

LaunchPointUser Guide ~ On Premises

- ❖ Provides general information about system features.
- ❖ User instructions for Wizards, Viewers, and Configuration Editors.
- ❖ Glossary of Terms



LaunchPoint User Guide

On Premises

Information in this document is subject to change without notice. Therefore, no claims are made as to the accuracy or completeness of this document.

Galaxy Control Systems makes no claims on the requirements or limitations of software or devices of 3rd Party Manufacturers. Every effort is made to include all known requirements and capabilities as they relate to System Galaxy. Information herein may not supersede requirements of 3rd party manufacturers.

Second Edition • 2020

Copyright (c) 2020 • Galaxy Control Systems • All rights reserved

(Revision 2.0)

No part of this document may be reproduced, copied, adapted, or transmitted, in any form or by any means, electronic or mechanical, for any purpose, without the express written consent of Galaxy Control Systems. Copyright protection claims include all forms and matters of copyrighted material and information, including but not limited to, material generated from the software programs, which are displayed on the screen such as icons, look and feel, etc.

TRADEMARKS

VMS System: LENSEC®, Perspective VMS®, or PVMS™ are trademarks, or registered trademarks, of LENSEC or Progressive Systems, LLC. Other VMS Solutions are registered trademarks of their respective owners.

Badging Solution: idProducer may be a trademark or registered trademark of SpecsID or their owner in the US, Canada, and/or other countries.

SCOPE & NOTICES

This guide covers known requirements and instructions to configure and operate LaunchPoint web client as a cloud-based product.

For 3rd Party integrations, such as the VMS and Badging Solutions, always consult the appropriate *LaunchPoint Integration Guide*, as well as *3rd Party Manufacturer's documentation* for system and requirements and capabilities as they relate to the applicable product (i.e. OS, install/set up, speed, bandwidths, peripheral device models and features, codecs, specifications, printer specifications, etc.).

The availability/compatibility/functionality* of features and peripheral devices (i.e. cameras, printers, etc.), are determined by *product licensing*, 3rd Party drivers and API/Plug-ins, and the 3rd Party Manufacturer's product development. These may change without notice. Contact your authorized LaunchPoint Integrator for questions.

Galaxy Control Systems

www.galaxysys.com

www.concierge.galaxysys.com

Table of Contents ...

- Getting Started with LaunchPoint** 12
 - Features Supported 12
 - FEATURES 12
 - The editor includes the following 14
 - What's New? 26
 - New Features & Functions 26
 - New Features & Functions 27
- Administrative Settings** 30
 - FEATURED TOPICS 30
 - Administrative Settings 30
 - FEATURED TOPICS 30
 - Camera Group Settings 31
 - Create a User-Camera Group 31
 - OTHER OPTIONS 34
 - Add Cameras to a Camera Group 35
 - REQUIREMENT 35
 - STEPS 35
 - OTHER OPTIONS 37
 - Remove Cameras from a Camera Group 37
 - OTHER OPTIONS 40
 - Delete a Camera Group 40
 - OTHER OPTIONS 43
 - Elevator Floor Group Mapping 43
 - Elevator Floor Group Mapping (admin only) 44
 - REQUIRED HARDWARE SETUP 44
 - STEPS 44
 - User Login Multi-Factor Authentication 47
 - FEATURED TOPICS 47
 - About Multi-Factor Authentication (MFA) 47
 - PREREQUISITES AND NOTES 47
 - Update User Contact Information (MFA) 48
 - STEPS 48
 - User's First-Time Logon 49
 - Multi-factor User Login 52
 - FEATURED TOPICS 53
 - Overview and Prerequisites 53
 - PREREQUISITES AND NOTES 53
 - HOW TO OPEN THE MULTI-FACTOR SETTINGS 53
 - Using the Multi-Factor Authentication 54
 - Change Multi-Factor Authentication Settings 56

LaunchPoint Wizards	60
Featured Wizards	60
OVERVIEW: ABOUT WIZARDS	60
Prerequisites and Notes ...	61
Navigation Controls and Buttons ...	61
In the Add Cardholder Wizard, you can enter the following information ...	61
Prerequisites and Notes	62
Navigation Controls and Buttons ...	62
In the Add Card Wizard, you can enter the following information ...	63
Prerequisites and Notes	63
Navigation Controls and Buttons ...	63
In the Add Access Group Wizard, you can enter the following information ...	64
Prerequisites and Notes	64
Navigation Controls and Buttons ...	65
In the Add Time Schedule Wizard, you can enter the following information ...	65
Add Cardholder Wizard	65
featured topics	65
See Related Topics	66
About Enrolling a New Cardholder	66
PREREQUISITES & NOTES	66
From the Dashboard:	67
From the Cardholder List screen:	67
Adding a Cardholder	69
REQUIREMENTS	69
OTHER TIPS	70
NEXT : Do one of the following things to proceed ...	71
NOTES	72
Adding Additional Information	73
NEXT : Do one of the following things to proceed ...	74
NOTES	74
Adding Data in Fields 5 - 50	75
NOTES	76
Adding a Photograph	76
NOTES	78
Access Card Data	79
IMPORTANT	80
Choosing an Access Location	81
IMPORTANT NOTES	82
Assign Access Permissions (per Loop)	83
See Related Topics	84
Adding a Card	84
See Cardholder Enrollment Topics	85

See Other Related Topics	85
Add Access Group Wizard	85
featured topics	85
See Related Topics	85
About the Access Group Wizard	85
PREREQUISITES & NOTES	86
OPEN THE WIZARD	86
ADDING AN ACCESS GROUP	88
See Related Topics	89
STEPS	89
MODIFYING OR DELETING AN ACCESS GROUP	92
See Related Topics	93
Add Time Schedules Wizard	93
FEATURED TOPICS	93
See Related Topics	93
About Time Schedules	93
TERMS:	93
Access is granted if all these things are true	95
Access is denied if any of the following things are true	95
OPEN THE SCHEDULES WIZARD	95
ADDING A TIME SCHEDULE	97
See Related Topics	98
LaunchPoint Features	100
FeatureS by Category	100
Cardholders Search & Enroll	101
Using the Search Panel	101
How the Search Panel Works	101
PREREQUISITES	102
How to Control Search Results	102
INCLUSIVE MATCH	102
EXAMPLES	103
How to Open the Search Panel	104
Using the Search Panel	105
SEARCHING BY NAME CRITERIA	105
Editing Cardholders	106
FEATURED TOPICS	106
About the Cardholder Editor	107
PREREQUISITES AND NOTES	107
Supported Functionality	108
Buttons and Controls	109
EDITOR BUTTONS - TOP OF SCREEN	109
CARDHOLDER INFORMATION - TOP SECTION	109

CARD/BADGE SETTINGS - MID SECTION	109
Fields in the Cardholder Editor	110
How to Find a Cardholder	110
Edit an existing Cardholder or Card	113
Access & Schedules	121
Editing Access Groups	121
FEATURED TOPICS	121
About Editing Access Groups	122
PREREQUISITES TO EDITING ACCESS GROUPS	122
TERMS	122
How to Open Access Group Editor	126
How to Edit Access Groups	128
STEPS	128
Next Steps	129
Editing Time Schedules	129
FEATURED TOPICS	129
About Editing Schedules	130
PREREQUISITES & NOTES	130
In the Time Schedule Editor, you can change the following things	132
Prerequisites and Notes	133
Navigation Controls and Buttons	134
In the Add Time Schedule Wizard, you can enter the following information	134
How to Open Time Schedules Editor	134
How to Edit Time Schedules	137
OPEN THE EDITOR	137
STEPS	139
OTHER BUTTONS	141
Configure Holiday Day Types (Special Days/Holidays)	141
OPEN THE SCHEDULE EDITOR	141
STEPS	143
Next Steps	145
One Time Scheduled Action	145
FEATURED TOPICS	145
Create a Scheduled Action	146
RULES OF OPERATION	146
PREREQUISITES	146
OPEN THE ONE-TIME SCHEDULE PAGE	146
CREATE A SCHEDULED ACTION	147
Action Frequency (Behaviors droplist)	147
Device Actions	147
STEPS	147
Delete a Scheduled Action	148

STEPS	149
Remove multiple Scheduled Actions	150
STEPS	150
	151
Hardware & Diagnostics	151
Access Readers	151
FEATURED TOPICS	151
Configure Readers	152
RULES OF OPERATION	152
PREREQUISITES AND NOTES	152
OPEN THE READER PAGE	152
STEPS	153
Send User Commands to Door	154
STEPS	154
View Reader Activity History	155
STEPS	155
MANAGE PAGE SIZES	156
Export Activity History Report	157
STEPS	157
Elevator Readers	158
FEATURED TOPICS	158
About the Elevators Page	159
RULES OF OPERATION	159
PREREQUISITES AND NOTES	159
OPEN THE ELEVATORS PAGE	160
How to View Video from Elevators Page	160
STEPS	161
Send User Commands to Relay (Floor)	164
STEPS	164
PULSE FLOOR	165
EARLY ON / EARLY OFF	166
CANCEL EARLY ON / CANCEL EARLY OFF	167
REFRESH ELEVATOR STATUS	167
View Reader Activity History	167
STEPS	168
MANAGE PAGE SIZES	168
Export Activity History Report	169
STEPS	169
Loop Diagnostics	171
FEATURE TOPICS	171
Loop Diagnostics Overview & Prerequisites	171
PREREQUISITES & NOTES	172

How to Open the Diagnostics Page	172
Send a Diagnostic Command	173
STEPS	173
RESULT OF SENDING DIAGNOSTIC COMMANDS	175
Available User Commands	176
GET CARD COUNT	176
Things you can do to troubleshoot this situation	176
GET HARDWARE INFORMATION	177
Fields of Interest	177
GET LOGGING INFORMATION	178
Fields of Interest	178
SEND CRISIS MODE COMMANDS	178
Fields of Interest	179
PING CONTROLLERS	180
Fields of Interest	180
Live Events	180
FEATURED Topics	181
Event Overview	181
FEATURED TOPICS	181
Overview of Operation	181
Prerequisites & Notes	182
The Process of Operating the Events Page	182
In the Live Events page, an user can do the following	184
Event Types	187
OPEN THE EVENT VIEWER	187
HOW TO VIEW LIVE EVENTS	188
Monitoring Events	188
FEATURED TOPICS	189
Configure Events (Settings)	189
PREREQUISITES & NOTES	189
OPEN THE EVENTS PAGE	189
OPEN THE SETTINGS WINDOW	190
CONFIGURE EVENT SETTINGS	190
STEPS	190
DEVICE DROPLISTS	191
EVENT TYPE DROPLISTS	191
EVENT MESSAGES	192
Monitoring Live Events	192
STEPS	193
SETTING THE 'NUMBER OF EVENTS' PER PAGE	193
OPERATOR COMMANDS	194

There are two places to find user commands ...	194
STEPS	195
LIST OF COMMANDS IN MENU	195
Alarms & Crisis Mode	196
Handling Alarms	196
FEATURED TOPICS	196
About Alarm Events	196
Configure Alarms (Activation Settings)	197
PREREQUISITES & NOTES	197
OPEN THE EVENTS PAGE	198
OPEN THE ALARM SETTINGS WINDOW	198
ALARM SETTINGS	198
STEPS	199
"TYPE" DROPLIST	199
"DEVICE" DROPLIST	199
"EVENTS" DROPLIST	200
EVENT MESSAGES	200
Monitoring Alarm Events	201
STEPS	201
ACKNOWLEDGE OPERATOR FEEDBACK	202
OPERATOR COMMANDS	203
STEPS	203
COMMAND BUTTONS	203
Activating Crisis Mode	204
FEATURED TOPICS	204
Crisis Mode Overview & Prerequisites	204
PREREQUISITES & NOTES	204
The following caveats apply ...	205
Activating Crisis Mode Button (system-wide)	207
PREREQUISITES & NOTES	207
OPEN CRISIS MODE SETTINGS	207
STEPS	207
RESULT OF ACTIVATING CRISIS MODE	208
Deactivating Crisis Mode (system-wide)	209
STEPS	209
VALID CRISIS MODE EXCEPTIONS	210
Activate or Reset Crisis Mode from Loop Diagnostics	211
OPEN THE DIAGNOSTICS PAGE	211
STEPS	213
VALID CRISIS MODE EXCEPTIONS	214
Video & Photo Viewers	215
Photo Verification	215

FEATURE TOPICS	215
Photo Verification - Overview and Prerequisites	215
RULES OF OPERATION	216
Photo Verification Screen	216
PREREQUISITES & NOTES	216
Always Active / Live Photo Updates	217
How to open the Photo Verification screen	217
How to View Photo Verification	218
Viewing VMS Video	221
FEATURED TOPICS	221
See Related Topics	221
Overview & Prerequisites	222
PREREQUISITES & NOTES	222
How to View Video	222
HOW TO OPEN THE VMS SCREEN	222
STEPS	223
See Related Topics	228
Reports	228
Reader Activity History	228
FEATURED TOPICS	228
Overview and Prerequisites	228
PREREQUISITES AND NOTES	229
Pull the Reader Activity History	229
Viewing Video from the Reader Activity History	231
Who's In Report	233
FEATURED TOPICS	233
Overview and Prerequisites	234
PREREQUISITES AND NOTES	234
TERMS	234
RULES OF OPERATION	234
OPEN THE WHO'S IN REPORT	234
Pulling Who's In Report by Area	235
There are 2 ways to pull the Who's In Report	235
STEPS	236
Pulling Who's In Report by Cardholder	236
STEPS	237
Custom Report Scheduler	238
FEATURED TOPICS	238
Rules and Requirements	238
How to Create a New Scheduled Report	239
STEP 1 • HOW TO OPEN A SCHEDULED REPORT	240
STEP 2 • CHOOSE "NEW" REPORT	241

STEP 3 • SELECT REPORT FILTER/GROUP CRITERIA	241
STEP 4 • ADD EMAIL CRITERIA FOR THE REPORT	242
STEP 5 • CHOOSE THE REPORT DURATION (Past # Hours)	243
STEP 6 • CHOOSE THE REPORT CYCLE (Scheduled vs On-Demand)	244
STEP 7 • SAVE YOUR REPORT	246
List of Available Scheduled Reports	247

Getting Started with LaunchPoint

LaunchPoint is a web-based *Access Control & Security Management Software* that offers access monitoring, cardholder enrollment, and management of user privileges - through user-friendly Editors, Viewers, and Reports.

Features Supported

The main **operational features** allow a user to perform a variety of tasks such as search, program or edit, monitor, view, and report - as well as control hardware, send user commands, manage crisis mode, and more.

There are also **administrative features** that support admin-level tasks like create Dual-Authentication Logins, manage user permissions, create VMS Camera Groups and Elevator Floor Groups, and change the LaunchPoint window appearance.

- **Edit Cardholders** - including add Photos, assign Access Permissions, assign, preview and print badges.
- **Configure Access** - Access Groups (permissions), Time Schedules, and Special Days.
- **Control Hardware** (doors & elevator floors) - includes viewing/exporting Activity History Reports.
- **Manage Crisis Mode** - for all or selected hardware.
- **Monitor and manage Live Events & Alarm Events** - for all or hardware (selectable).
- **Send User Commands** in various situations.
- **View/print/export Reports** - Activity History and Who's In Reports
- **Administer User Permissions** - including Dual-Authentication login.
- **Administer Camera Group mapping**
- **Administer Elevator Floor Group mapping**
- **Administer Scheduled Reports**
- **Administer App Settings** - including dashboard appearance

[See Help for Features](#)

FEATURES

The LaunchPoint Cloud App supports these major features and functionality.

Managing Cardholders Information

The following screens are related to editing cardholders ...

Search Panel / Cardholder List

Cardholder Editor

Cardholder List / Search Panel

The **Cardholder List / Cardholder Search Panel** allows the user to search for a cardholder based on selected criteria and see the results of the search displayed in the Cardholder List.

- **Search for Cardholders** by specified criteria such as name, department, etc. (search criteria list is configurable)
- Use the **A - Z Index** to jump to the section of cardholder population appearing at that position on the Cardholder List.
- View the **Cardholder List** of enrolled population that meets the search criteria.
- Open the **Cardholder Editor** for an individual cardholder record
- Launch the **Add Cardholder Wizard** if you determine your cardholder has not been enrolled.
- **Synchronize badge templates** (updates the badge droplist)



Cardholder List / Search Panel
(hover/tap to open/close thumbnail)



Cardholder List

See [Features](#) | [See Search Panel Topic](#) | [Go to Cardholder Editor](#)

Cardholder Editor

The **Cardholder Editor** allows the user to change information for an existing cardholder record.

The editor includes the following ...

- previewing or printing ID Badges; assigning badge templates
- modifying, deleting or adding more **access cards**,
- updating **access permissions** and **locations**
- updating any discretionary information, such as photographs, personnel information, card expiration,
- synchronizing badge templates (updates the badge droplist)
- completing any information that was not done in the wizard screens
- disabling a card or cardholder without deleting the record (to preserve current history reporting)



Cardholder List / Search
(hover/tap to open/close thumbnail)



Cardholder Editor
(hover/tap to open/close thumbnail)

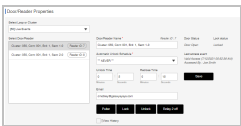
See [Features](#) | [Search Panel](#) | [Cardholder Editor](#)

Hardware Control for Doors and Elevators

Door Control

The **Door Control** features allows the system user to issue commands to the doors.

- Unlock doors
- Lock doors
- Pulse doors (momentary unlock)
- Relay-2 Off
- Also configure the unlock and reclose times for the door hardware



Reader/Door Screen
(hover/tap to open/close thumbnail)

See [Features](#) | [Go to Readers](#)

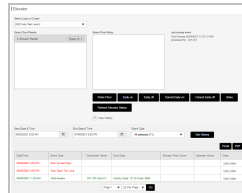
Elevator Floor Control

The **Floor Control** features allows the system user to issue commands to the elevator floors (relays).

- Pulse Floor (momentary pulse)
- Early On / Early Off
- Cancel Early On / Cancel Early Off
- View Video
- Refresh Elevator Status



Elevator Floor Screen
(hover/tap to open/close thumbnail)



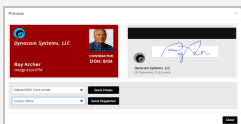
Elevator Screen
(hover/tap to open/close thumbnail)

See [Features](#) | [Go to Elevators](#)

Preview and Printing Badge Templates

The **Badge** feature supports the following things ...

- synchronizing badge templates (updates the badge template droplists)
- previewing badges (Cardholder Editor)
- printing badges (Cardholder Editor)
- removing or changing badges (Cardholder Editor)



Badge Print/Preview window
(hover/tap to open/close thumbnail)

See [Features](#) | [Cardholder Editor](#)

Managing Custom Access Privileges

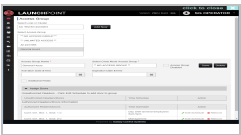
LaunchPoint allows you to manage **Access Privileges** at the individual cardholder or on the global system level.

1. **Change access permissions for one person to be different from other people in the same group:**
You can add a second (additional) access group to the person while keeping the existing group assigned. Or you can remove the existing access group and add a different access group to the card. In this way, only the individual cardholder is affected. A third possible option is to issue a separate card with the additional access group. LaunchPoint can support multiple access groups on one card or support multiple cards on the same cardholder with different cardholder access.
2. **Change which doors are authorized vs. unauthorized to an access group:**
You can add or remove the doors in an access group. This will impact all cardholders that are assigned to the modified access group. Other access groups are not affected.
3. **Change which schedules are assigned to an access group:**
You can change which schedule is assigned to the door(s) in an access group. You can change the schedule of an individual door, or multiple doors, or all doors. This will impact every cardholder that has the assigned access group. Other access groups and cardholders are not affected.
4. **Change the time and/or day that cardholders have access to a specific door:**
You can edit the time schedule; assuming you have only used this schedule on the door in question.
5. Be sure you understand where schedules are applied. If you change a schedule that is used/applied to multiple access group which doors "are in the same group" or "in other access groups are using the schedule you intend to change. Remember you can always make a new custom schedule and swap it out on the doors you need to change. Updates to a time schedule will affect any door in every access group that is linked to it. If you are sure you want to change all the doors, then change the schedule. If you have some doors that still need the schedule to remain as-is, then make a new schedule and assign it only to the doors you need.

Creating Custom Access Groups

The **Access Group** feature supports the following ...

- assigning doors and time schedules to each access group
- assigning a crisis mode schedule to each access group
- assigning activation and deactivation dates to an access group
- disabling an access group



Access Group Editor
(hover/tap to open/close thumbnail)

See [Features](#) | [Access Group Editor](#)

Creating Custom Time Schedules

The **Time Schedule** feature supports the following ...

- creating custom time schedules
- assigning holidays or special days



Time Schedules Editor
(hover/tap to open/close thumbnail)

See [Features](#) | [Schedules Editor](#)

Printing System Reports

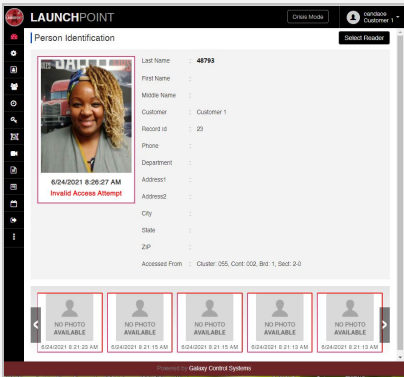
The **Reporting** features support the following ...

- [Cardholder List](#) (Scheduler)
- [Who's In](#) (real-time snapshot)
- [Reader Activity Report](#) (configurable)

See [Features](#)

Photo Verification / Identification

The **Photo Verification** feature allows the user to view the photograph of the cardholder (photo identity). This adds an extra measure of security to access control. A human user will compare the photograph with the person's face who is entering the facility.

