timestamp <  '2026-05-01'
GROUP BY CAST(b.timestamp AS DATE), d.name
ORDER BY scan_date, door_name
```

Note: Advanced Reports require familiarity with SQL and knowledge of the XPressEntry database schema. Always expand the view in the Tables panel to confirm exact column names before writing a query, as column names differ from the labels shown in the Dynamic Report interface. Contact Telaeris support at (858) 627-9700 or helpdesk@telaeris.com if you need assistance with query construction or schema documentation.

Choosing the Right Report Type

Use the table below to determine which report type fits the user's needs:

Consideration	Dynamic Report	Advanced Report
Query method	Visual table and column selector	Custom SQL query

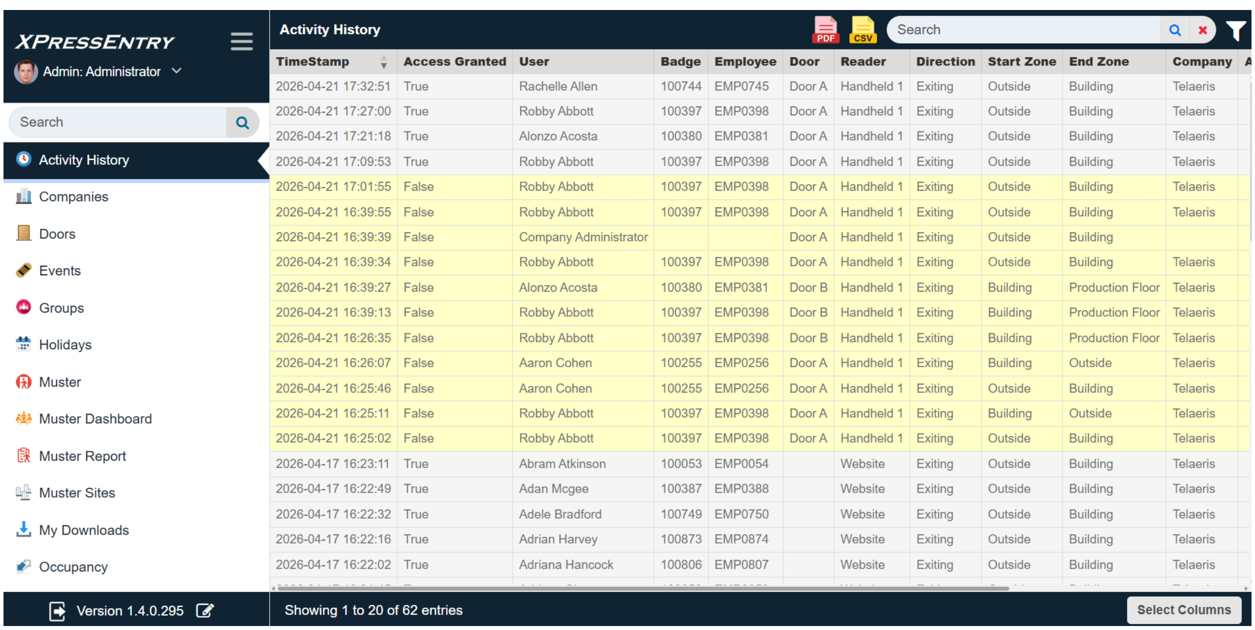
Technical skill required	None — no coding required	SQL knowledge required
Filtering	Visual filter panel with dropdowns and input fields	SQL WHERE clause, with optional user-facing filter parameters
Flexibility	Limited to available table/column combinations	Full SQL flexibility: joins, aggregations, subqueries
Best for	Routine operational reports run by security or HR staff	Custom integrations, compliance exports, or complex multi-table queries

Activity History

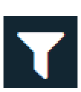
The Activity History tab provides a searchable, filterable log of every badge scan across all connected handheld readers. It is the primary tool for reviewing historical access events.