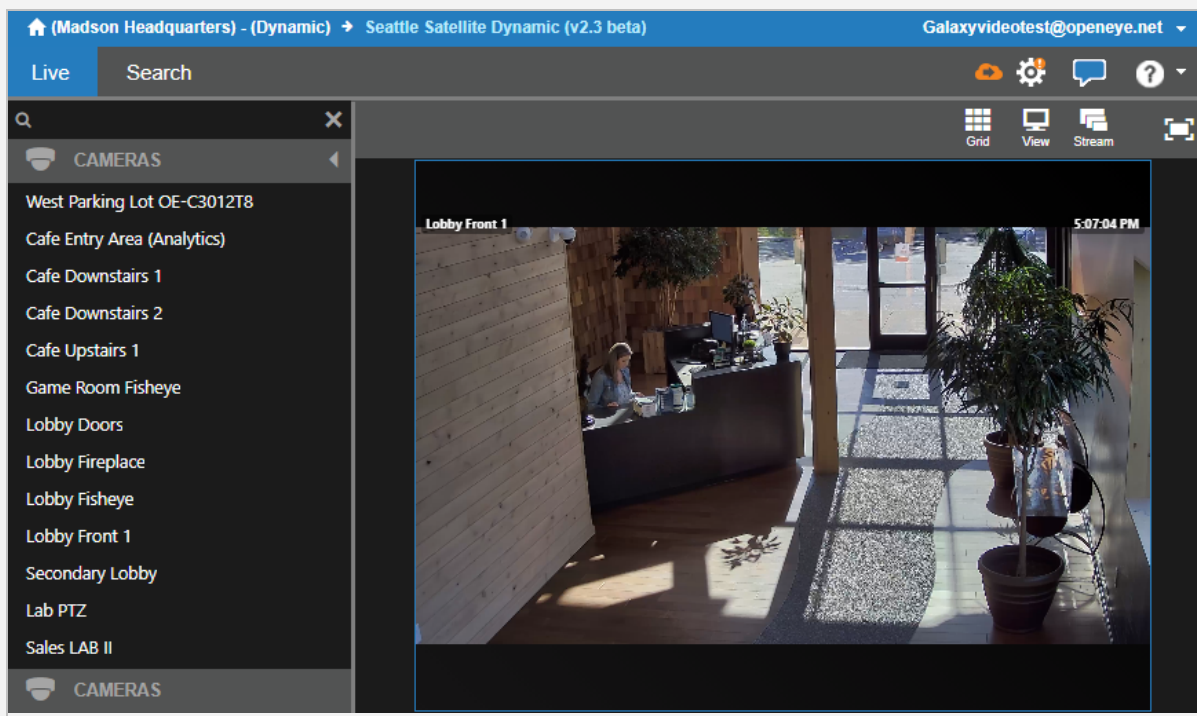


See [Features](#) | [Photo ID](#)

Viewing VMS Video

The **VMS Video** feature supports the following ...

- logging into the VMS system
- selecting a camera to view video from
- viewing live or recorded video through the VMS Viewer Interface (i.e. Lensec)



See [Features](#) | [View VMS](#)

WORKSPACE / USER INTERFACE

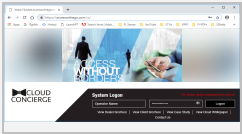
The LaunchPoint user interface (UI) is designed with user-intuitive, task-oriented design, which helps the user perform the task.

SIGN-IN TO LAUNCHPOINT

When the LaunchPoint web app opens in a browser window, the user can sign-in with a valid user login. The user login consists of a login name and password.

- Enter the **Log-in Name**.
- Enter the **Password** (case sensitive).
- Click the sign-in button and the Dashboard should appear.

If the user is inactive too long, the session will expire and the user must sign-in again to resume working.



user Login Screen
(hover/tap to open/close thumbnail)

See [HOME](#)

THE START PAGE - DASHBOARD

When the user signs in, LaunchPoint automatically opens the Dashboard

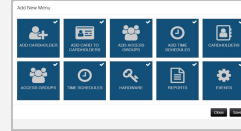
1. the **Wizard Tiles** (clicking these will open the appropriate Wizard)
2. the **Configure Tiles** (clicking these will open the appropriate Editor screen)

The user can control (show/hide) which Tiles are visible.

The user can always get back to the Dashboard by clicking the **Dashboard Icon** on the side menu.



LaunchPoint Dashboard
(hover/tap to open/close thumbnail)



Set Up which Dashboard Tiles are visible.
(hover/tap to open/close thumbnail)

See [Settings](#) | [HOME](#)

MAIN SECTIONS OF THE UI

The main sections of the LaunchPoint UI are as follows ...

1. the **web page Header** - shows the logo and user name who is signed-in.
2. the **side Menu** - includes a expand/collapse button to show and hide Menu Titles.
3. the **Quick-Launch Dashboard** - includes a tile/icon for each feature (wizard or editor).
4. the **Editors and Wizards** - UI screens where information is entered into the system.
5. the **Cardholder List** - shows the list-view of filtered cardholder records, based on search criteria.
6. **Search Panel** - provides search criteria fields to retrieve cardholder records.
7. the **Report or Event Grids** - provides date-range fields for querying events.
8. the **Photo Verification** window - provides a window to view cardholder photo
9. the **VMS Viewer** - provides portal to the VMS API Plugin to launch the VMS viewer.
10. the **Door Control** screen - provides option to lock and unlock doors.



See [HOME](#)

User Interface Layout
(hover/tap to open/close thumbnail)

How the LaunchPoint UI Operates

The *Sidebar Menu* and *Dashboard Tiles* are the main method of navigating in LaunchPoint.

- **SIDEBAR MENU** - When the user signs in to LaunchPoint, the Sidebar Menu is displayed along the left margin of the window.
If user expands the menu width, the Menu Names are visible. If the user collapses the sidebar menu, only the menu icons are visible.
- **DASHBOARD TILES** - The tiles for each function are displayed on the Dashboard provided the administrator has not hidden them.
Hover over a tile to see its sub-menu. Click to choose which screen to open.

USING EDITOR SCREENS

When the user can open an Editor by clicking the related Tile on the Dashboard or Side Menu.

1. The Editors are task-oriented. Data fields are arranged in a logical top-down workflow - with related fields and dependent fields grouped together.
2. Required fields are outline in red and have a red asterisk beside them. These cannot be blank or unset.
3. Optional fields can be configured at the user discretion but the workplace policy may mandate optional fields be set.
4. Disabled/hidden fields are locked/grayed or not visible until the user has first chosen a dependent option or satisfied a condition. For example the access permissions cannot be assigned until a loop/cluster is chosen.

You can open an Editor screens from the sidebar menu or from the appropriate dashboard tile.

USING WIZARD SCREENS

The user can launch the Wizards by clicking the related Tile on the Dashboard.

Also a wizard can be launched by clicking the appropriate button in the screens.

- for example, in the Cardholder Editor, you can launch the Card Wizard by clicking the [Add Card] button.
- likewise, in the Cardholder Editor, you can launch the Cardholder Wizard by clicking the [Add New Cardholder] button.

How Wizard screens operate...

1. The Wizard steps the user through the screens in the proper order to complete the task.
2. Wizards will not advance or save the record until the required or mandatory fields are satisfied
3. User can skip optional / discretionary fields.
4. User can navigate back and forth between screens.
5. When the user saves the record, the Wizard may prompt the user to add another record.
6. After the record is saved, the record can be viewed or changed in the editor screens.

TABS, ACCORDIONS, SUB-SCREENS (Modals), ETC.

LaunchPoint screens group related fields and related buttons together.

Typical UI controls let the user navigate and manipulate the fields.

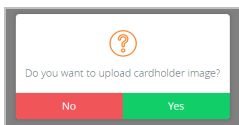
1. **Tabs** offer a stacked way to visit or cycle through groups of fields without leaving the main screen. Clicking a tab will show the related fields and had all other tabs.
2. **According controls** will show/hide or expand/collapse a section of the screen where related fields are grouped.
3. Some editors have **push buttons** that open sub-screens where more options are found.
4. Some UI functions use a set of fields to let the user to define the starting and ending date or time. This is found in the Schedules screen and any Screen where reports can be queried by start and stop dates.

5. Sub-screens, Models and messages pop open when a choice is made or button is pushed or trigger happens. User must close them to proceed.

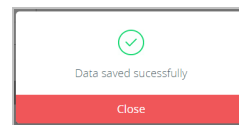
USER FEEDBACK MESSAGES, ERRORS, ETC.

LaunchPoint screens use colors, symbols and text to communicate errors or confirmations.

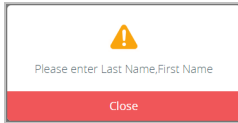
1. **CONFIRMATION DIALOGS** - prompt user to make a decision - such as to save or cancel.
2. **ERROR DIALOGS** - communicate a text message letting user know an action failed, is missing data, or has not met requirements. This often works in tandem with highlighted fields.
3. **INFORMATIONAL DIALOGS** - communicate a text message to let user know a fact or tip or notice that is related to the function being used.
4. **HIGHLIGHTED FIELDS** - typically red and bold outline is used to let the user know the field needs data.
5. **RED ASTERISK SYMBOL (*)** - the red asterisk is used to indicate that a field is mandatory or required. The app will not save the record or perform the action until the data is satisfied.
6. **ON-SCREEN CAPTIONS** - these text messages are static text that are always on the screen to instruct user how to use a field.
7. **FIELD LABELS** - there is a text label for every field and option on the screen that intuitively describes the purpose of the field.
8. **LOCKING AND UNLOCKING FIELDS** - some fields are locked until the user satisfies a piece of data or has saved a record. For example you cannot print a badge until you have assigned it and saved it to the cardholder. Some fields don't even appear until something has been selected or configured.



User Confirmation Needed
(hover/tap to open/close thumbnail)



User Action Successful
(hover/tap to open/close thumbnail)



Required Field is Empty
(hover/tap to open/close thumbnail)



Required Field is Wrong Value
(hover/tap to open/close thumbnail)

See [HOME](#)

What's New?

Click on the Release Dates to see the list of new features and enhancements made to each release of LaunchPoint.

NEW RELEASE - April 2024

These are the changes and features introduced with LaunchPoint - spring of 2024.

New Features & Functions

1. **UPDATE Dashboard Tiles** - the **Dashboard Tiles** have been updated to streamline and consolidate the features and improve usability.
2. **NEW Express Add - Cardholder Quick Enrollment Screen**: the **Express Add** feature provides the essential enrollment fields needed to enroll a cardholder all on the same screen (web page).
 - a. **Cardholder Information** - the user can add a Cardholder and the main photograph, personal data and other related settings.
 - b. **Add an Access Card** - the user can add the access card data
 - c. The user can assign a Badge Template, Access Card Data, and assign Access Location and Access Profile.
3. **UPDATE Photo Verification window** - will now keep a running history of events.
4. **UPDATE Scheduled Reports** - added custom report scheduler for 'Cardholder List by Client ID'.

NEW RELEASE - Spring 2021

These are the major features introduced into LaunchPoint - spring of 2021.

New Features & Functions

1. **Crisis Mode** - added ability to activate and reset Crisis Mode using the
 - a. **Crisis Mode Button** that displays in the *LaunchPoint webpage header*
 - b. **Crisis Mode Command** in the *Diagnostics* page.
2. **Hardware Diagnostics Page** - provides the ability to check controller status, warm and cold start panels, send operator commands, ping a controller, get the card count, and more.
3. **User Profile** - added a feature to prevent an individual operator (user) from deleting cards (administrative setting).
4. **Live Events page** - always opens in new browser tab:
 - a. added the ability to see real-time incoming events from the system hardware and activity.
 - b. added the ability to filter which *event types* and which *devices* you want to see events from.
 - c. added the ability to send *user commands* with a single-click from the "quick action" menu for incoming events.
 - d. added the ability to *view video* from a camera that is linked to a door/reader where an access card was presented or an incoming event was detected.
5. **Alarm Events** - in Live Events window:

- a. added Alarm Event (pop up modal) to Live Events page.
 - b. added support for Bosch Alarm panel alarm acknowledgment.
- 6. **Photo Verification window** - will now keep a running history of events.
- 7. **Who's In Report** - ability to run a who's in report directly in LaunchPoint (proper reader configuration set up by integrator required).
- 8. **Elevator Floor Relay Control** - configuration required.
 - a. ability to see floor relay status (on/off).
 - b. able to pulse floor relays.
 - c. able to select multiple relays at a time.
 - d. able to control floor schedules
 - e. able to view video from elevator floors
 - f. able to view activity report and export the report to xcel file format.
- 9. **Reader Properties** (door/reader)
 - a. added the ability to view activity report and export the report to xcel file format.
 - b. added email settings for door level alerts.
- 10. **VMS Systems** -
 - a. Hanwha Video Integration support added (WiseNet Sync).
 - b. Open Eye OWS integration support added.
- 11. **Reader Activity reports**
 - a. now allows for selecting all, one, or multiple readers.
 - b. added request to exit to reader activity reports.
- 12. **Cardholder Photo Upload**- added rotate option to photo upload.
- 13. **Scheduled Reports** - added custom report scheduler for Cardholder List by Client ID.

(-)

Administrative Settings

This topic covers the settings that are available in LaunchPoint.

FEATURED TOPICS

[Dashboard Layout Settings](#)

[Elevator Floor Group Mapping](#)

[Report Settings](#)

[User Logon - Multi-Factor Authentication](#)

[VMS Camera Group Mapping](#)

Administrative Settings

This topic covers the settings that are available in LaunchPoint.

FEATURED TOPICS

[Dashboard Layout Settings](#)

[Elevator Floor Group Mapping](#)

[Report Settings](#)

[User Logon - Multi-Factor Authentication](#)

[VMS Camera Group Mapping](#)

Camera Group Settings

This topic covers the system administrator's ability to map users to camera groups for the VMS system used by LaunchPoint.

The VMS Setting allows a *system administrator* to "map" *users* to *cameras* in the VMS system that are programmatically linked to readers in the LaunchPoint system. Once the Camera Group is created, the administrator can modify or delete it.

FEATURED TOPICS

[Create a Camera Group](#)

[Add Cameras to a Camera Group](#)

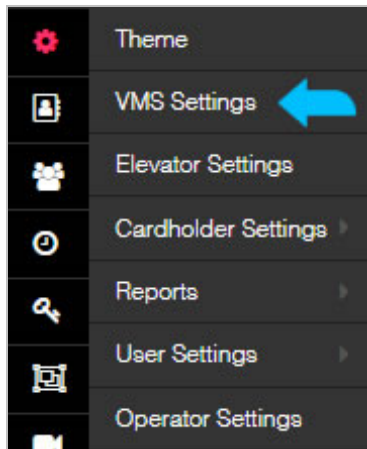
[Remove Cameras from a Camera Group](#)

[Delete a Camera Group](#)

Create a User-Camera Group

This section describes how to *Create A New Camera Group* by mapping one or more cameras to a user name.

1. Click on the **Settings** icon on the side menu and choose *VMS Settings*.



2. The *User Camera Mapping Page* will open.

Result: The page has 3 columns (User Select List, Camera Select List, and Mapped List of User-Camera Groups).

NOTE: The page has inclusive search fields at the top of each column.

(Inclusive search means if you enter "d" in the search field, it will include ever person with the letter D in their name - even if it doesn't start with D.)

User Camera Mapping

User - Select User

Search by User

AA9003YQP7
securitypursuit
IMPORT_SYSOP
cyber_swift
customer1
customer2
customer3
customer4
customer5
candace
Joe
Jeff
Mark

Camera - Select Camera

Search by Reader Search by Camera

Game Room Fisheye - (Cluster: 055, Cont: 001, Brd: 1, Sect: 1-0)
Lab PTZ - (Cluster: 055, Cont: 001, Brd: 1, Sect: 2-0)
Sales Lab - (Cluster: 055, Cont: 002, Brd: 1, Sect: 1-0)
Lobby Front 1 - (Cluster: 055, Cont: 002, Brd: 1, Sect: 2-0)
Secondary Lobby - (Cluster: 055, Cont: 003, Brd: 1, Sect: 1-0)
Lobby Doors - (Cluster: 055, Cont: 003, Brd: 1, Sect: 2-0)
Cafe Downstairs 1 - (In Elevator Reader)
Game Room Fisheye - (Reader 4 in home office)
Sales Lab - (B 5512 Point 1)
Lobby Doors - (B 5512 Point 2)
West Parking Lot OE-C3012T8 - (B 5512 Point 3)

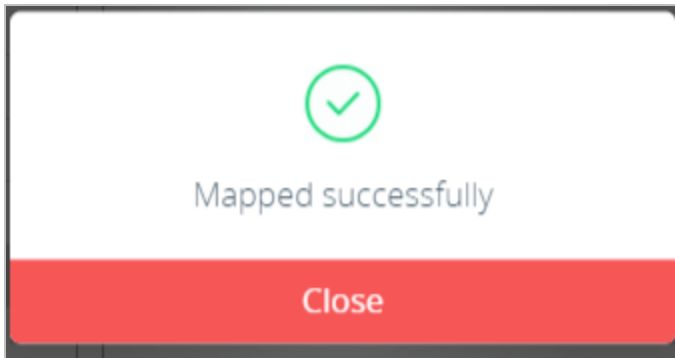
Mapped User - Camera List

Search by User Search by Reader

Search by Camera

AA9003YQP7	All selected (8)	<input type="button" value="Update"/>
customer1	All selected (11)	<input type="button" value="Update"/>
customer4	All selected (3)	<input type="button" value="Update"/>
candace	All selected (6)	<input type="button" value="Update"/>
Joe	All selected (6)	<input type="button" value="Update"/>
Jeff	All selected (11)	<input type="button" value="Update"/>
Mark	All selected (11)	<input type="button" value="Update"/>
Todd	All selected (11)	<input type="button" value="Update"/>

3. First, select (click) a **User Name** in the first column to begin creating the Camera Group.
[HINT: clicking the *user name* a second time will deselect it.]
4. Next, select (click) the individual **Cameras(readers)** from the second column to choose it for the group.
[HINT: you can click more than one camera to give the user access to multiple cameras (shown above).]
[HINT: to deselect a camera, click the camera a second time.]
5. Click the **Map** button to assign the group of cameras to the user.
6. Click Close on the User Confirmation message.
Result: This message confirms your Camera Group is created.



7. The new **User-Camera Group** is created and added to the Camera Groups list (3rd column).
[HINT: you can see the total number of cameras in the parentheses.]
[In our example four "(4)" cameras belong to the user named 'Customer 3'.]

Mapped User - Camera List

Search by User Search by Reader

Search by Camera

AA9003YQP7	All selected (8) ▼	Update
customer1	All selected (11) ▼	Update
customer3	All selected (4) ▼	Update
customer4	All selected (3) ▼	Update
candace	All selected (6) ▼	Update
Joe	All selected (6) ▼	Update
Jeff	All selected (11) ▼	Update
Mark	All selected (11) ▼	Update
...

8. You can close the page if you are finished or choose *Other Options*.

OTHER OPTIONS

- [Add Cameras to a Camera Group](#)
- [Remove Cameras from a Camera Group](#)
- [Delete a Camera Group](#)

Add Cameras to a Camera Group

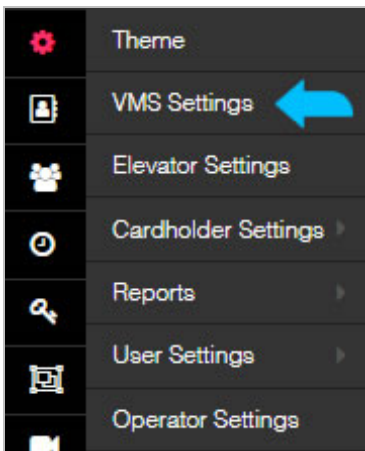
This section describes how to add more cameras to an existing User-Camera Group (a.k.a Camera Group).

REQUIREMENT

- The user's Camera Group must already be created.
- If you have not yet created the camera group, see [Creating Camera Groups](#).

STEPS

1. Click on the **Settings** icon on the side menu and choose *VMS Settings*.



2. The *User Camera Mapping Page* will open.

User Camera Mapping

User - Select User
Search by User

Camera - Select Camera
Search by Reader

Search by Camera

AA9003YQP7
securitypursuit
IMPORT_SYSOP
cyber_swift
customer1
customer2
customer3
customer4
customer5
candace
Joe
Jeff
Mark

Game Room Fisheye - (Cluster: 055, Cont: 001, Brd: 1, Sect: 1-0)
Lab PTZ - (Cluster: 055, Cont: 001, Brd: 1, Sect: 2-0)
Sales Lab - (Cluster: 055, Cont: 002, Brd: 1, Sect: 1-0)
Lobby Front 1 - (Cluster: 055, Cont: 002, Brd: 1, Sect: 2-0)
Secondary Lobby - (Cluster: 055, Cont: 003, Brd: 1, Sect: 1-0)
Lobby Doors - (Cluster: 055, Cont: 003, Brd: 1, Sect: 2-0)
Cafe Downstairs 1 - (In Elevator Reader)
Game Room Fisheye - (Reader 4 in home office)
Sales Lab - (B 5512 Point 1)
Lobby Doors - (B 5512 Point 2)
West Parking Lot OE-C3012T8 - (B 5512 Point 3)

Map

Mapped User - Camera List
Search by User

Search by Reader

Search by Camera

AA9003YQP7	All selected (8)	<input type="button" value="Update"/>
customer1	All selected (11)	<input type="button" value="Update"/>
customer4	All selected (3)	<input type="button" value="Update"/>
candace	All selected (6)	<input type="button" value="Update"/>
Joe	All selected (6)	<input type="button" value="Update"/>
Jeff	All selected (11)	<input type="button" value="Update"/>
Mark	All selected (11)	<input type="button" value="Update"/>
Todd	All selected (11)	<input type="button" value="Update"/>

- First, select (click) the **User Name** in the first column that you want to add cameras to.

[HINT: If you made a camera group for a user (Customer 3) and you want to add more cameras, then you will select the same username again in the first column. You might think you are creating a new group, but if the user already has a group, this will just add cameras to the existing group's camera list.]

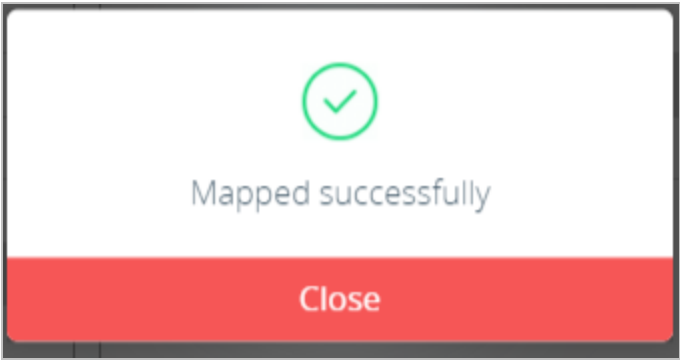
- Next, select (click) the individual **Cameras(readers)** from the second column that you want to add to the existing camera group.

[HINT: you can click more than one camera to give the user access to multiple cameras (shown above).]

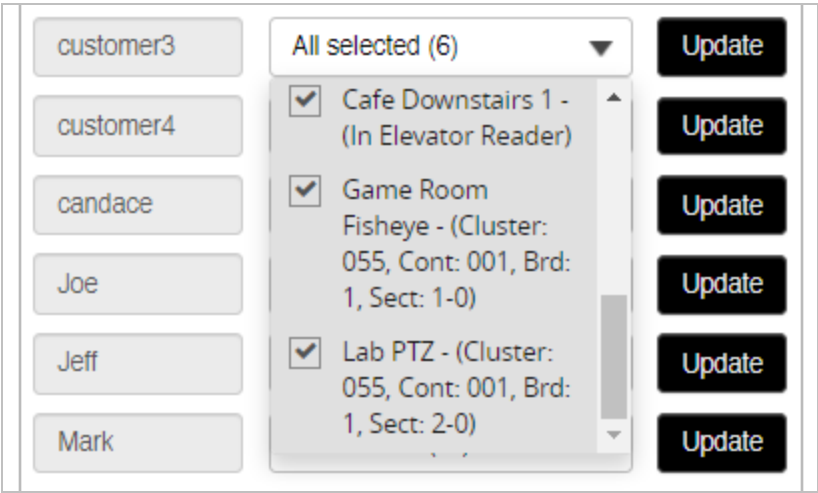
[HINT: to deselect a camera, click the camera a second time.]

- Click the **Map** button to assign the group of cameras to the user.
- Click Close on the User Confirmation message.

Result: This message confirms your Camera Group is created.



7. The existing **User-Camera Group** is updated and the additional cameras are added to the Camera Groups list (3rd column).
[HINT: you can see the total number of cameras will increase in the parentheses. You can see new cameras in the list.]



8. You can close the page if you are finished or choose *Other Options*.

OTHER OPTIONS

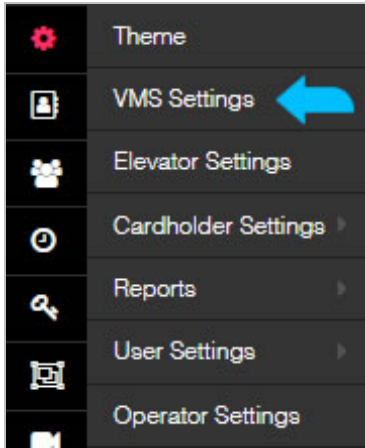
- [Create a Camera Group](#)
- [Remove Cameras from a Camera Group](#)
- [Delete a Camera Group](#)

Remove Cameras from a Camera Group

This section describes how to remove cameras from a User-Camera Group (a.k.a update the camera list in a Camera Group).

STEPS

1. Click on the **Settings** icon on the side menu and choose *VMS Settings*.



2. The *User Camera Mapping Page* will open.

NOTE: The page has inclusive search fields at the top of each column.

(Inclusive search means if you enter "d" in the search field, it will include ever person with the letter D in their name - even if it doesn't start with D.)

User Camera Mapping

User - Select User
 Search by User

Camera - Select Camera
 Search by Reader

Search by Camera

AA9003YQP7
securitypursuit
IMPORT_SYSOP
cyber_swift
customer1
customer2
customer3
customer4
customer5
candace
Joe
Jeff
Mark

Game Room Fisheye - (Cluster: 055, Cont: 001, Brd: 1, Sect: 1-0)
Lab PTZ - (Cluster: 055, Cont: 001, Brd: 1, Sect: 2-0)
Sales Lab - (Cluster: 055, Cont: 002, Brd: 1, Sect: 1-0)
Lobby Front 1 - (Cluster: 055, Cont: 002, Brd: 1, Sect: 2-0)
Secondary Lobby - (Cluster: 055, Cont: 003, Brd: 1, Sect: 1-0)
Lobby Doors - (Cluster: 055, Cont: 003, Brd: 1, Sect: 2-0)
Cafe Downstairs 1 - (In Elevator Reader)
Game Room Fisheye - (Reader 4 in home office)
Sales Lab - (B 5512 Point 1)
Lobby Doors - (B 5512 Point 2)
West Parking Lot OE-C3012T8 - (B 5512 Point 3)

Mapped User - Camera List
 Search by User

Search by Reader

Search by Camera

AA9003YQP7	All selected (8)	<input type="button" value="Update"/>
customer1	All selected (11)	<input type="button" value="Update"/>
customer4	All selected (3)	<input type="button" value="Update"/>
candace	All selected (6)	<input type="button" value="Update"/>
Joe	All selected (6)	<input type="button" value="Update"/>
Jeff	All selected (11)	<input type="button" value="Update"/>
Mark	All selected (11)	<input type="button" value="Update"/>
Todd	All selected (11)	<input type="button" value="Update"/>

- (optional) If your *User/Camera List* (3rd col.) is too long, you can use the search fields (above) to narrow your list.
- Select (click) the **Camera List dropdown field** beside the **User's Name** that you want to change.

Result: the Camera droplist will open and show a list of the assigned cameras.

[In this example there are 2 cameras in the list. The *Select All* is a 'toggle checkbox' to *select all* or *deselect all*.]

The screenshot shows a user interface with a list of users on the left: customer3, customer4, candace, and Joe. To the right of 'customer3', a dropdown menu is open, displaying 'All selected (2)'. The dropdown contains three items, each with a checked checkbox: 'Select all', 'Lobby Front 1 - (Cluster: 055, Cont: 002, Brd: 1, Sect: 2-0)', and 'Lobby Doors - (Cluster: 055, Cont: 003, Brd: 1, Sect: 2-0)'.

- "UNCHECK" a camera(s) you want to remove from the authorized camera list.
(Leave the cameras 'checked' that you want to keep in the group.)

Result: the chosen checkbox will be empty to remove the camera.

[checked = keep / unchecked = remove]

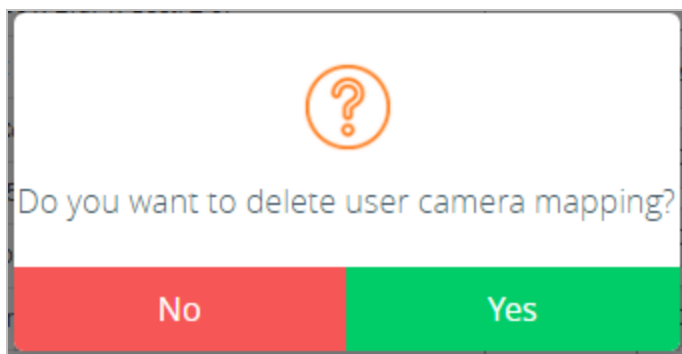
The screenshot shows the 'Mapped User - Camera List' interface. At the top, there are three search fields: 'Search by User', 'Search by Reader', and 'Search by Camera'. Below these is a table with columns for User Name, Camera List, and an 'Update' button. The 'Search by Camera' field has a magnifying glass icon. The table contains the following data:

User Name	Camera List	Update
AA9003YQP7	All selected (8)	Update
customer1	All selected (11)	Update
customer3	Lobby Front 1 - (Cluster: 055, Cont: 002, Brd: 1, Sect: 2-0)	Update
customer4	Lobby Front 1 - (Cluster: 055, Cont: 002, Brd: 1, Sect: 2-0)	Update
candace	Lobby Front 1 - (Cluster: 055, Cont: 002, Brd: 1, Sect: 2-0)	Update
Joe	Lobby Front 1 - (Cluster: 055, Cont: 002, Brd: 1, Sect: 2-0)	Update
Jeff	Lobby Front 1 - (Cluster: 055, Cont: 002, Brd: 1, Sect: 2-0)	Update
Mark	Lobby Front 1 - (Cluster: 055, Cont: 002, Brd: 1, Sect: 2-0)	Update

The dropdown menu for 'customer3' is open, showing a list of cameras with checkboxes. The 'Select all' checkbox is unchecked. The 'Lobby Front 1 - (Cluster: 055, Cont: 002, Brd: 1, Sect: 2-0)' checkbox is checked. The 'Secondary Lobby - (Cluster: 055, Cont: 003, Brd: 1, Sect: 1-0)' checkbox is unchecked. The 'Lobby Doors - (Cluster: 055, Cont: 003, Brd: 1, Sect: 2-0)' checkbox is unchecked.

6. Click the **UPDATE** button to update or save your changes to the camera list.

Result: LaunchPoint will prompt user to confirm the choices.

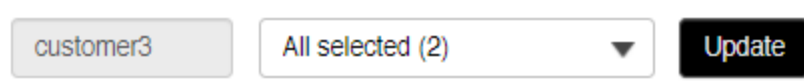


[Yes = update (changes will be saved). No = cancel update (no changes will be saved)]

7. The **Camera List** dropdown will reflect the changes you made.

Result: The Camera dropdown list will indicate the number of cameras now in the list.

[In this case, the user kept 2 cameras in the group.]



8. You can close the page if you are finished, or you can go to *Other Options*.

OTHER OPTIONS

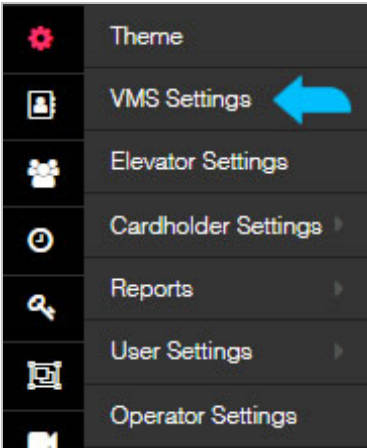
- [Create a Camera Group](#)
- [Add Cameras to a Camera Group](#)
- [Delete a Camera Group](#)

Delete a Camera Group

This section describes how to delete the entire Camera Group from the VMS Settings Camera Group list.

STEPS

1. Click on the **Settings** icon on the side menu and choose *VMS Settings*.



2. The *User Camera Mapping Page* will open.

NOTE:

The page has inclusive search fields at the top of each column.

(Inclusive search means if you enter "d" in the search field, it will include ever person with the letter D in their name - even if it doesn't start with D.)

User Camera Mapping

User - Select User

Search by User

Q

AA9003YQP7

securitypursuit

IMPORT_SYSOP

cyber_swift

customer1

customer2

customer3

customer4

customer5

candace

Joe

Jeff

Mark

Camera - Select Camera

Search by Reader

Q

Game Room Fisheye - (Cluster: 055, Cont: 001, Brd: 1, Sect: 1-0)

Lab PTZ - (Cluster: 055, Cont: 001, Brd: 1, Sect: 2-0)

Sales Lab - (Cluster: 055, Cont: 002, Brd: 1, Sect: 1-0)

Lobby Front 1 - (Cluster: 055, Cont: 002, Brd: 1, Sect: 2-0)

Secondary Lobby - (Cluster: 055, Cont: 003, Brd: 1, Sect: 1-0)

Lobby Doors - (Cluster: 055, Cont: 003, Brd: 1, Sect: 2-0)

Cafe Downstairs 1 - (In Elevator Reader)

Game Room Fisheye - (Reader 4 in home office)

Sales Lab - (B 5512 Point 1)

Lobby Doors - (B 5512 Point 2)

West Parking Lot OE-C3012T8 - (B 5512 Point 3)

Mapped User - Camera List

Search by User

Search by Reader

Search by Camera

Q

Map

AA9003YQP7

All selected (8)

▼

Update

customer1

All selected (11)

▼

Update

customer4

All selected (3)

▼

Update

candace

All selected (6)

▼

Update

Joe

All selected (6)

▼

Update

Jeff

All selected (11)

▼

Update

Mark

All selected (11)

▼

Update

Todd

All selected (11)

▼

Update

3. (optional) If your *User/Camera List* (3rd col.) is too long, you can use the search fields (above) to narrow your list.

4. Select (click) the **Camera List dropdown field** beside the **User's Name** that you want to change.

Result: the **Camera** droplist will open and show a list of the assigned cameras.

[. The *Select All* is a 'toggle checkbox' to *select all* or *deselect all*.]

customer3

customer4

candace

Joe

All selected (2)

- ☒ Select all
- ☒ Lobby Front 1 - (Cluster: 055, Cont: 002, Brd: 1, Sect: 2-0)
- ☒ Lobby Doors - (Cluster: 055, Cont: 003, Brd: 1, Sect: 2-0)

5. "UNCHECK" the Select All option which will uncheck all the camera(s) in the list.

Result: all checkboxes will be empty.

[checked = keep / unchecked = remove]

customer3

customer4

candace

Joe

Jeff

Mark

None selected

- ☐ Select all
- ☐ Lobby Front 1 - (Cluster: 055, Cont: 002, Brd: 1, Sect: 2-0)
- ☐ Lobby Doors - (Cluster: 055, Cont: 003, Brd: 1, Sect: 2-0)

6. Click the **UPDATE** button and click **Yes** to update or save your changes to the camera list.

Result: LaunchPoint will prompt user to confirm the choices.

Do you want to delete user camera mapping?

No Yes

[Yes = update (all cameras will be deleted). No = cancel update (no changes will be saved)]

7. The **Camera List** dropdown will reflect the changes you made.

Result: The Camera Group is removed from the list (col 3).

customer1	All selected (11) ▼	Update
customer4	All selected (3) ▼	Update

8. You can close the page if you are finished, or you can go to *Other Options*.

OTHER OPTIONS

- [Create a Camera Group](#)
- [Add Cameras to a Camera Group](#)
- [Remove Cameras from a Camera Group](#)

End of VMS Settings section.

Elevator Floor Group Mapping

This topic covers the system administrator's ability to map users to elevator floor groups for the Elevator system used by LaunchPoint.

FEATURED TOPICS

[Elevator Floor Group Mapping](#)

Elevator Floor Group Mapping (admin only)

This screen allows a *system administrator* to map users to floors in the Elevator system.

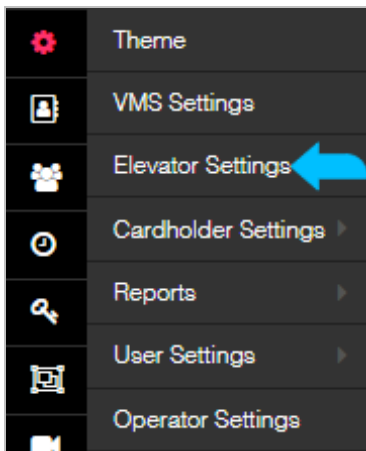
REQUIRED HARDWARE SETUP

Before the *Elevator Floor Mapping* can be done in LaunchPoint, the following hardware programming must be completed in System Galaxy (SG).

- At least one reader must be configured to be an “elevator reader” in the SG Configure > Hardware > Reader Properties screen.
- For *elevator relays* to be visible in LaunchPoint, the output relays must be configured to “show in tree” in Output Properties screen.

STEPS

1. Click on the **Settings** icon on the side menu and choose *Elevator Settings*.



2. The *User Elevator Mapping Window* will open.

NOTICE: The search fields in this page use *inclusive search rules* to help filter or narrow down the information shown in the list.

TERM: An “inclusive search” means that the **search results** will contain records that *include* the search criteria you provide.

For example: If the letter “d” is the search criteria, the search will only return records (i.e. user names) that *include* the letter “d” even if the name does not start with “d”. Thus, the results would contain names like Andrews, Davis, Edwards, ... because each name includes the letter “d”.

The screenshot shows the 'Elevator Mapping' interface. It is divided into three main sections:

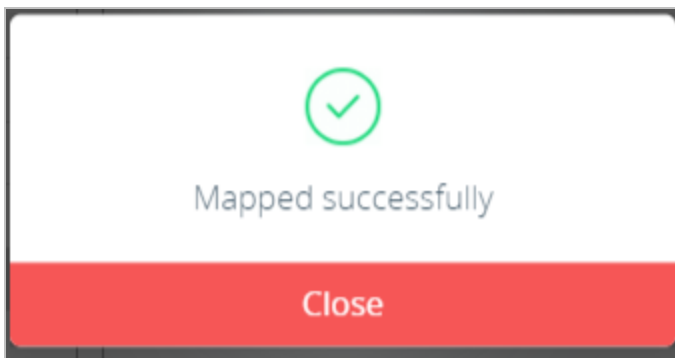
- User - Select User:** A search bar with a magnifying glass icon and a list of users: AA9003YQP7, securitypursuit, IMPORT_SYSOP, cyber_swift, and customer1.
- Elevator - Select Elevator:** A search bar with a magnifying glass icon and a list of relays: Relay 01 - (In Elevator Reader), Relay 02 - (In Elevator Reader), Relay 03 - (In Elevator Reader), Relay 04 - (In Elevator Reader), and Relay 05 - (In Elevator Reader).
- Mapped User - Elevator List:** A section showing the mapping results. It includes search bars for 'Search by User' and 'Search by Elevator', and a 'Search by Floor/Relay' bar. Below these are three rows of results:

Search by User	Search by Elevator	Search by Floor/Relay	Action
customer3	All selected (8)		Update
securitypursuit	Relay 01 - (In Elevator Reader)		Update
customer1	All selected (8)		Update

A 'Map' button is located between the 'Elevator - Select Elevator' and 'Mapped User - Elevator List' sections.

3. Select (click) a **User Name** in the first column to begin creating the Floor Group.
[HINT: clicking the *user name* a second time will deselect it.]
4. Next, select (click) the individual **Floor Relays(readers)** from the second column to choose them for the group.
[HINT: you can click more than one group to give the user access to multiple floors(shown above).]
[HINT: to deselect a camera, click the camera a second time.]
5. Click the **Map** button to assign the group of floors to the user.
6. Click Close on the User Confirmation message.

Result: This message confirms your Floor Group is created.



7. The new **User-Floor Group** is created and added to the Floor Groups list (3rd column).

[HINT: you can see the total number of Floors/Relays in the parentheses.]

The screenshot displays the 'Administrative Settings' interface for mapping users to floor relays. It is divided into three main sections:

- User - Select User:** A search bar and a list of users: AA9003YQP7, securitypursuit, IMPORT_SYSOP, cyber_swift, and customer1.
- Elevator - Select Elevator:** A search bar and a list of relays: Relay 01 - (In Elevator Reader), Relay 02 - (In Elevator Reader), Relay 03 - (In Elevator Reader), Relay 04 - (In Elevator Reader), and Relay 05 - (In Elevator Reader).
- Mapped User - Elevator List:** A search bar, a 'Map' button, and a list of mapped users. Each entry shows the user name, a dropdown menu indicating the number of selected relays (e.g., 'All selected (3)', 'All selected (8)'), and an 'Update' button.

8. You can close the page if you are finished.

9. To **Add more floor/relays to an existing Floor Group**, do the following ...

- Select the same user name in the first column.
- Select the additional floor relays in the second column -
(no need to reselect floors/relays that already belong to the group, just pick the new ones you want to add).
- Click MAP button to add the floor/relays to the existing Floor Group in the third column.
- You should see your chosen floors are added to the Floor droplist - and the *total count* in parentheses will increase.

10. To **Remove one or more floors from a Floor Group**, do the following ...

- Open the Floor droplist in the 3rd column for the user you want to update,
- Uncheck only the floors you want to remove.
- Click the UPDATE button to remove the floors.
- You should see the deselected floors are no longer in the Floor droplist - and the *total count* in parentheses has decreased.

11. To **Delete a Floor Group entirely**, do the following ...

- Open the Floor droplist in the 3rd column for the user floor group you want to update
- "Uncheck" the **Select All** option to remove all checkmarks from every floor/relay in the list.
(Note: if any floor remains checked, the group will not be deleted.)
- Click the UPDATE button to delete the Floor Group completely.

- d. You should see the Floor Group has been deleted from the 3rd column.

User Login Multi-Factor Authentication

This topic covers how users can configure their contact details for multifactor authentication for their LaunchPoint login accounts.

FEATURED TOPICS

[About Multi-Factor Authentication](#)

[Update User Contact Information](#)

[First-Time Logon with MFA Settings](#)

About Multi-Factor Authentication (MFA)

This setting allows an user to add their own contact details for multi-factor authentication (i.e., email and phone) on their logon account.

PREREQUISITES AND NOTES

- First, a system administrator must enable *Multi-factor Authentication* (MFA) on the user logon account in the system programming.
- The user will be prompted to set up their contact details on their first-time logon attempt.
When the user submits their contact information at the first logon page, LaunchPoint immediately issues a random **OTP Code** (plain text) to the user's email and phone.
- Every time the logs-in, a new OTP Code is issued. The user must enter the code into the login page when prompted.

- If the LaunchPoint session expires or the user logs out, the system will generate a new code. LaunchPoint issues a new/different code each time the user signs in.

Update User Contact Information (MFA)

The user can update the *multi-factor authentication* settings from the User Settings in LaunchPoint. Each user can only see and update their own contact details while they are actively logged in.

STEPS

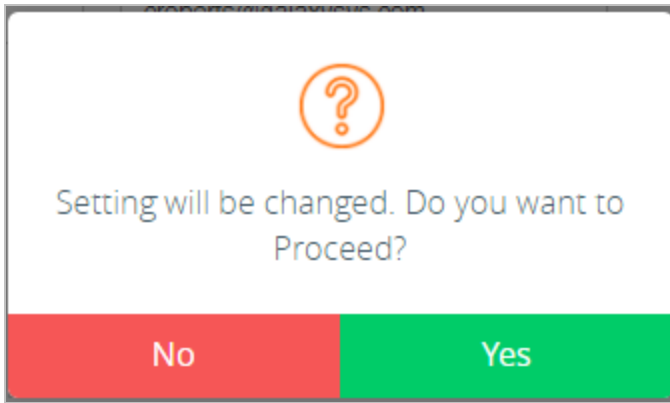
1. Sign in as normal to the LaunchPoint application - *this will include submitting the OTP Code when prompted.*
2. Click **Settings menu option** (side menu).



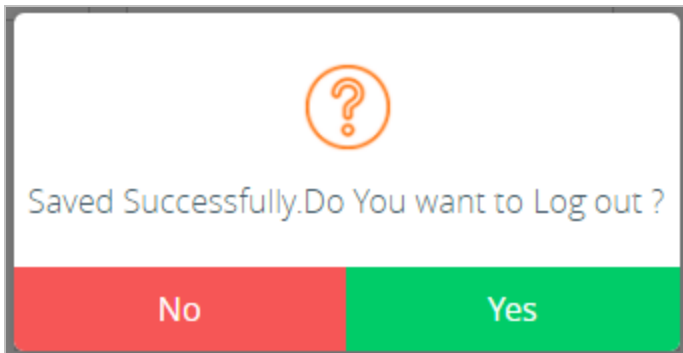
3. Choose **User Settings > Multi-Factor Authentication** from the settings menu.
4. When the *Profile Settings Page* opens, it will display the currently configured information.

A screenshot of the 'Profile Settings' page. The page has a light gray background. At the top, there's a header 'Profile Settings' with a blue vertical bar to its left. Below the header, there's a section titled 'Profile Information'. Inside this section, there are two input fields: 'Phone No' with the value '3015048888' and 'Email' with the value 'crogers@galaxsys.com'. Below these fields is a black 'Save' button with white text.