Accessing Activity History

1. In the left-hand navigation panel, click Activity History.
2. The log will display the most recent scan activity by default, sorted with the newest events at the top.

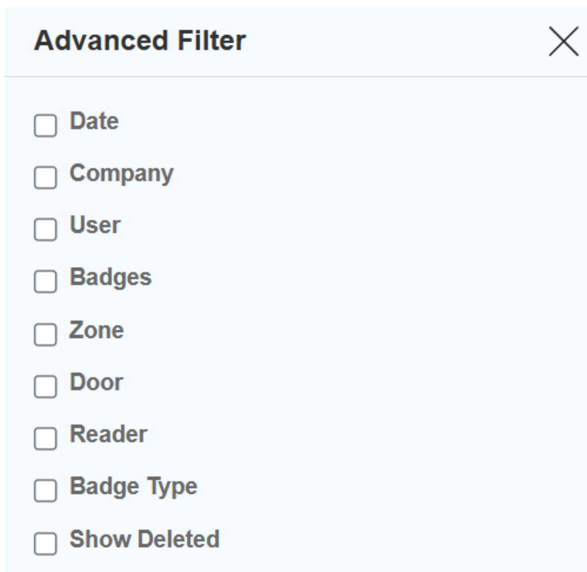


Filtering Activity History



Use the filter controls at the top of the Activity History view to narrow results:

- Date - Set a start and end date to view events within a specific window.
- Company - Filter results to activity from a specific company or contractor organization.
- User - Search by employee name to view events for a specific individual.
- Badges - Filter by badge number to view all scan events associated with a specific credential.
- Zone - Narrow results to activity recorded within a specific zone or area of the facility.
- Door - Filter by a specific door or gate to view all scans at that entry point.
- Reader - Filter by a specific handheld reader device.
- Badge Type - Filter by credential type to view activity for a particular class of badge.
- Show Deleted - Include records for users or badges that have since been removed from the system.



Note: Filters can be combined. For example, the user can filter by a specific door and a specific date range simultaneously to review all scans at a given entrance over the past week.

Exporting Activity Data

Activity History data can be exported as a CSV file for use in external applications such as Microsoft Excel, payroll systems, or compliance reporting tools.

1. Navigate to the **Activity History** tab and apply any desired filters.
2. Click the CSV icon or PDF icon in the toolbar at the top right of the screen.
3. The file will download immediately. Open it in Excel or any compatible application.

Note: If a report takes a while to generate due to a large data set, the Web Console will offer an option to email the report when ready rather than waiting for an immediate download.

Best Practices

- Schedule reports to run overnight - Configure daily reports to run in the early morning hours so they are ready in administrators' inboxes at the start of the workday.
- Use date range filters before exporting - Applying filters before downloading a CSV reduces file size and makes the exported data easier to work with.
- Configure a dedicated report mailbox - Sending scheduled reports to a shared mailbox (e.g., security-reports@yourcompany.com) ensures reports are accessible to the full security team and are not lost if an individual's inbox is full.
- Monitor reader status daily - Review the Readers tab at the start of each shift to confirm all handheld devices are online and synced before scanning begins.
- Retain activity exports for compliance - For sites with mandatory training or regulatory compliance requirements, export and archive Activity History CSVs on a regular schedule. Reports stored on the Web Console are accessible at any time but maintaining local archives provides an additional backup.
- Test SMTP configuration after any email server changes - If the organization updates its mail server settings, use the Test Email function in the SMTP settings to confirm reports will continue to deliver successfully.

Troubleshooting

Reports Tab Not Visible

- Confirm that the user role has permission to view Reports. Navigate to Roles in the Web Console to review and update role permissions.

Scheduled Reports Not Being Delivered

- Verify that SMTP settings are correctly configured and that a test email is sent successfully.
- Confirm that the report is set to Active in its settings.
- Check that the recipient email addresses are entered correctly, with no extra spaces or typos.
- Check the spam or junk folder if emails are not appearing in the inbox.

Activity History Showing No Results

- Confirm that the date range filter is set correctly. A very narrow date window (e.g., a single hour) may return no results if no scans occurred during that period.

- Check that the correct door or reader is selected in the filter, or clear all filters to return all events.
- If handheld readers were offline during the period in question, scans may not yet have synced. Wait for the device to reconnect and sync, then refresh the Activity History view.

CSV Export Is Empty or Incomplete

- Apply filters in Activity History before exporting to confirm there is data in the view.
- If the export is unexpectedly cut short, the dataset may be very large. Try narrowing the date range and exporting in smaller segments.