5. Enter a **valid phone number** in the Phone field.
6. Enter a **valid email address** in the Email field.
7. Click **Save** button and you will be prompted to confirm changes.
 - Yes = proceed with saving changes.
 - No = cancel changes.

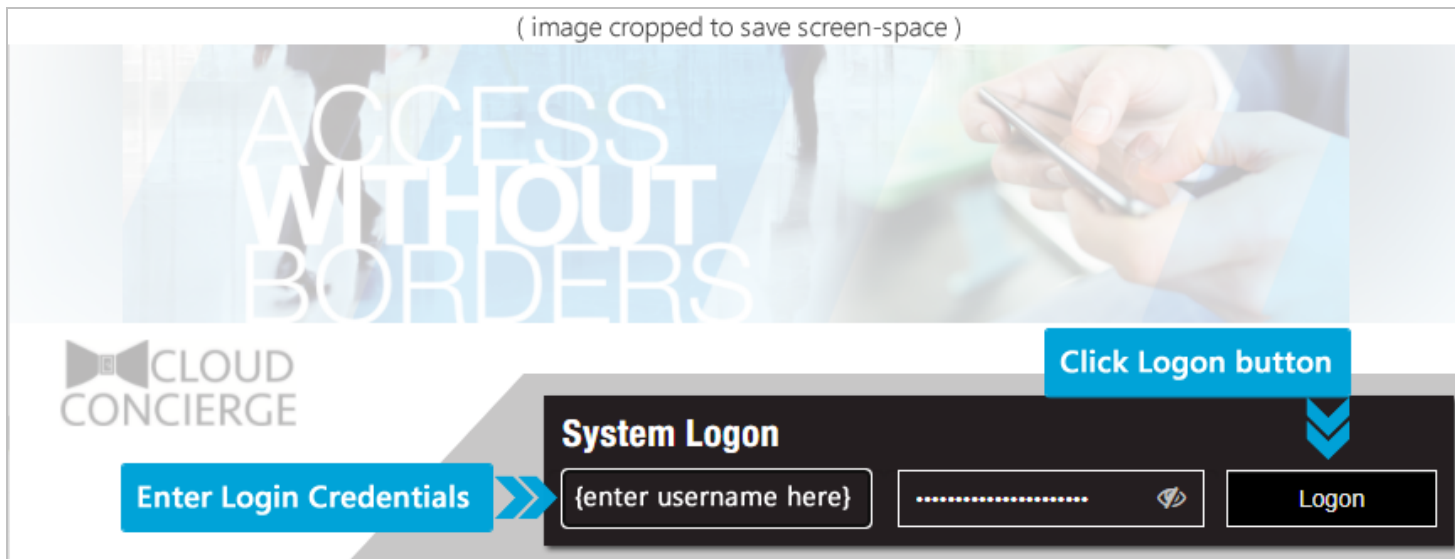


8. Click **YES** to save changes, and you will be prompted to confirm whether to log-out or stay logged-in.
- Yes = log-out (session will close; you need to logon using your new contact info).
 - No = remain logged-in (session remains open, but system will use the new contact info the next time you logon).



User's First-Time Logon

1. The system administrator must enable the *MFA Feature* for the individual user account.
2. Open the *LaunchPoint Window*, and enter the **User Name** and **Password**, and click the **Logon button**.



3. If this is the first login, MFA Registration popup will display.

The window will only popup on the first logon attempt.

- Enter a valid *phone* and *email*
- Click **Send button** to generate a random **OTP code** (plain text).

RESULT: a random code is sent to both the phone and email at the same time.

Multi-Factor Authentication

You have not registered for multi-factor authentication, please enter

Phone No 3015048888

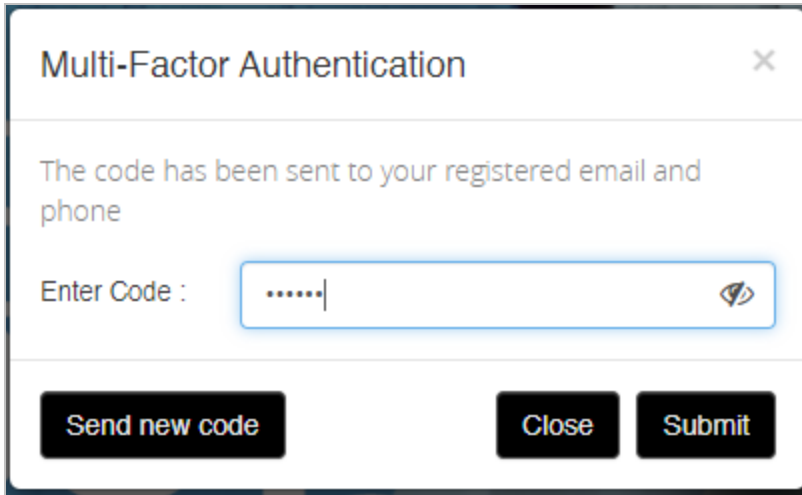
Email chughes@galaxysys.com

Close Send

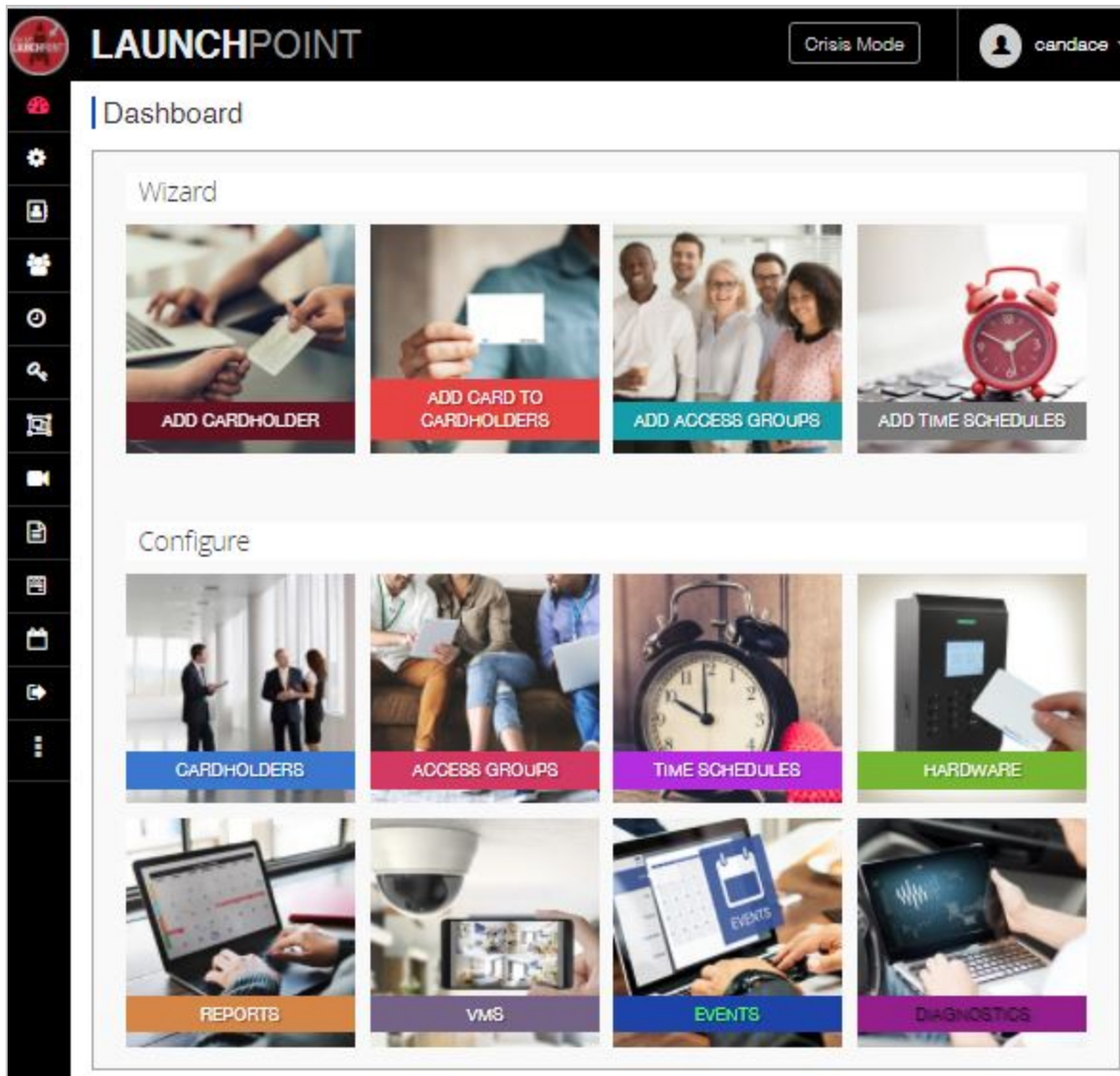
4. When the text arrives, enter the **OTP Code** into the *MFA Authentication Popup* and click **Submit** to logon.
- Clicking *Submit* will submit the OTP Code you entered.
 - Clicking *Send New Code* button will issue a new random OTP Code to your phone.

- Clicking *Close* will exit the MFA popup message-box without logging in.

Note: clicking the eyeball icon to show/hide the code, which helps user see they are typing correctly.

A screenshot of a 'Multi-Factor Authentication' popup dialog. The dialog has a title bar with the text 'Multi-Factor Authentication' and a close button (X) in the top right corner. Below the title bar, the text 'The code has been sent to your registered email and phone' is displayed. Underneath, there is a label 'Enter Code :' followed by a text input field containing five dots and a cursor. To the right of the input field is an eyeball icon for toggling visibility. At the bottom of the dialog, there are three buttons: 'Send new code', 'Close', and 'Submit'.

5. If the code is rejected, the system will *resend another code* until you have exhausted your retry attempts.
6. When the code is accepted, the *LaunchPoint Dashboard Page* will display.



Multi-factor User Login

This topic covers how to configure **multi-factor authentication** for the user login (a.k.a. dual authentication) .

FEATURED TOPICS

Overview and Prerequisites

Using the Multi-Factor Login

Change User's Multi-Factor Settings

Overview and Prerequisites

The *Multi-factor Login feature* allows the user to add their **email** and **phone** to receive a *multi-factor authentication contact* (MFA), which the user must respond to at the time of their login.

PREREQUISITES AND NOTES

- The system administrator must enable *Multi-factor Authentication* (MFA) for each individual user, in the system programming.
- On the first logon attempt, the user must enter their *contact information* into the Multi-factor popup box.
- When the user submits the contact information at the logon page, the system immediately issues a random OTP Code (plain text) to the user. The system issues a new/different code each time.
- User must use the code to sign in each time. If the session expires or the user logs out, the system will generate a new code.

HOW TO OPEN THE MULTI-FACTOR SETTINGS

There is one way to open the Multi-Factor Settings page.

1. From the side menu, click the **Settings icon**.
2. From the *cascading menu*, choose the **Multi-Factor option** (it may be the only option the user can see, depending on user privileges). *This option is not found on the Dashboard.*



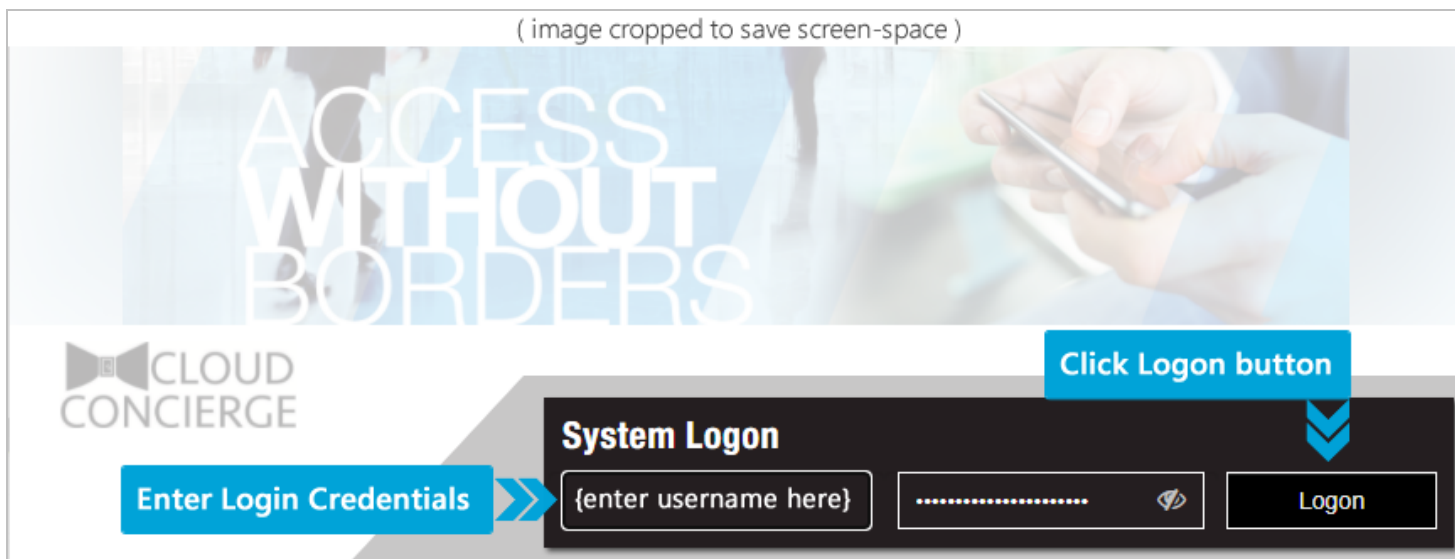
← Settings Icon (side menu)

Using the Multi-Factor Authentication

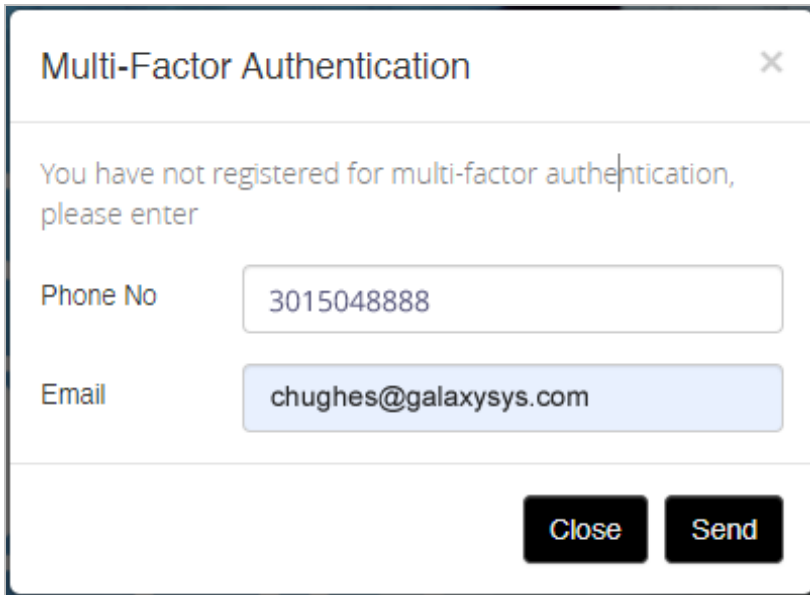
The user must set up a **valid email** and **phone number** when prompted the first time logging in.

The system will send an OTP Code to the user that must be entered in at the time of login.

1. The system administrator must enable the *MFA Feature* for the individual user account.
2. Open the *LaunchPoint Window*, and enter the **User Name** and **Password**, and click the **Logon button**.



3. If this is the first login, the system will prompt user for their **email** and **phone**.



A dialog box titled "Multi-Factor Authentication" with a close button (X) in the top right corner. The message inside says "You have not registered for multi-factor authentication, please enter". Below this, there are two input fields: "Phone No" with the value "3015048888" and "Email" with the value "chughes@galaxysys.com". At the bottom right, there are two buttons: "Close" and "Send".

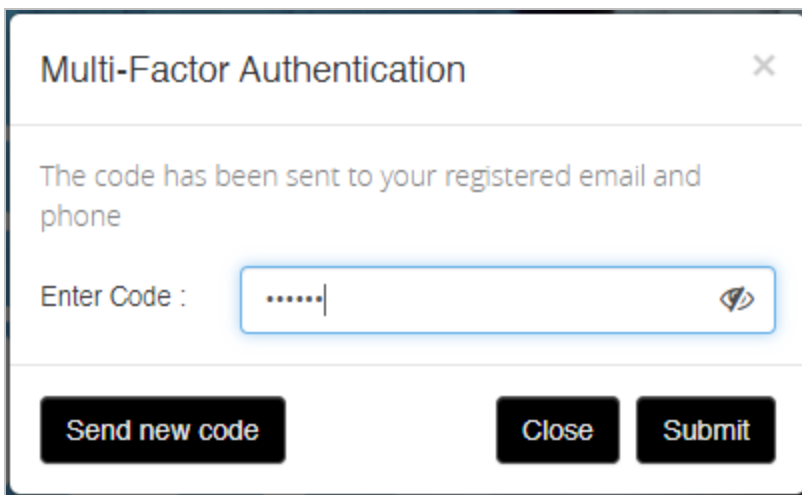
4. Click **Send button** to generate and send a random **OTP code** (plain text) to yourself.

RESULT: a random code is sent to both the phone and email at the same time.

5. When the **OTP Code text** arrives, enter the code into the **OTP Prompt** and click **Submit** to sign in.

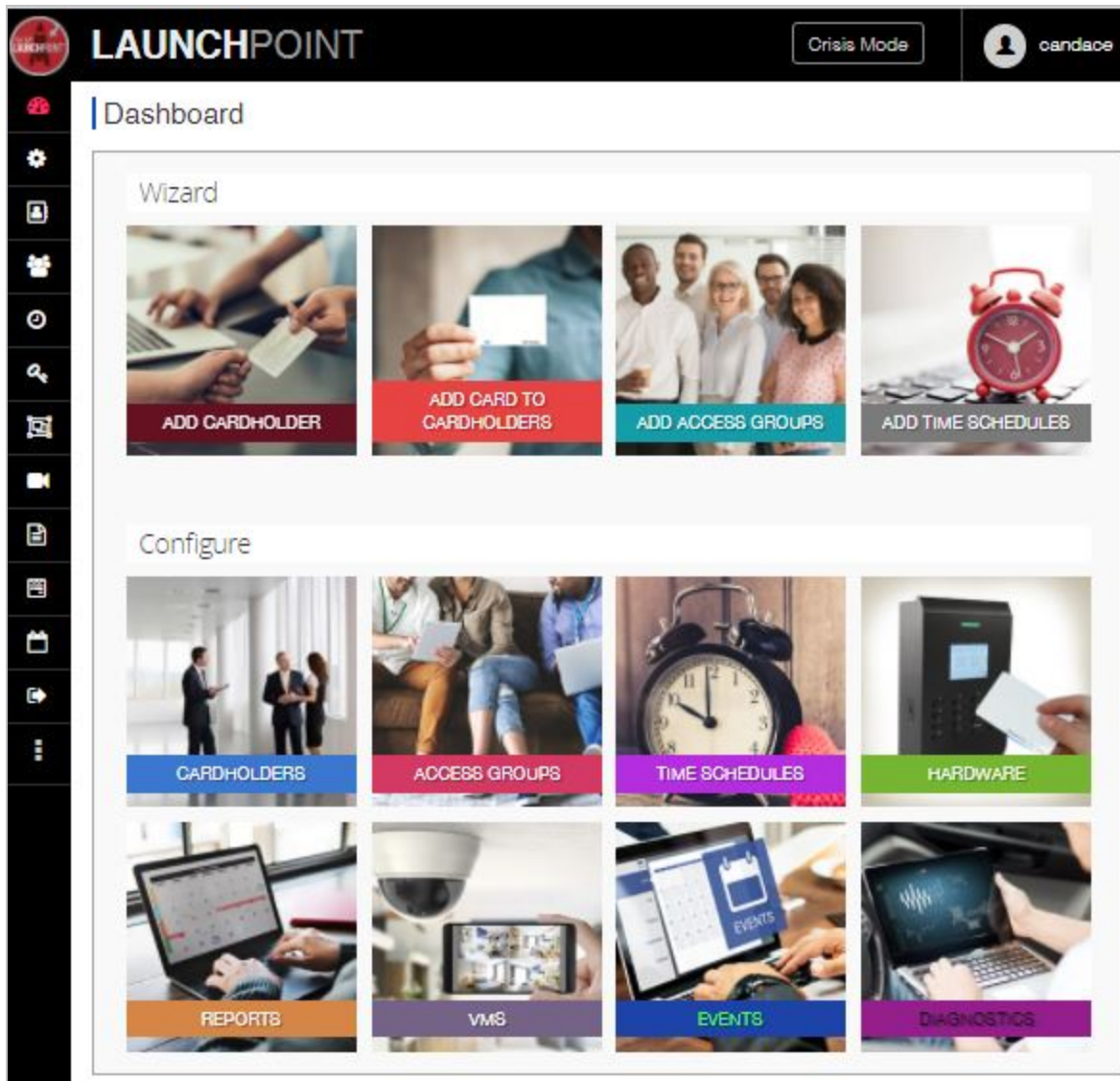
- Clicking Submit will submit the OTP Code you entered.
- Clicking Send New Code button will issue a new random OTP Code to your phone.
- Clicking Close will exit the MFA popup message-box without logging in.

Note: clicking the eyeball icon to show/hide the code helps ensure you are typing it correctly.



A dialog box titled "Multi-Factor Authentication" with a close button (X) in the top right corner. The message inside says "The code has been sent to your registered email and phone". Below this, there is a label "Enter Code :" followed by a text input field containing six dots "....." and an eyeball icon to toggle visibility. At the bottom, there are three buttons: "Send new code", "Close", and "Submit".

6. If the code is rejected, the system will *resend another code* until you have exhausted your retry attempts.
7. If the code is accepted, *The Dashboard Page* will display.



Change Multi-Factor Authentication Settings

The user can update the *multi-factor authentication* settings from the User Settings in LaunchPoint.

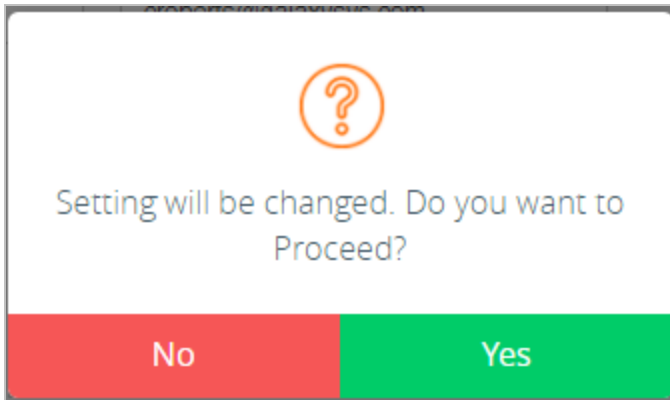
1. Sign in as normal to the LaunchPoint application - *this will include submitting the OTP Code when prompted.*
2. Click **Settings** menu option, and choose **User Settings** > **Multi-Factor Authentication** from the menu.



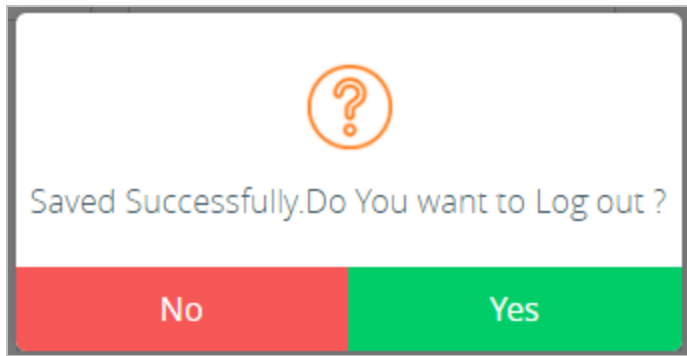
3. When the Profile Settings page opens, it will display the currently configured information.

A screenshot of a web application's 'Profile Settings' page. The page has a light gray background. At the top, there's a header 'Profile Settings' with a blue vertical bar to its left. Below the header, there's a section titled 'Profile Information' in a darker gray box. Inside this section, there are two input fields: 'Phone No' with the value '3015048888' and 'Email' with the value 'crogers@galaxysys.com'. Below these fields is a black button with the text 'Save' in white.

4. Enter a **valid phone number** in the Phone field.
5. Enter a **valid email address** in the Email field.
6. Click **Save** button and you will be prompted to confirm changes.
 - Yes = proceed with saving changes.
 - No = cancel changes.



7. Click **YES** to save changes, and you will be prompted to confirm whether to log-out or stay logged-in.
 - Yes = log-out (session will close; you need to log-in using your new info).
 - No = remain logged-in (session will remain open, you need to log-in using new info next time).



LaunchPoint Wizards

LaunchPoint Wizards will help the user *add new records* to the system - such as adding new *Cardholders, Cards, Schedules, or Access Groups*.

To find and update existing records, use the *Configuration screens* (Editors) - [see Features for more info](#)

FEATURED WIZARDS

- [Add New Cardholder Wizard](#)
- [Add New Card Wizard \(imbedded\)](#)
- [Add Access Group Wizard](#)
- [Add Schedule Wizard](#)
- [Find an Existing Cardholder \(Lookup\)](#)
- [Other Features \(editors\)](#)

Click a link to open the topic.

OVERVIEW: ABOUT WIZARDS

This section provides a functional overview of each wizard.

LaunchPoint Wizards are designed help you perform tasks using the correct sequence of steps. Each wizard screen provides the appropriate fields for the related step. This helps you to repeat tasks with a consistent process and avoid missing steps.

LaunchPoint Wizards let you add new records to the system for cardholders, cards, access groups, and time schedules. If you need to edit a record that already exists, you must use the Editor screens. Editor screens have all the fields in one screen and do not enforce the order you move around the fields. If you press the ADD button in the Editor, you will launch the wizard.

- Use the [Quick links](#) above to see the user instructions for each wizard .
- If you have already added your record, you can [go to the Features menu](#) and find the topic for the appropriate editor.

About the 'Add Cardholder' Wizard

This wizard allows you to add a new cardholder to the system, as well as assign access credentials, and more.

Prerequisites and Notes ...

- The access group(s) you wish to assign must exist in the system (i.e. added before you launch the wizard).
- The Cardholder cannot exist in the system. You cannot edit an existing Cardholder from the wizard.
- If you already added the cardholder, either use the [Add Card Wizard](#) to add a credential and permissions, or use the [Cardholder Editor](#) to continue editing cardholder information.
- Contact your system administrator or authorized dealer if you do not see your access locations.
- You cannot print an ID Badge from the Wizard. See the [Cardholder Editor](#).

Navigation Controls and Buttons ...

The user can use the following buttons and controls to navigate through the wizard screens.

- **Additional Fields** (cbx control) - expands/collapses a set of additional fields that are usually optional.
- **Data Fields 5-50** - opens the **5 - 50 Data Fields** screen.
(You must expand **Additional Fields** checkbox to find this button.)

TIP: Using these fields is up to the discretion of the system subscriber / administrator unless they have been designated as mandatory by the system administrator or authorized dealer. Fields designated as mandatory must be non-blank for the user to advance to the next screen.

- **Synchronize Badge** - syncs the badge template field (droplist) for the system subscriber.
- **Next** - moves forward to the next screen in sequence.
- **Back** - moves backward to the last screen in sequence.
- **Skip** - skips the current screen and moves the user to the next screen in sequence.
- **Finish** - completes the task, saves the card record and closes the wizard. User is returned to the starting screen or the dashboard.

In the Add Cardholder Wizard, you can enter the following information ...

1. cardholder **first, middle, last name** - (mandatory to save cardholder)
2. personal information (phone, address, etc.)
3. assign a department
4. import a photograph
5. add an access card *
6. assign an ID Badge **
7. assign authorized access locations (loops)
8. assign access permissions (access groups)

NOTE: The *Cardholder wizard* can be configured to show or hide specific fields that the system subscriber does not want to see or use. This is handled by an authorized administrator or dealer.

- * You can also add an *arming card* through the wizard.
- ** You must be licensed for a badging solution and Badge Designs must be imported & synchronized.

About the 'Add Card' Wizard

The **Add Card Wizard** allows you to add a new card to an existing cardholder in the system, as well as assign permissions.

If your cardholder has not been added, see the [Add Cardholder Wizard](#), which also allows you to add a card.

If your card has already been added, see the [Cardholder Editor](#) to modify existing credentials.

Prerequisites and Notes

- The **access group(s)** you wish to assign must exist in the system (i.e. added before you launch the wizard).
- The Cardholder must exist in the system. See the [Add Cardholder Wizard](#) to add a new cardholder if needed.
- The card cannot already exist in the system. If you already added the card, use the [Cardholder Editor](#) to modify existing card information.
- Contact your system administrator or authorized dealer if you do not see your access locations.
- You cannot print an ID Badge from the wizard. See the [Cardholder Editor](#).

Navigation Controls and Buttons ...

The user can use the following buttons to navigate through the wizard screens.

- **Additional Fields** (cbx control) - expands/collapses a set of additional fields that are usually marked as optional.

TIP: Using these fields is up to the discretion of the system subscriber / administrator unless they have been designated as mandatory by the system administrator or authorized dealer. Fields designated as mandatory must be non-blank for the user to advance to the next screen.

- **Synchronize Badge** - syncs the badge template field (droplist) for the system subscriber.
- **Next** - moves forward to the next screen in sequence.
- **Back** - moves backward to the last screen in sequence.
- **Skip** - skips the current screen and moves the user to the next screen in sequence.
- **Finish** - completes the task, saves the card record and closes the wizard. User is returned to the starting screen or the dashboard.

In the Add Card Wizard, you can enter the following information ...

1. add an access card *
2. choose one or more locations (loops)
3. assign an ID Badge **
4. assign access permissions

NOTE: The *wizard* can be configured to show or hide specific fields that the system subscriber does not want to see or use. This is handled by an authorized administrator or dealer.

* You can also add an *arming card* through the wizard.

** You must be licensed for a badging solution and Badge Designs must be imported & synchronized.

About the 'Add Access Group' Wizard

The **Add Access Group Wizard** allows you add a new access group to the system, - this includes assigning **authorized doors** and **schedules**, as well as **crisis mode** behavior and more.

- If the Time Schedules have not been added, see the [Add Time Schedules Wizard](#), which also allows you to add **special days** (holidays).
- If you need to change and existing access group or time schedule, see the [Access Group Editor](#) or [Time Schedules Editor](#) as appropriate.

Prerequisites and Notes

- The **time schedules** you wish to assign must already exist (i.e. added before you launch the wizard).
- The **access group** cannot exist in the system already. You cannot edit an existing access group from the wizard.
- If you already added the access group, use the [Access Group Editor](#) to continue editing cardholder information.
- Contact your system administrator or authorized dealer if you do not see your access locations.
- An access group will not function in the system if it does not have a valid schedule assigned to at least one door.

Navigation Controls and Buttons ...

The user can use the following buttons to navigate through the wizard screens.

- **Additional Fields** (cbx control) - expands/collapses a set of additional fields that are usually marked as optional.

TIP: Using these fields is up to the discretion of the system subscriber / administrator unless they have been designated as mandatory by the system administrator or authorized dealer. Fields designated as mandatory must be non-blank for the user to advance to the next screen.

- **Add New** - opens the Add Access Group Wizard screen.
- **Next** - moves forward to the next screen in sequence.
- **Prev** - moves backward to the last screen in sequence.
- **Finish** - completes the task, saves the card record and closes the wizard. User is returned to the starting screen or the dashboard.

In the Add Access Group Wizard, you can enter the following information ...

1. choose an existing Loop/Cluster
2. enter an access group name *
3. choose a crisis mode (for how the system behaves in crisis mode)
4. enter an activation and expiration date/time
5. set options to make the system treat the group as disabled or as extended
6. enter notes, comments, and service comments
7. add authorized doors and time schedules **

* A system number will be assigned to the access group when you exit the Access Group Name field.

** You must have already created the time schedule you want to assign.

About the 'Add Time Schedule' Wizard

The [Add Time Schedule Wizard](#) is actually the same screen as the Schedules Editor. This feature allows you to add a new time schedule to the system, which includes configuring **special days (holidays)**.

- If you need to change an existing time schedule, see the [Time Schedules Editor](#) as appropriate.

Prerequisites and Notes

- The **time schedule** you wish to add cannot already exist in the system already. You can select and edit an existing schedule from the wizard.
- If you already added the schedule, see the [Time Schedule Editor](#) for the topic on editing existing schedules.
- An schedule will not function in the system if it does not have a time configuration for each day completed.

Navigation Controls and Buttons ...

This wizard essentially has one screen. It makes a difference whether you are adding a new schedule (add new) or if you are selecting an existing schedule to edit.

- **Add New** - opens the wizard so user can add the name of the new schedule.
- **Save** - saves the schedule and any modifications.
- **Delete** - deletes the selected schedule from the system.
- **Affected by Special Days** (cbx control) - expands/collapses a set of additional *time configuration fields*.

TIP: Adding special days (holidays) is up to the discretion of the system subscriber. If your schedule needs to work the same way all the time (365-days a year) then do not configure special days. This could be true of a schedule that is assigned to hardware or to emergency personnel who may be immune to holidays.

In the Add Time Schedule Wizard, you can enter the following information ...

1. choose an existing Loop/Cluster
2. enter a time schedule name *
3. show/hide the time schedule bars for special days (holidays) **
4. configure the start and stop times for each week day.
5. configure the start and stop times for time schedules.

- * A system number will be assigned to the schedule when you exit the Schedule Name field.
- ** Configuring special days is optional - up to subscriber discretion.

Add Cardholder Wizard

TASK: Add (enroll) a new **Cardholder** to the system including adding the photo, access card, and assigning access permissions.

featured topics

[Adding a New Cardholder \(including requirements\)](#)

[Adding Personal Data \(inclu. Data Fields 2 - 4\)](#)

[Adding More Data \(Fields 5 -50\)](#)

[Adding a Photograph](#)

[Adding an Access Card](#)

[Adding a Location \(cluster\)](#)
[Assigning Access Permissions](#)

FAQs : Enrolling a New Cardholder

[Prerequisites & Notes](#)
[Opening the Cardholder Wizard](#)
[About Cardholder Data Fields](#)
[About Adding Cardholder Information Later](#)

See Related Topics

[Add Card](#)[Cardholder Look-up](#)[Add Access Group](#)[Add Time Schedule](#)[Other Features](#)

About Enrolling a New Cardholder

This section explains information about adding a Cardholder to the system in general, with some information specifically related to the cardholder wizard.

Enrolling a Cardholder includes adding personal data, adding a photograph, enrolling an access card, and assigning access permissions and/or an ID badge - at the user's discretion. The Add Cardholder Wizard allows the customer to customize the process according to client needs.

If you begin enrolling a cardholder and cannot finish all the fields, you have two choices ...

- A. you can exit the Wizard without saving and restart the enrollment from the Cardholder Wizard when you have the information.
- B. you can save what you have in the Wizard, then enter the remaining information from the Cardholder List (Cardholder Editor).

PREREQUISITES & NOTES

- The *Access Group* must already exist in the system before you can add it to the cardholder. See the [Add Access Group](#) if you need to add the group.
- You can enroll an access card during the Cardholder Wizard session, provided you know the card data.
- You can assign access permissions
- If you already added the cardholder name, see [Cardholder List \(Editor\)](#).

How to Open New Cardholder Wizard

This section covers information about adding a new cardholder through the Cardholder Wizard.

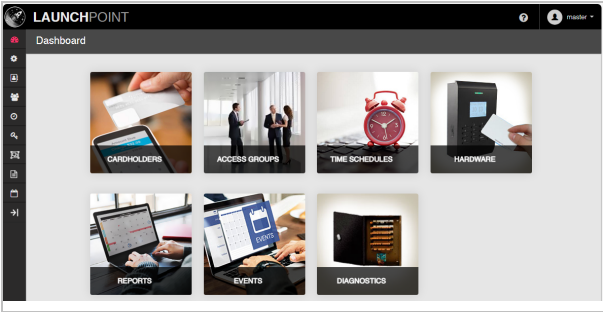
How to Launch the Cardholder Wizard ...

The cardholder wizard is typically launched from the dashboard screen.

From the Dashboard:

Simply click the **Add Cardholder** tile to open the wizard.

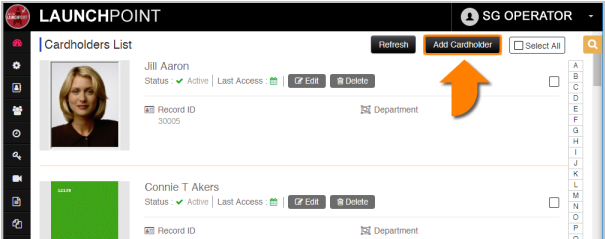
The tile is located on under Wizards heading near the top of the screen.



← LaunchPoint Dashboard

From the Cardholder List screen:

Also, if you click the **Add Cardholder** button in the Cardholder List screen, the Cardholder Wizard will be launched .



← Cardholder List (thumbnail)

About Cardholder Data Fields

The user can only add or enroll a *new cardholder* through the Cardholder Wizard screen.

Required System Fields Explained ...

To add a new record in the system, you must satisfy "required" fields, such as the *name* field. The wizard will not allow the user to save a record or leave a screen until the required field is satisfied.

NOTE: Any unsaved discretionary data will not be saved if the user aborts/cancels the wizard.

Mandatory Fields Explained ...

Fields that are normally optional or discretionary can be configured to behave as mandatory by the system administrator. Mandatory fields are designated with a red asterisk. The user must satisfy any fields that have been designated as "mandatory" by the system administrator before advancing to the next screen.

Conditionally Required Fields Explained ...

The Cardholder Wizard allows the user to add different types of information, such as a *photograph*, *access card*, *access permissions*, or a *badge template*. Although this information is discretionary, key fields are "required" if the user begins programming an option.

The wizard will prompt the user to satisfy the missing information and highlight the fields with a red border. The user cannot advance or save until the missing information is satisfied or the user removes the partial information.

NOTE: *All the system rules apply concerning required, mandatory, conditionally required, and discretionary fields. If you begin adding a card, you must satisfy any conditionally required fields or remove the card programming to skip it.*

Optional and Discretionary Fields Explained ...

The Cardholder Wizard allows the user to add or omit different types of information, such as a *photograph*, *access card*, *access permissions*, or a *badge template*.

Optional and discretionary fields are performed at the user discretion if the information is readily available, or as a matter of the enrollment policy of the system owner (i.e. the company that operates the system).

If the information is not required by policy, or if it is not available at the moment of enrollment, then the user can opt-out or skip the fields in the wizard. Most data fields are optional in the Cardholder Wizard.

NOTE: *You can add optional or discretionary data later in the Cardholder Editor.*

Can I Add Cardholder Information Later?

If you skip optional and discretionary fields during the Wizard session (such as photograph, card, permissions, badge, etc.), you can always add this data later in the *Cardholder Editor* screen.

[← Cardholder Editor \(thumbnail\)](#)

The Cardholder record must have been saved before you exit the wizard in order to find and open the cardholder in the editor screen.

NOTE: the cardholder is automatically saved when the user advances the wizard from the **Cardholder Information** screen by pressing the Next button in the wizard.

All the system rules apply concerning required, mandatory, conditionally required, and discretionary fields.

Adding a Cardholder

You must add a First name and Last name in order to create (save) a new cardholder. Other fields are considered discretionary, based on the enrollment policy -- meaning whether or not you are adding a photograph, a card, a badge, and additional information.

REQUIREMENTS

- First and Last names are required, plus any custom-designated mandatory fields and conditionally required fields (these are marked with red asterisk). User cannot save until the required fields are satisfied.
- If you are adding a card, you will need to know the **access card code**.
- To assign access permissions, the **access groups** must already be created.
- To assign a badge template, the **badge template** must already be imported into the system.

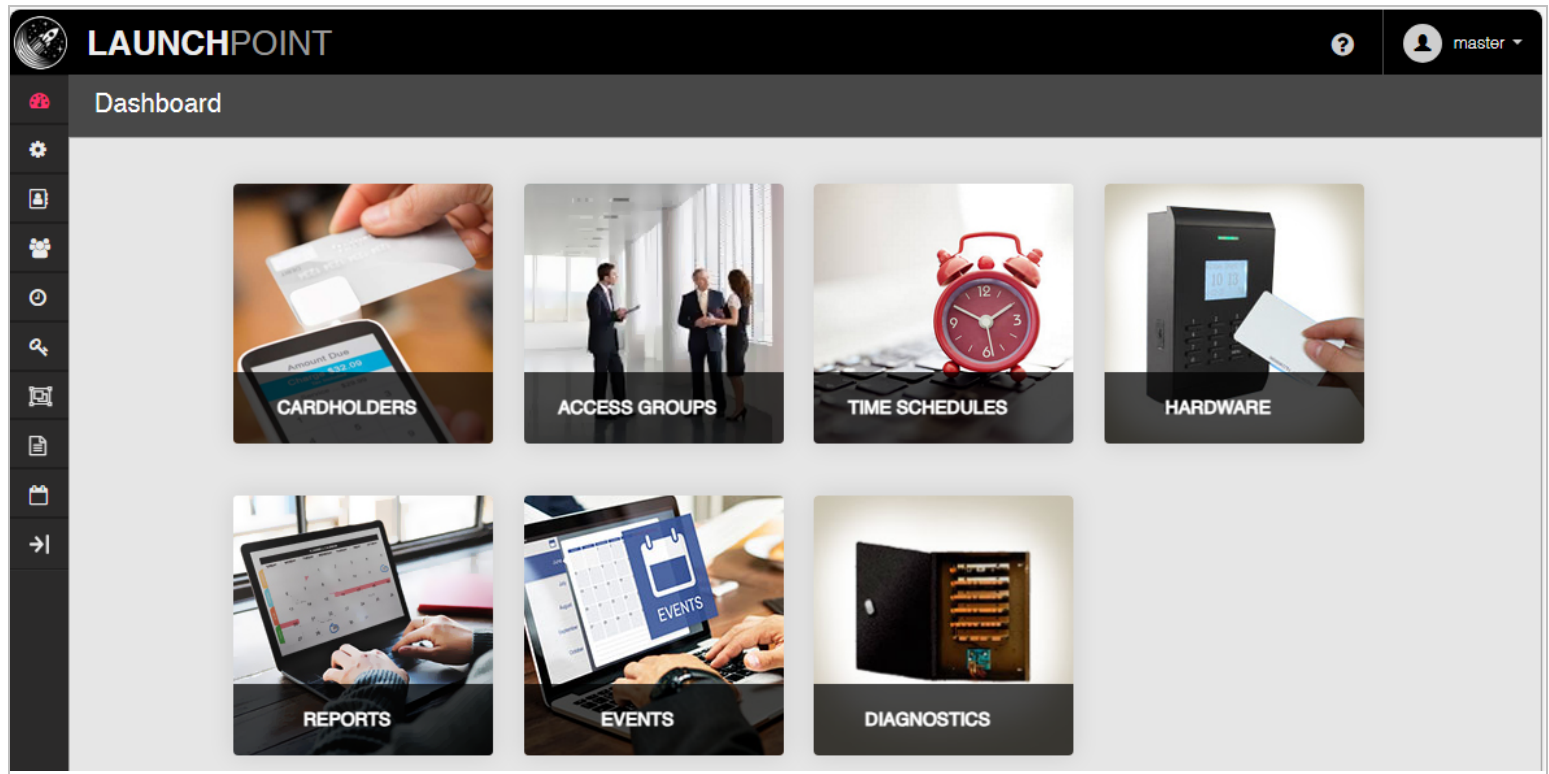
- To print a badge you must go to the **Cardholder Editor**.
- If you exit the wizard prematurely or skip items, you can use the **Cardholder List** to look up the person and finish the task in the Cardholder Editor screen..

OTHER TIPS

Contact your administrator or authorized dealer with questions about access locations, access profiles, departments, customized data fields, badge templates, or questions related to VMS or Badging license.

Add Cardholder Information

To add a new cardholder from the Cardholder Wizard, you must launch the Wizard. The first screen of the Wizard is the Cardholder information screen.



[◀ LaunchPoint Dashboard](#)

◀ Cardholder Wizard - Information screen

1. Sign-in to **LaunchPoint** and go to the Dashboard 🏠 page.
2. Click **Add Cardholder Tile** on the Dashboard to open the wizard (see above screenshot).
3. In the *Cardholder Information* window, enter **First and Last Names** (**mandatory**)
4. Choose a **Customer Name** from the *Customer droplist* as appropriate.
(“No Customer” is the default in some systems, while cloud systems may be defaulted to their own client name.)
5. Choose a **Department Name** from the *Department droplist* as appropriate.
6. Click on the **D.O.B.** field to enter a date using the calendar function.
7. Click on **Date 1** or **Date 2** fields and enter a date as appropriate using the calendar function.
(the date-1 and -2 fields can be used for any date at the discretion of the system subscriber – like date of hire.)

NEXT : Do one of the following things to proceed ...

- click **Additional Fields** checkbox to open more fields (opens the [Additional Fields](#) section).
- click **Data Fields 5-50** to open more fields (opens the [Data Fields 5-50](#) window)
- click **Sync Template** button to synchronize badge templates.

- click **FINISH** button to save the cardholder now and exit the wizard (without adding a photo or access card, etc.).
- click **NEXT** to advance to the next screen (should be the [Add Photo](#) window).

Additional Fields

These fields are optional or discretionary unless your administrator has configured them to be mandatory in the system.

- A mandatory field will be red and have an asterisk (*) beside it. It cannot be skipped - the screen will not advance until it is satisfied.
- You can configure optional/discretionary fields later in the *Cardholder Editor Screen* if you want to skip them now in the wizard.

NOTES

- Some grayed/disabled fields are locked by your system administrator or by the system.
 - Some grayed fields will be auto-filled by the system after the cardholder is enrolled; such as Last Access, Date Added, Last Modified.
 - Contact your administrator for questions regarding configuring Data # field names.
 - All 50 Data fields should always be used consistently for reporting and administrative purposes.
-

Adding Additional Information

LaunchPoint

https://accessonthego.com/cc/AddPerson/Index?ref=1

LAUNCHPOINT

Version : PRO | Build : 305

SG OPERATOR

Cardholder Wizard

Cardholder Information

☒ Additional Fields

Record ID

Common ID

Record Type

Select

Email Address

cer@galaxysys.com

Address 1

111 Park Road

Address 2

City

Big Sur

State

California

Zip Code

21701

Home Phone

240-402-9900

Data 1

Engineering

Data 2

Data 3

Data 4

Last Access

☐ Inactive

Date Added

Last Modified

Data Fields 5-50

<Prev

Next >

Finished

Sync Template

Powered by Galaxy Control Systems

◀ Additional Fields screen

- 8. If **Record Type** droplist is available/unlocked in your system, you can choose the appropriate option.
- 9. The User can enter the **Personnel Data** as required by administrative policy, such as email, address, home phone, etc.
- 10. The User can also enter data into the **Data 1, 2, 3, and 4** fields. These extra fields are provided for the administrative needs of the client.

11. The **Inactive** checkbox should remain unchecked if you want the cardholder to be active. Checking this field will prevent the card from working at any door.

NOTICE: the *Inactive option* controls whether a Cardholder is active in the system. This is a quick way to disable all credentials for a single person. All access credentials assigned to this cardholder record will stop working if this option is checked. This does not affect credentials assigned to another cardholder record.

TIP: There are additional ways to control the activation of an access card in the system. You can configure the *active date* of an access card (credential) in the *Add Card screen*, in a later step in this wizard. You can also disable the access card, or you expire it in the *Add Card screen*.

NEXT : Do one of the following things to proceed ...

- click **Data Fields 5-50** to open more fields (opens the [Data Fields 5-50](#) window)
- click **Sync Template** button to synchronize badge templates.
- click **FINISH** button to save the cardholder now and exit the wizard (without adding a photo or access card, etc.).
- click **NEXT** to advance to the next screen (should be the [Add Photo](#) window).

Data Fields 5-50

These fields are optional or discretionary unless your administrator has configured them to be mandatory in the system.

- A mandatory field will be red and have an asterisk (*) beside it. It cannot be skipped - the screen will not advance until it is satisfied.
- You can configure optional/discretionary fields later in the *Cardholder Editor Screen* if you want to skip them now in the wizard.

NOTES

- The 50 Data fields are all discretionary fields and should always be used consistently for reporting purposes.
- Contact your administrator for questions regarding configuring Data # field names.

Adding Data in Fields 5 - 50

Data Fields 5-50

Data 5

Data 8

Birth Date

Vehicle Type

Data 44

Data 47

Data 50

Data 6

Data 9

Zodiac Sign

Vehicle Color

Data 45

Data 50

Data 7

Mother's Maiden Name

Occupation

Blood Type

Data 46

Data 49

Close

Done

50 Data Fields screen

12. When User clicks the **Data Fields** button, the *50 Data Fields Screen* opens.
13. The User can enter data into any of the Data 5-50 fields. These extra fields are provided for the administrative needs of the system subscriber.

NOTE: The system does not impose rules on these fields unless the integrator has configured them to work a certain way (i.e. as a droplist or as a mandatory field). Be careful to use these fields in a consistent way for reporting purposes.

14. Click **CLOSED** or **DONE** to save your changes.
(this returns user to the *Cardholder Information Screen*.)
15. From the Cardholder Information window, click the **NEXT** button to advance to importing a photograph.

Add a Photograph

The **main photograph** is typically used for ^(A) printing a Photo ID Badge or ^(B) using the Photo Identification/Verification feature.

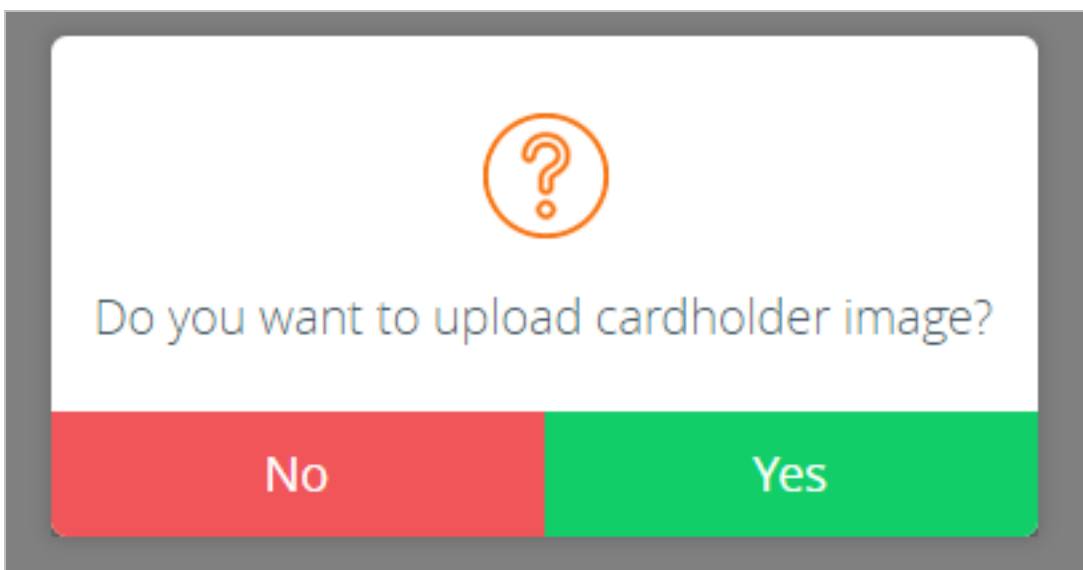
Adding a main photograph is optional. You can save the Cardholder enrollment without it unless the Sys-Admin has made it mandatory.

You can add the photograph later in the *Cardholder Editor screen* if you need to skip adding it in the Express Add or Cardholder Wizard screens.

NOTES

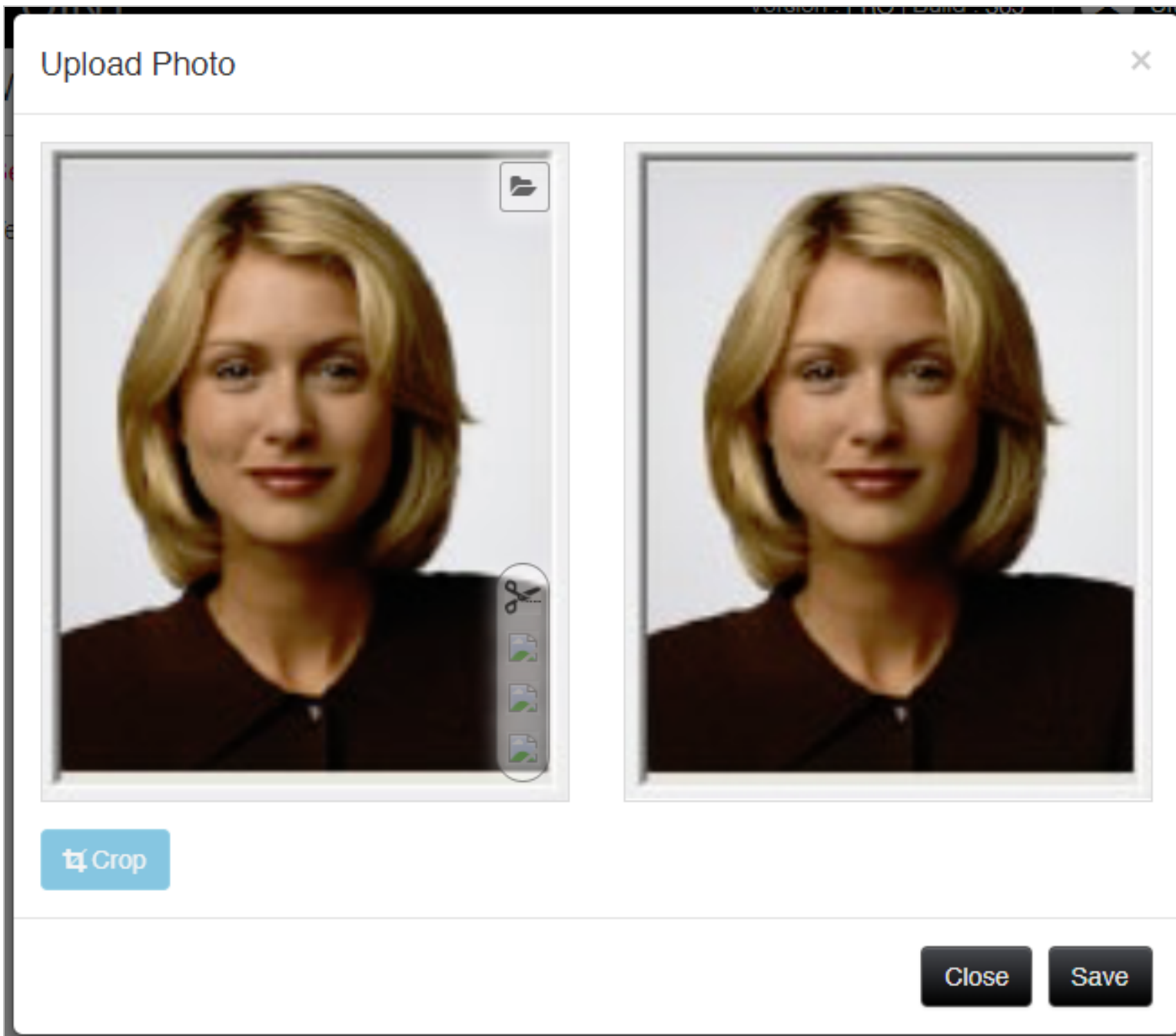
- You must already have captured the photograph you wish to upload.
- The photograph file must be in a folder location that the SG User has permission to access.

Adding a Photograph



[Add Photo Y/N message](#)

box



< Upload Photo screen

16. LaunchPoint will open a message box : *"Do you want to upload a cardholder image?"*
 - a. Click **NO** only if you want to skip adding a photograph.
 - b. Click **YES** to add a cardholder photograph;
The Import Photo Screen will open showing two empty frames.
The left frame is used to import and crop the photo.
The right frame will hold the finished photo after the user crops the desired area of the image
17. Click the Folder icon to browse to the desired photograph file. The folder icon is in the upper corner of the left frame.
18. When the photograph is loaded into the frame, the user will see some overlay controls.

The user can zoom-in or zoom-out by using the overlay controls.

The user can also *click-n-drag* the photograph to adjust the position of the photo within the frame.

19. Click the **CROP** button to create the official cardholder photo image. The photo image will pop into the photo frame on the right side.
20. Click **SAVE** button to save your changes and advance to the *Add Access Card Screen*.

Add Access Card

This step is required to create a valid access card.

- If you are not ready to assign an access card right now, you can **SKIP** this section or Exit the wizard.
- If you do not save card data, you can simply use to the Add Card Wizard to add the card later.
- If you have at least saved the first and last name of the cardholder, the cardholder and any saved programming will be in the system. This can be found from the Cardholder List (cardholder editor) screen.

NOTES

- You must correctly enter the **Card ID Code** and any facility code or company code needed for the card to work correctly.
 - You can set a **Future Activation Date** if you don't want the card to be active immediately.
 - The **Disable Card** checkbox will disable only the card you are programming and will not affect other cards on the same cardholder.
-

Access Card Data

Add Access Card

Card Description

Card 1

Card Technology

26 Bit Wiegand

Facility Code

99

ID Code

5047

PIN / Additional Information

☐ Card Disabled

Badge Design

Select

☒ Additional Fields

☐ Card Reversed
☐ PIN Exempt
☐ Duress Enabled
☐ Passback Exempt
☒ Active Date

02/28/2019 9:13 PM

Card Role

Access Control

Dossier Design

Select

Expire Mode

No Expiration

Skip

Sync from Reader

Next

◀ Add Card Data screen

21. Enter the **Card Description** if desired - (*recommend using default system description*)
22. Select the appropriate **Card Technology** such as 26bit Wiegand.
23. Enter the **Card Code**, including ID Code and Facility code as appropriate for the technology type.
24. Enter **PIN Code** if applicable.
25. (optional) Check the **Additional Fields** checkbox if you need to change the card role or set the active or expire date for the card.
26. (default) Select the correct **Card Role** of the card. (access card is default; set to alarm card if needed.)
27. (optional) Set the future **Activation Date/Time** as appropriate.
28. Set the **Expiry Mode** as appropriate and choose the appropriate value for the expiration.
29. Select a **Badge Template** for the cardholder. (only used if you are printing ID Badges)
30. Select a **Dossier Template** as needed. (only used if you are printing Dossiers)
31. Click **NEXT** to advance

Choose a Locations (Clusters)

This step is required to create a valid access card.

If you are not ready to assign access privileges right now, you can exit the wizard. However you must complete the task of assigning access privileges later in the Cardholder Editor. See [Editing Cardholder](#) For More Information.

IMPORTANT

- You must choose at least one Location.
 - You can choose multiple Locations as desired.
 - You can also add more locations later in the Cardholder Editor screen.
-

Choosing an Access Location

Select Location to Grant Access

Accounting Offices

East Parking Entrance

Lobby / Front Entrance

General Access

Back

Skip

Next

< Select Location

screen

- 32. Select a Location (or multiple locations by clicking and holding the control key while clicking more Locations.)
- 33. Click the Next button to advance.

Assign Access Permissions

This step is required to create a valid access card.

If you are not ready to assign access privileges right now, you can exit the wizard. However you must complete the task of assigning access privileges later in the Cardholder Editor. See [Editing Cardholder](#) For More Information.

TIP: The best way to work through assigning the access rules is to select each authorized loop (one at a time) and set up its access rules. Then set up the next Authorized Loop, working in turns until they are all configured.

IMPORTANT NOTES

- You must have already created the Access Groups before you can assign them.
- You must assign at least one Authorized Loop (Location) to the card for it to work.
You can assign multiple Authorized Loops (Locations) to the card/credential.
- You must assign at least one Access Group to an Authorized Loop for it to work.
You can assign multiple Access Groups to a selected Location (Authorized Loop).
- Assigning "no access" to all access groups will disable the access permissions for that Location/Loop.
- If you assign "unlimited access" to any group on a Location/Authorized Loop, the card will have access to all doors on that loop, all the time (24/7).

Assign Access Permissions (per Loop)

assign access permission to card

Access Profile

Authorized Loops

Accounting Offices

Access Group 1

Weekdays 8 - 5

Access Group 2

** NO ACCESS GROUP **

Access Group 3

** NO ACCESS GROUP **

Access Group 4

** NO ACCESS GROUP **

Back

Skip

Next

Assigning Access Permissions screen

Message

Add another card?

No

Yes

Add Another Card ? - Y/N message box

✓

Cardholder saved successfully

Close

Successfully Saved confirmation message

33. Select the first **Authorized Loop** that you want to configure. If you have multiple Loop-Clusters chosen for this card, you will configure them separately.

TIP: the Authorized Loop field is beneath the Access Profile field.

34. Assign the Access Permissions by assigning an **Access Group(s)** as needed. The access rules you assign here are associated with the selected Authorized Loop, and will be applied to the access card. Now your new card will have access to the selected loop for the days/times covered in the access group(s).

TIP: You can assign multiple Access Groups to the card for the selected Authorized Loop.

35. Repeat steps 35 and 36 for each additional Authorized Loop until you have them all configured.
36. Click the **Next** button when you are sure you have finished the card access assignment.
37. LaunchPoint will ask if you want to add another card.
If you click YES, you will return to the Add Card screen.
38. Click **NO** when you do not want to add any more cards.

LaunchPoint will automatically save the Cardholder record.

39. Click **CLOSE** to acknowledge the save confirmation.

At this point you have enrolled the cardholder. And if you entered photo, card data, location, access permissions, that data also has been saved.

If you skipped any information, you can open the Cardholder List to search for your new cardholder and finish editing the cardholder record - like adding a badge or printing a badge.

See Related Topics

[Add Card](#)
[Cardholder Look-up](#)
[Add Access Group](#)
[Add Time Schedule](#)
[Other Features](#)

Adding a Card

This topic covers adding a **new access card** to an existing cardholder and assigning access permissions.

The **Card Wizard screen** is no longer a stand-alone wizard screen on the Dashboard Tile.

The Card Wizard will seamlessly open when the Operator selects the option (button) to “Add Card”.

Adding a Card is now an embedded function within the **Cardholder Editor**, the **Express Add**, and the **Add Cardholder** feature.

- The **Add Cardholder** wizard allows the operator to enroll multiple access cards while enrolling a new cardholder.
- The **Cardholder Editor** allows the operator to enroll multiple access cards on an existing cardholder record.

- The *Express Add* screen allows the operator to enroll only one access card while enrolling a new cardholder. (This screen does not use the Card Wizard function.)

See Cardholder Enrollment Topics

- Add Cardholder Wizard
- Express Add (NEW)
- Cardholder Editor

See Other Related Topics

- Access Group Wizard
- Time Schedule Wizard
- Other Features
-

Add Access Group Wizard

TASK: Adding or creating a new Access Group with authorized doors and assigned time schedules.

featured topics

- About Access Groups
- Open the Add Group Wizard
- Add a New Access Group

See Related Topics

- Add Card
- Add Cardholder
- Cardholder Look-up
- Add Schedule
- Edit Access Groups
- Other Features
-

About the Access Group Wizard

The Add Access Group Wizard allows the user to choose the *doors* and *time schedule* that controls access cards.

- Proceed with **Add Access Group Wizard** (this topic) to add an access group to the system.
- To learn more about how access groups work, see [Editing Access Groups](#).

PREREQUISITES & NOTES

- The **Time Schedules** you need to assign must be created before you add the Access Group.

IMPORTANT - AVOID CREATING OVERLAPPING OR CONFLICTING ACCESS PRIVILEGES: [MORE ...](#)

This happens when **two or more access groups** (on the same card) **contain the same door but used a different schedules**. The access control system will automatically grant/deny access to the earliest time schedule that authorizes - which might be different than you intended. In this way you could grant access to a door at a different time that you intended because the door belongs to multiple access groups.

This is known as overlapping access privileges. *For example: If access group 1 is inactive at 6am, but access group 2 is active at 6am, the card will be granted access. Also if a door is unauthorized in access group 1, but authorized in access group 2, the system will grant access.* **THE SYSTEM WILL GRANT ACCESS ...** Be aware that the system will grant access to any authorized door if any access group on the card has an active schedule when the card is presented to a reader. Conversely, be mindful of only partially removing access by removing only one of the overlapping access groups. The system will still grant access for the remaining groups. It may be undesirable to allow overlapping access permissions on a card. Consider creating a new access group with the specific access the cardholder needs.

IMPORTANT - ABOUT UPDATING PANELS: Online panels should be updated when the access group is saved (or deleted from the system). **OFFLINE PANELS ...** continue using the known access rules until the panels are brought back online and loaded with the new changes. After the data is loaded to the panels, all changes are effective for associated cards.

OPEN THE WIZARD

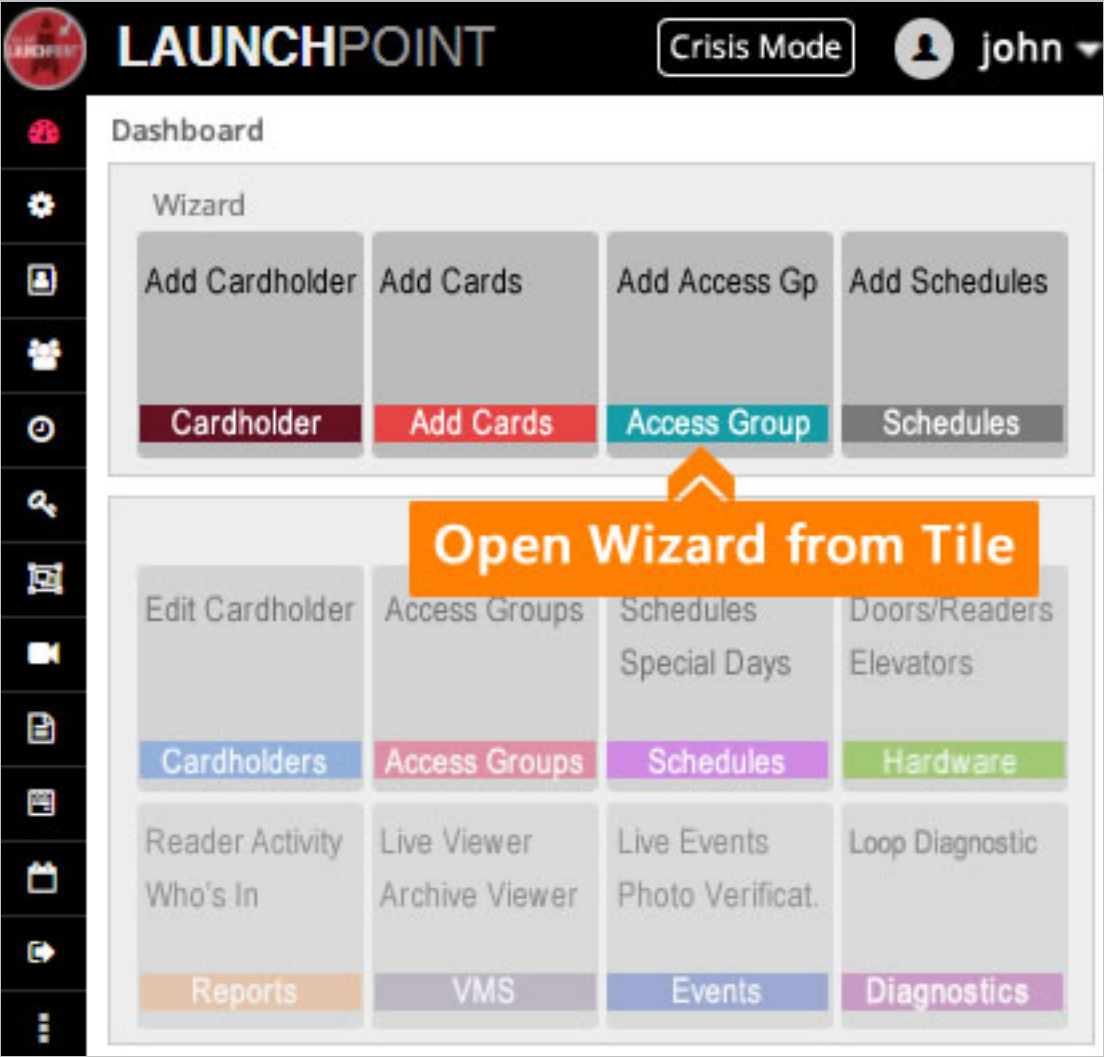
To open the Access Group Wizard ...

- Go to the *Dashboard screen* and click the Add Access Group tile, under the Wizard section.
- Or open the *Access Group screen* from the left side Menu, and click **Add New** button to launch wizard.

Click on thumbnails to open and close them.




◀ Access Group menu icon



← LaunchPoint Dashboard

(thumbnail)


LAUNCHPOINT
Version : PRO | Build : 305
click to close X
SG OPERATOR

Access Group Wizard

Select Loop or Cluster *


Access Group Name *

☒ Additional Fields

Access Group Number
 ☐ Extended Group


Select Crisis Mode Access Group

Notes

Activation Date &Time
 

Comments

Service Comments

Expiration Date &Time
 

☐ Access Group Disabled

<Prev Next > Finished

Powered by **Galaxy Control Systems**

[← Access Group Wizard screen](#)

ADDING AN ACCESS GROUP

This section describes adding a new access group using the *Access Group Wizard*. If your access group already exists, use the [Access Group Editor](#).

See Related Topics

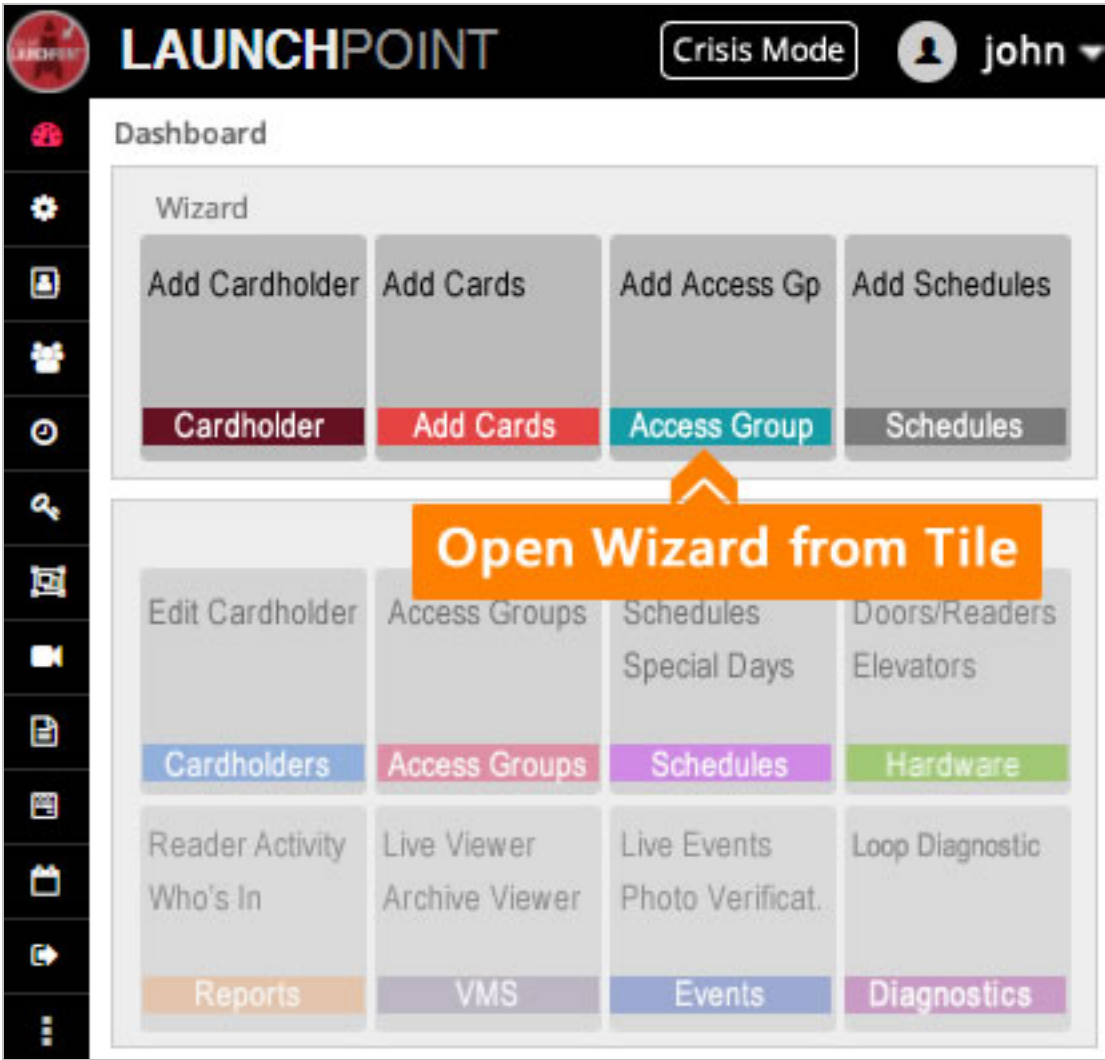
- Look-up a Cardholder
- Access Group Editor
- Time Schedule Wizard
- Other Wizards
- Other Features

STEPS

- To open the Access Group Wizard ...
- a. Go to the *Dashboard screen* and click the Add Access Group tile, under the Wizard section.
 - b. Or open the *Access Group screen* from the left side Menu, and click Add New button to launch wizard.
- Click on thumbnails to open and close them.




Access Group menu icon




LaunchPoint Dashboard

(thumbnail)



**LAUNCHPOINT**

Version : PRO | Build : 305

[click to close](#) **X**

 **SG OPERATOR**

Access Group Wizard

Select Loop or Cluster *	Access Group Name *	
<input type="text" value="CC Test Environment"/>	<input type="text" value="General Hours"/>	
<input checked="" type="checkbox"/> Additional Fields		
Access Group Number	Notes	
<input type="text" value="2"/> <input type="checkbox"/> Extended Group	<input type="text" value="Administrative notes about the access group placed here."/>	
Select Crisis Mode Access Group		
<input type="text" value="** NO ACCESS GROUP **"/>		
Activation Date &Time	Comments	Service Comments
<input type="text"/> 	<input type="text" value="Enter Comments here."/>	<input type="text" value="Enter Service Comments here."/>
Expiration Date &Time		
<input type="text"/> 		
<input type="checkbox"/> Access Group Disabled		

<Prev

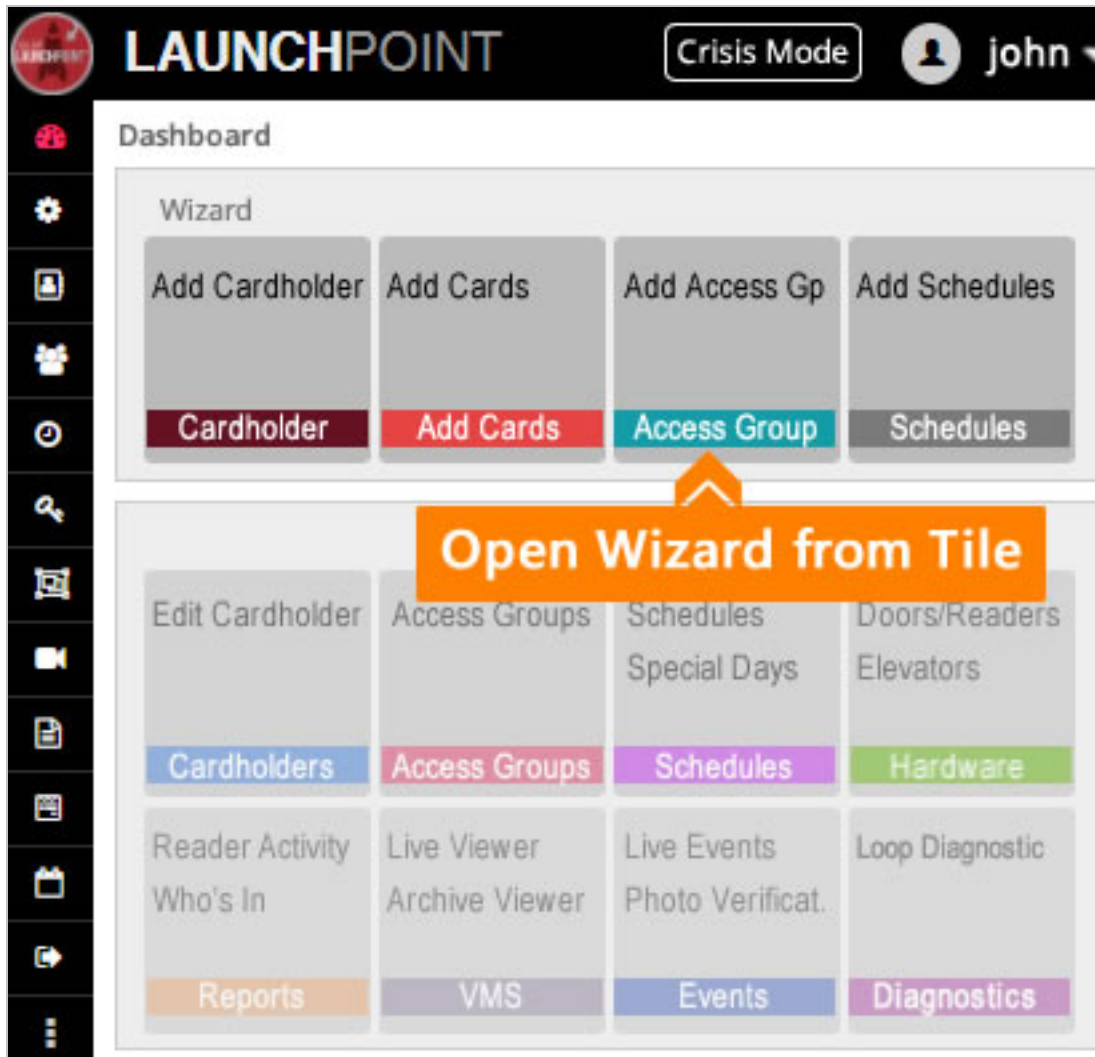
Next >

Finished

Powered by **Galaxy Control Systems**

◀ Access Group Wizard screen

1. Open the Access Group Wizard by clicking on Add Access Group Tile.



2. Select a **Loop/Cluster** that you want to add an Access Group to.
3. Enter an **Access Group name** - (mandatory) create a name that is logical.
4. Click the **Additional Fields** checkbox- shows/hides additional fields.
 - When checked, the **Additional Fields** show.
 - When unchecked, the **Additional Fields** are hidden.
5. **Access Group Number** - system assigned number - is assigned when user enters the name.
6. Set the **Crisis Mode Access Group**- this affects how all the doors on the Loop behave during crisis mode.
7. Set the **Activation Date/Time** - sets a future activation date for the access group.

Note: The card will not work in the system until the date elapses. All associated cards are impacted.
8. Set the **Expiration Date/Time** - sets a future expiration date for the access group.

Note: It will not work in the system after the date elapses. Associated cards are likewise impacted.
9. **Notes, Comments, and Service Comments** fields - enter information at user discretion.
10. **Extended Group** checkbox - set this only if you want an *extended access group*.

- When checked, the access group is treated as an extended group.
 - When unchecked, the access group is treated or behaves as a normal group.
11. **Access Group Disabled** checkbox - typically this is only used to disable an access group without deleting it.
 - When checked, the access group will not work in the system (or will stop working).
 - When unchecked, the access group will work in the system.
 12. Click the **NEXT** button to advance the wizard screen.
 13. Choose (click) a door in the *Unauthorized List* that you want to assign.
 14. Click the **Edit Schedule** link in the *Action column*.

Result: This unlocks the 'Time Schedule' column so you can choose a schedule to assign to the selected door.

15. Select a **Time Schedule** for the Reader/Door.

PREREQUISITE: The desired Schedule must already exist - See the [Add Schedules Wizard](#) if you need to create a schedule.

16. Click **SAVE** in the *Action column* to link the schedule to the door/reader.

Result: This will move the door into the *Authorized Readers List* and link it to the chosen schedule.

NOTE: This access group will only grant valid access to the "authorized" doors only during "active" (green) time periods** of the linked schedule.

NOTE: Cards never have access to *unauthorized doors***. And cards do not have access to *authorized doors* during "inactive" (gray) time periods**.

***IMPORTANT - OVERLAPPING ACCESS RULES ***: Remember if any doors in this group are also members of another access group and both groups are assigned to the same card, then the system will grant access to the overlapping doors during the active times of either schedule. Meaning if one group starts active access at 8 am and the other group gives access at 6am - the card will have access starting at 6am because of the "overlapping schedules".

17. Repeat the steps above for each Door/Reader until you are satisfied with your choices.

Result: Doors that do not have a schedule will remain in the unauthorized list.

18. Click **FINISH** button to save the Access Group.

The browser may prompt you to confirm leaving the screen - say OKAY.

19. LaunchPoint will return you to the [Access Group Editor](#) screen where you can preview your new Access Group.
20. Note Clicking the **Add New** button lets you start another access group.

MODIFYING OR DELETING AN ACCESS GROUP

If you need to modify or delete an access group, use the [Access Group Editor](#).

See Related Topics

- Add Card
- Add Cardholder
- Cardholder Look-up
- Add Schedule
- Edit Access Groups
- Other Features

Add Time Schedules Wizard

TASK: Adding a new Time Schedule with or without special days.

FEATURED TOPICS

- About Schedules
- Open the Schedules Wizard
- Add a Time Schedule

See Related Topics

- Add Card
- Add Cardholder
- Cardholder Look-up
- Add Access Group
- Edit Time Schedule
- Other Features

About Time Schedules

This topic shows you how to add a new Schedule using the Add Schedules Wizard.

NOTE: If you already added the schedule you can use the [Schedule Editor](#) to make changes.

TERMS:

Time Schedule: a *Time Schedule* is a set of incremental *time periods* that cover a 24-hour period, which are configured to be *active* or *inactive* (green vs. red/gray) at specified times. **MORE:** a *schedule's* time periods can be divided into *15-minute intervals* (or *1-minute intervals*), depending on the format chosen for the loop/cluster). These incremental *time periods* are either active (green) or inactive (red/gray). And when a schedule is assigned to a card, they control when a

card/credential is granted or denied access to the 'authorized doors' that belong to the access group. Once a *Schedule* is created, it can be assigned to any door within an access group, or elsewhere in the system to door groups, i/o groups, ...

Custom Schedule: is a *Time Schedule* that is created by the system admin or user, which defines the *active* and *inactive* time periods. **MORE:** Typically 'active' means unlock/grant access and 'inactive' means lock/deny access.

System Default Schedule: is a predefined *Time Schedule* in the system for default use. There are two predefined *Time Schedules*; i.e., "***Always***" and "***Never***". **MORE:** "Always" means all time periods are active/on (green). "Never" means all time periods are inactive/off (red/gray).

Time Format: is a configurable system-level setting that defines the *default system size of the time periods* into '15-minute intervals' or '1-minute intervals'. The time format is an administrative setting of the loop/cluster programming. All panels in a loop/cluster will use the same time format.

Crisis Mode Schedule: is simply the *time schedule* that is assigned to the crisis mode field in any part of the system programming - including Access Groups, door groups, and i/o groups - which the system will use during an 'active crisis mode'. **MORE:** The crisis schedule can be a *custom schedule* or use one of the *default system schedules* ("always" or "never").

Special Day (Holiday): a specified day when the *doors are not unlocked* or *access is not allowed*. It is a specified day/date on the calendar that is treated differently than a "regular day" - such as a holiday or special observance. A special day might affect a *half day* or a *whole day* or make any other *exception* to the regular day or normal hourly schedule when the doors do not open or access is not allowed.

Process Overview

- A. First you will create the schedule(s) you need for the access permissions (this topic).
- B. After the Time Schedule is saved, you can assign the schedule to Access Groups in the [Access Group Wizard](#) (or the [Access Group Editor screen](#)). Access is granted to authorized doors in the group.
- C. And when the Access Group is saved, you can assign the access group to an Access Card in the [Add Card/Add Cardholder](#) wizards; or in the [Cardholder Editor](#) screen if the cardholder already exists.

How Schedules Affect Access

Schedules determine when a card has access to a door. The system will grant access during the green/active hours of the schedule.

NOTE: A card will not be granted access during inactive portion of the schedule.

Special days can be added to the schedule that will cause the schedule to behave differently than normal days. Special days are configured by the system administrator - i.e. full day, half day, etc.

When creating an access group, you can only assign one schedule to a door. However, there can be multiple doors in the access group, so you can assign a different schedule to each door. Likewise, you can assign the same schedule to every door in the group. Or you can mix and match, so to speak, perhaps some doors have the same schedule and some doors have different schedules. You can also omit some doors in the access group by simply not assigning a schedule to the door, which means the door is not authorized.

When you assign an access group to a card, you are giving the cardholder permission to access all the "authorized" doors in the group, during the "active" days and times are in the assigned schedules.

When is access granted and denied (things to check)?

Access is granted if all these things are true ...

- the access card is a valid card (card is active/not expired and not deactivated).
- the card is presented to an authorized door/reader (in the access group).
- the card presented during its active schedule (in the schedule assigned in the access group").
- the cardholder is active (not inactive in cardholder information screen)

Access is denied if any of the following things are true ...

- the card is presented at the wrong door/reader (access group programming or access permissions in cardholder editor)
 - the card is presented at the wrong time/wrong day (access group or schedule programming)
 - the card is not activated, or is expired, or has reached a usage limit
 - the card is deactivated (checkbox)
 - the cardholder is inactive in the system (inactive checkbox)
 - the card is not in the system (not enrolled)
-

OPEN THE SCHEDULES WIZARD

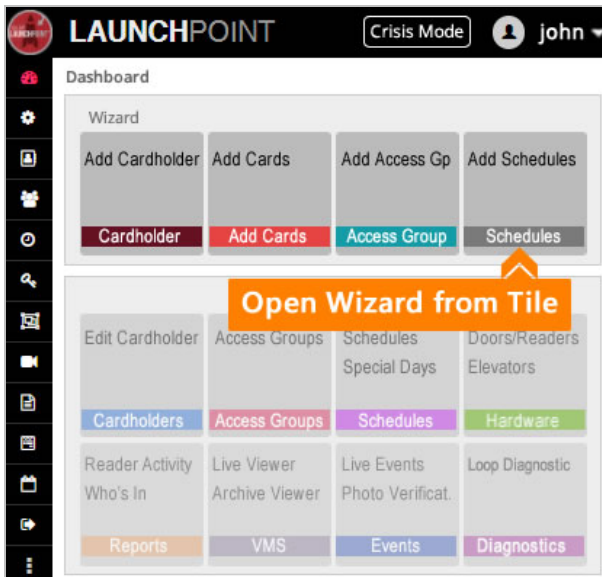
There are two ways open the Time Schedules Wizard ...

- a. Go to the ***Dashboard*** and click the **Add Time Schedules**, under the Wizard section.
- b. Or click **Add New** button from the ***Time Schedule Editor*** (opened from the left side Menu. You might prefer this method if you need to search for the schedule to see if it is already added.

[Click on thumbnails to open and close them.](#)



◀ Schedule Wizard icon (system default)



◀ LaunchPoint Dashboard

LAUNCHPOINT Version : PRO | Build : 305 UMBRELLA_CORPORATION

Time Schedules

Select Loop or Cluster

CC Test Environment

Time Schedule Name *

Regular Hours

Time Schedule Number

7 ☐ Schedule is effected by Special Days

Save

Sunday

Morning Evening

12am 1am 2am 3am 4am 5am 6am 7am 8am 9am 10am 11am 12pm 1pm 2pm 3pm 4pm 5pm 6pm 7pm 8pm 9pm 10pm 11pm

Monday

Morning Evening

12am 1am 2am 3am 4am 5am 6am 7am 8am 9am 10am 11am 12pm 1pm 2pm 3pm 4pm 5pm 6pm 7pm 8pm 9pm 10pm 11pm

Tuesday

Morning Evening

12am 1am 2am 3am 4am 5am 6am 7am 8am 9am 10am 11am 12pm 1pm 2pm 3pm 4pm 5pm 6pm 7pm 8pm 9pm 10pm 11pm

Wednesday

Morning Evening

12am 1am 2am 3am 4am 5am 6am 7am 8am 9am 10am 11am 12pm 1pm 2pm 3pm 4pm 5pm 6pm 7pm 8pm 9pm 10pm 11pm

Powered by Galaxy Control Systems

◀ Time Schedule Wizard screen

ADDING A TIME SCHEDULE

See [Opening the Wizard](#) above, if needed.

See [Schedules Editor](#) to modify an existing schedule, if needed.

1. Click the **ADD NEW** button to launch the wizard.
2. Select the **Loop/Cluster** (Location) that the Schedule will belong to. **NOTE** a schedule is only available for the loop you choose. it will not appear in other loops. you must make the schedules you need for each loop.
3. Enter an **Schedule name** - (mandatory) enter a name that is logical.

4. If the schedule is affected by **Special Days**, check the Special Days checkbox.
5. Click on the **Time Period** bars for each day of the week that you want to set active hours.
"Active" time periods are green, while inactive times are gray.
6. Click on the **Special Days (Holiday Types)** for each type you want to configure. You do not have to add special days.
7. Click the **SAVE** button to save the new schedule.
8. You can now assign the schedule to an access group.

See [Add Access Group Wizard](#) to use this schedule in a new access group.

See [Access Group Editor](#) to add this schedule to an existing access group.

NOTE: Clicking the **DELETE** button will delete a schedule.

See Related Topics

Add Card
Features

Add Cardholder

Cardholder Look-up

Add Access Group

Edit Time Schedule

Other

LaunchPoint Features

LaunchPoint **Features** include configuration *editors*, *viewers* (monitoring pages), *reports*, and *user commands*.

FEATURES BY CATEGORY

EDITORS (System Programming)

[Access Groups](#)

[Cardholders & Cards](#)

[Express Add \(NEW\)](#)

[Schedules & Holidays](#)

[Door Properties](#)

VIEWING & MONITORING (Live/Archived)

[Alarm Handling \(Live\)](#)

[Event Monitoring \(Live\)](#)

[Loop Diagnostics](#)

[Photo Verification](#)

[View Video \(Live/Archived\)](#)

CONTROL HARDWARE

[Doors/Reader Control](#)

[Elevator Floor Control](#)

(Also see User Commands - below)

SYSTEM REPORTS

[Reader Activity History](#)

[Who's In \(Muster\)](#)

[Scheduled Reports \(Cardholder List\)](#)

OPERATOR COMMANDS

[Crisis Mode](#)

[Card Count \(Diagnostics\)](#)

[Cardholder Properties \(Events\)](#)

[Disable Cardholder \(Events\)](#)

[Forgive Passback \(Events\)](#)

[Pulse Doors & Unlock/Lock Doors](#)

[Pulse Elevator Floors & Early On/Off](#)

* Licensing may apply for some features. Contact your authorized dealer for assistance.

Cardholders Search & Enroll

Using the Search Panel

Task: Use the **Search Panel** to find an existing cardholder in the system. This is done by opening the *Cardholder List*, and entering search criteria into the Search Panel that will retrieve the desired cardholder record(s).

[How the Search Panel Works](#)

[How to Control Search Results](#)

[Using the Search Panel](#)

How the Search Panel Works

The *Search Panel* provides several different search filters to narrow your search results.

Searches are controlled by two fields - i.e., the **Search Criteria droplist** and the **Search Value field**. The user can simply select the Search Criteria and enter a search value.

- The **Search Criteria droplist** - allows the user to choose the method of the search and controls the format of Search Value field
- The **Search Value field** - allows the user to enter the value for the chosen Search Criteria; such as *text value* for cardholder name, or a droplist of system-defined options, so you can pick the exact value in the system.

The following Search Methods are the available ...

- A. Retrieve the **Unfiltered Cardholder List** by clicking **Search** without any criteria.
- B. Find a **Cardholder By Name** (default) - returns only the cardholder records that meet the criteria given.
- C. Use **Advance Search** to filter cardholders by unique criteria - returns only the cardholder records that meet the criteria given.
- D. Use the **A-Z Index Tabs** on the right edge of the Cardholder List to pop to a specific location in the cardholder list.

PREREQUISITES

- The Cardholder must already exist. Using the Search Panel you can determine if a cardholder record already exists.
 - The data criteria that you search for must be valid and really configured in the cardholder you are seeking. **FOR EXAMPLE** if a department was never assigned, then you must use a different criteria because department will never pull back that cardholder. Also consider, if the cardholder was assigned to a different department than you expect. Or if a cardholder name was misspelled, you must try different spellings, or simply choose a criteria you will know.
 - The LaunchPoint user/user must have the privileges to view, edit, and save changes in the cardholder screen.
-

How to Control Search Results

The Search Panel provides several ways to control your search results.

You can query the database to find one cardholder or a group of cardholders that meet your criteria.

INCLUSIVE MATCH

The Search Panel uses the "inclusive match" method. This means the result-set will include one or more records that match your criteria and will exclude every record that does not meet the criteria.

Each search method is effective in different ways.

1. **All Cardholders** (unfiltered) - this method returns the entire list of cardholders - i.e. by clicking Search without entering criteria.
(The results are unfiltered. You will use the scroll or the A-Z Index to locate your cardholder.)
 2. **Name Search Criteria** (default) - this method filters the cardholder population by First Name or Last Name as the search criteria.
-

(The results will include/exclude cardholders with alternate spellings or similar names depending on what Search Text you enter.)

3. **Advance Search Criteria** - this method refines search results by a unique criteria.
(The system will cull out cardholder records that meets the unique criteria).
4. **A-Z Index** - this feature lets you find a cardholder in a large result-set by clicking the letter on the A-Z Index strip that the name starts with.
(Use this to locate a record when the search yields a large result-set of dissimilar names. This is useful when search efforts fail because the name is misspelled or the criteria is unknown. Sometimes it is easier or faster to pull back the entire cardholder population)

All Cardholders - Unfiltered Results

The Search Panel allows you to retrieve the entire cardholder records by clicking the **SEARCH** button without entering any criteria. Once you retrieve your results, you can use the *scroll-bar* or the *A-Z Index strip* to navigate your results.

RESULT: The system will return the entire cardholder population.

PROS: It might be the fastest/easiest way to find your cardholder when you have a small cardholder population - or other methods failed.

CONS: If you have a very large cardholder population, the system may take some time to populate the Cardholder List page.

Name Search Criteria

By default, the Search Panel provides a Search Criteria droplist with two criteria - i.e. First Name and Last Name.

RESULT: The system will return only the records that match the name provided in the Search Text field.

PROS: You can easily find a cardholder by name without retrieving the entire list. Widening your results will catch similar spellings.

CONS: Narrowing the search criteria too much will omit names that use an alternate spelling and possibly misspelled names.

TIP: To ensure your success, similar or varied spellings need to be considered when providing the Search Text.

Examples of Name Search Criteria

To narrow your results, enter more letters. The more letters you enter, the more narrow your results will be.

To widen your search results, enter fewer letters. This can catch alternate spellings.

EXAMPLES ...

- Entering "Johnson" will greatly narrow the results to people named Johnson; but it omits alternate spellings Jonson, Johnston or other names Johnathan.
- Entering "J" greatly widens the results to all names starting with J. This could be a big list.

- Entering "John" will narrow results to John, Johns, Johnson, Johnston, Johnathan; but still omits alternate spellings Jon, Jonathan, Jonson.
- Entering "Jo" will widen the search to catch alternate spellings of John, Johnathan, Johnson, plus Jon, Jonathan, Jonson, as well as other names such as Joseph, Joshua, Joel, Jones.

Advance Search Criteria

The Search Panel provides an Advance search criteria checkbox. This option fills the Search Criteria droplist with a list of different criteria, such as card code, department, etc. so you can use a different piece of information, such as the department they belong in.

Reasons to use this method:

- You might need to find any and all cardholders who fit a certain criteria - such as those in a certain department, or hired after a certain date.
- You may not know the name or spelling of a cardholder, but you know a different piece of criteria to search by.

RESULT: The system will return only the records that inclusively match the selected criteria and the value provided in the Search Text field.

PROS: You can find a subset of cardholders who match that criteria regardless of their names.

CONS: Choosing the wrong piece of criteria could cause you to miss the record you are looking for.

TIP: To ensure your success, considered how the criteria you are using will satisfy your search goals.

How to Open the Search Panel

1. Sign-in to LaunchPoint from the Login Page if needed.
2. Click on the **Cardholder List icon**  from the Dashboard or from the side Menu.



3. The **Search Panel** is in the *Cardholder List Page*.



4. On a smaller screen-size, or when the Search Panel is hidden, click the **Yellow "Eyeglass" Tab** on the right edge of the window.


RESULT: The Search Panel will slide open.



Using the Search Panel

This section provides the basic steps to use the Search Panel.

SEARCHING BY NAME CRITERIA

1. Open the **Cardholder List icon**  from the Dashboard or from the side Menu
2. You can simply click the **[Search]** button to query all cardholders.
3. Select the **First or Last Name** in the *Search Criteria droplist*, as desired.
4. Enter the **Search Text** that meets your criteria. (see Controlling Search Results above, for assistance)
5. Click on the **Search button** to invoke the search.

RESULTS: The Cardholder List will be populated with the list of cardholders whose names match your Search Text.



POSSIBLE REASON YOUR CARDHOLDER WAS NOT FOUND ...

- you misspelled the name
(check your spelling and reenter the criteria)
- the name was misspelled when the person was enrolled
(try using a different spelling or choose Advance Search option for a different angle)
- your criteria was too narrow (you entered too many letters) and omitted record
(try entering only 2 or 3 letters in the Search Text field)
- your criteria was not effective in locating the record (try using Advance Search;
or remove all Criteria/Text and do a blank Search- then use the A-Z Index to locate the record)
- the cardholder is not enrolled (Click the Add Cardholder button to launch the Wizard - see the [Add Cardholder Wizard](#).)

See [other methods of searching](#) for more information.

Editing Cardholders

This topic covers editing the Cardholder information for an existing cardholder or card.

This is done by opening the **Cardholder List**, searching and selecting the desired cardholder, and editing the cardholder.

FEATURED TOPICS

[About the Cardholder Editor](#)

[How to Find a Cardholder](#)

[How to Edit an Existing Cardholder](#)

About the Cardholder Editor

The **Cardholder Editor** allows an *authorized* user* to change or modify the Cardholder information and Card information, including uploading a photo, assigning permissions, printing badges and more.

* The user must have permission to view and edit the Cardholder information. Permissions are configured by the system administrator.

PREREQUISITES AND NOTES

- The Cardholder must already exist in the system in order to open it in the Cardholder Editor.
- The LaunchPoint user must have the privileges to view, edit, and save changes in the cardholder screen. See system administrator as needed.
- If you want to upload a photograph, you must have captured the photo and placed the image file in the expected folder.
- If you want to assign departments, they must already exist in the Department droplist. *See system administrator as needed.*
- If you want to change access permissions, the access group(s) must already exist in the system. See [Add Access Groups Wizard](#).
- **Badge Templates:** If you intend to assign a badge template, the template must already exist in the Template droplist. *If you do not see the template, you can update the list by clicking the **Synchronize Templates** button.*
- **Preview/Print Badges:** the badge template must be assigned and saved to the cardholder before you can print or preview badges.
- Use the [Add Cardholder](#) or Express Add to add a new cardholder.
- If you did not yet add the card, you can launch the *Add Card Wizard* one of the following ways ...
 - a. Launch the [Add Card Wizard](#) from the Dashboard tile icon .
 - b. open the Cardholder List Editor (this topic), then click the **[Add Card]** button located in the *Access Card Info* section of the editor screen. *This method is useful if you need to search or look-up the cardholder record first.*

Cardholder Editor Screen

This editor allows you to modify or delete data on an existing cardholder in the system - this includes editing existing cards already added to the cardholder and their access privileges, ID badge assignment, Badge Preview and Printing, and more.

TIP: You can open the Cardholder Editor from the Cardholder List after you search and find your cardholder.

Supported Functionality

In the Cardholder Editor, you can do the following things

1. manage cardholder information
 - a. modify cardholder first, middle, last name, DOB, etc
 - b. modify personal information (phone, address, etc.)
 - c. modify department
 - d. disable cardholder record (this keeps cardholder activity/card activity in tact)
 - e. 50 data fields (discretionary unless configured by sys. admin. to be mandatory)
2. upload a main cardholder photograph
 - a. upload or replace the main photo
 - b. crop or reposition photo image
 - c. the main photograph can be added to the Badge ID Template
 - d. the main photograph is also used for Photo Identification feature
3. manage access card credentials
 - a. launch the Add Card Wizard from the Editor screen
 - b. modify / disable / delete an access card *
 - c. configure activation dates and expiration modes/dates
 - d. configure card role (access vs arming)
4. manage ID Badge Templates
 - a. synchronize the ID Badge Template list
 - b. assign an ID Badge Template **
 - c. preview and print ID Badges
5. manage access privileges
 - a. assign access locations (loops)
 - b. assign access permissions (access groups)
6. print the Cardholder Activity Report ([see Reports](#))

- * You can also configure an *arming card* through the editor.
- ** You must be licensed for a badging solution and Badge Designs must be imported & synchronized.

NOTE: The *Cardholder Editor* can be configured to show or hide specific fields that the system subscriber does not want to see or use. This is handled by an authorized administrator or dealer.

Buttons and Controls

The user can use the following buttons and controls to navigate in the editor screen.

EDITOR BUTTONS - TOP OF SCREEN

Sync Template - syncs the badge template field (droplist) for the system subscriber.

Delete - deletes the entire Cardholder record.

Refresh - refreshes the screen/login.

Cancel - cancels/exits the editor and any unsaved changes are lost.

Save - saves all the pending changes in the cardholder record without closing the editor.

CARDHOLDER INFORMATION - TOP SECTION

Photograph Field (image box) - clicking on the field/image opens the Upload Photo window.

Additional Fields Section (dropdown - starts collapsed) - reveals additional Data fields (optional).

Additional Fields (checkbox) - show/hide more additional fields that are usually optional.

TIP: Using additional fields is up to the discretion of the system subscriber / administrator unless they have been designated as mandatory by the authorized dealer. Fields designated as mandatory must be non-blank for the user to advance to the next screen.

CARD/BADGE SETTINGS - MID SECTION

Add Card button - launches the Add Card Wizard (adds a new card).

Select All (cbx control) - selects all the cards for disabling or deleting. Cardholder remains intact.

Disable Card button - sets 'Disable Card' option to "checked" for selected cards.

Selected cards will remain intact, but will no longer work. This preserves card activity records.

Delete Card button - deletes all the selected cards. Unselected cards remain intact.

Delete Single Card (trashcan) - deletes the individual card. Other cards remain intact.

Preview Badge (eyeball) - opens the Preview Badge window for the individual card. You can print also.

Print Badge (printer icon) - sends the ID Badge directly to the badge printer without previewing.

Select Card (cbx control) - selects/deselects the single card

Fields in the Cardholder Editor

There are additional data fields in the Cardholder Editor that can be used to store information according to the client's needs. These data fields should be used consistently. If you use Data 1 to store the cardholder's office number or some relevant piece of information, you should always use Data 1 for the same thing in all Cardholders. This can be simplified by changing the field name (field label) to something that identifies the purpose of the field - see tip below.

TIP: The administrator can also configure the *field labels* of generic data fields and may be able to apply rules such as making a field mandatory or behave like a droplist. Contact your authorized administrator or dealer for assistance.

How to Find a Cardholder

You must open the Cardholder List to open the *Cardholder Editor*. When you open the Cardholder List, you can use the *Search Panel* if needed to find your cardholder.

There are two ways to open the Cardholder List ...


- from the *Dashboard*
- from the sidebar *Menu*.

OPENING CARDHOLDER LIST FROM DASHBOARD


1. When you sign-in, the Dashboard automatically displays. Editors are located in the Configure section on the 2nd row of tiles.
2. Click the **Cardholder List Tile** to open the *Cardholder List screen*, which includes a Search Panel.
3. You can use the Search Panel to find your cardholder if you do not see your cardholder in the list. Click the orange magnifying glass on the left side of the window to reveal the Search Panel if it is closed or not visible.



OPENING CARDHOLDER LIST FROM MENU

From the **LaunchPoint Menu** (left side), click the **Cardholder List icon**  to open the *Cardholder List screen*, which includes a Search Panel.



1. An alphabetical list of cardholders may auto-generate.
2. If you don't see your cardholder, you can use the **Search Panel** to enter criteria and narrow your results.
3. If the Search Panel is hidden, click the [yellow eyeglass]  on the right edge of screen to expand it.
4. After entering search criteria, click [Search] button to query matching cardholders.
5. See [Using the Search Panel](#) for more info.

LAUNCHPOINT Version : PRO | Build : 305 SG OPERATOR

Cardholders List Refresh

Search Option

☐ Advance

First Name

A

Abigail Aaron
Status : ✔ Active | Last Access : 📅 | Edit Delete

Record ID: 30005 Department: [08] Umbrella Corpora

Angelita M Alvarado
Status : ✔ Active | Last Access : 📅 | Edit Delete

Record ID: 12674 Department: [16] Hooli / Emplo


Angela M Adams
Status : ✔ Active | Last Access : 📅 | Edit Delete

Record ID: 13976 Department: [09] Globex Corpora

click to close thumbnail



Powered by **Galaxy Control Systems**

USING THE SEARCH PANEL

You open the **Cardholder Search Panel** by clicking on the **yellow eyeglass**  near the top-right corner .

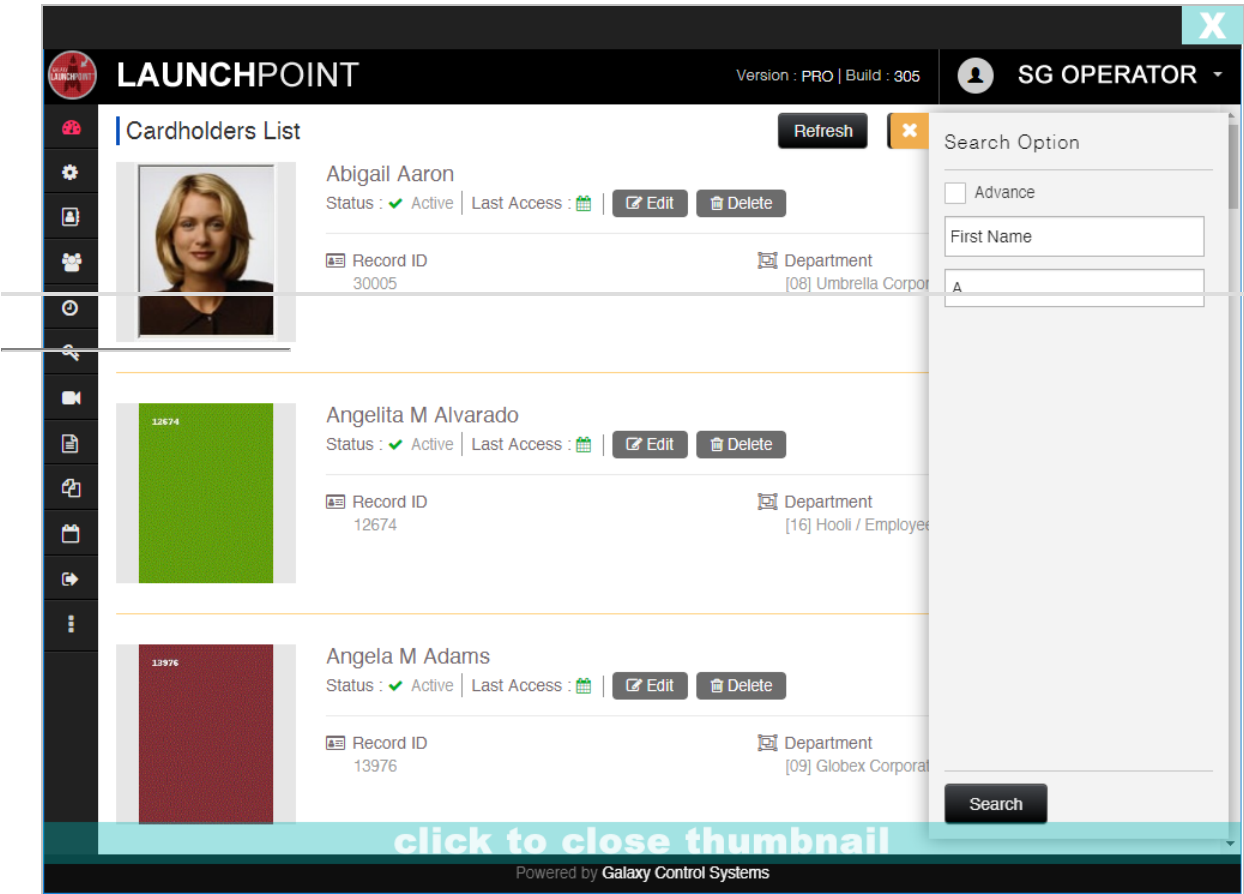
This will expand the Search Panel.



1. Click the **Cardholder List icon** , to open the Cardholder List window.
2. If the Search Panel is hidden, click the [orange eyeglass]  on the upper-right edge of screen to expand it.

Cardholder List / Search Panel
(hover/tap to open thumbnail)

3. You can simply click the [Search] button to query all cardholders.
4. You can use the **Alphabetical Index** on the right side of screen, to orient your place in the list to where you expect to see the name of your target cardholder. You need to hide the Search Panel to see the Index.
5. You can narrow your search results by entering *search criteria* using the search data fields on the Search Panel. Click [Search] button to query cardholders that match your criteria.



To see more on the Search Panel visit the [Search Panel Topic](#) .

Edit an existing Cardholder or Card

From the Cardholder List, click the Edit button to open the *Cardholder Editor* screen. See how to find your

TIP: The Edit

size

Cardholder List / Search Panel
(hover/tap to open thumbnail)

Link will change to an **Edit Button** if you shrink the screen width until it changes (screen size threshold).

TIP: If you want to delete the cardholder record, you can click the **Delete Button**, next to the Edit Button. Be aware that deleting a cardholder will also remove the cardholder activity history. To keep the history in tact, you should disable the cardholder or card in the system or at least .

LAUNCHPOINT Version : PRO | Build : 305 SG OPERATOR

Cardholder Editor Sync Template Delete Refresh Cancel Save

Cardholder Information

Last Name*	First Name*	Middle Name	Customer
Aaron	Jill		[08] Umbrella Corpora
Department	Data 1	Date Added	Last Modified
[17] Umbrella Corpora		02/14/2019 8:54 PM	02/27/2019 5:11 PM
D.O.B.	Date 1	Date 2	
02/14/1991			

> Additional Fields

> Card/Badge Settings Add Card ☐ Select All

> Activity History

Cancel Delete Save

click on photo to close thumbnail

Powered by Galaxy Control Systems

1. From the Cardholder List, click **EDIT** to open the *Cardholder Editor*.

Sync Template

syncs the Badge & Dossier Templates

Delete deletes the entire cardholder record.

Refresh refreshes the cardholder page. unsaved pending changes may be lost.

Cancel cancels all pending changes.

Save saves the pending changes on the record.

Search Icon - opens

Cardholder Editor
(hover/tap to open thumbnail)

the Search Panel.

Cardholder Editor Sync Template Delete Refresh Cancel Save





Cardholder Information

Last Name*	First Name*	Middle Name	Customer
Aaron	Abigail		[08] Umbrella Corporat

Cardholder Editor (top of screen)
(hover/tap to open thumbnail)

2. In the **Cardholder Information section** of the screen (upper half), you can modify the following data ...
- Name - first, middle, last
 - Inactive checkbox (checking this makes the cardholder inactive without deleting; keeps history intact)
 - Date of Birth (D.O.B.)
 - Date 1 and Date 2 fields
 - Select Department
 - Data 1 field
 - Photograph (needed for Photo Identification or Badge Printing)

Cardholder Information

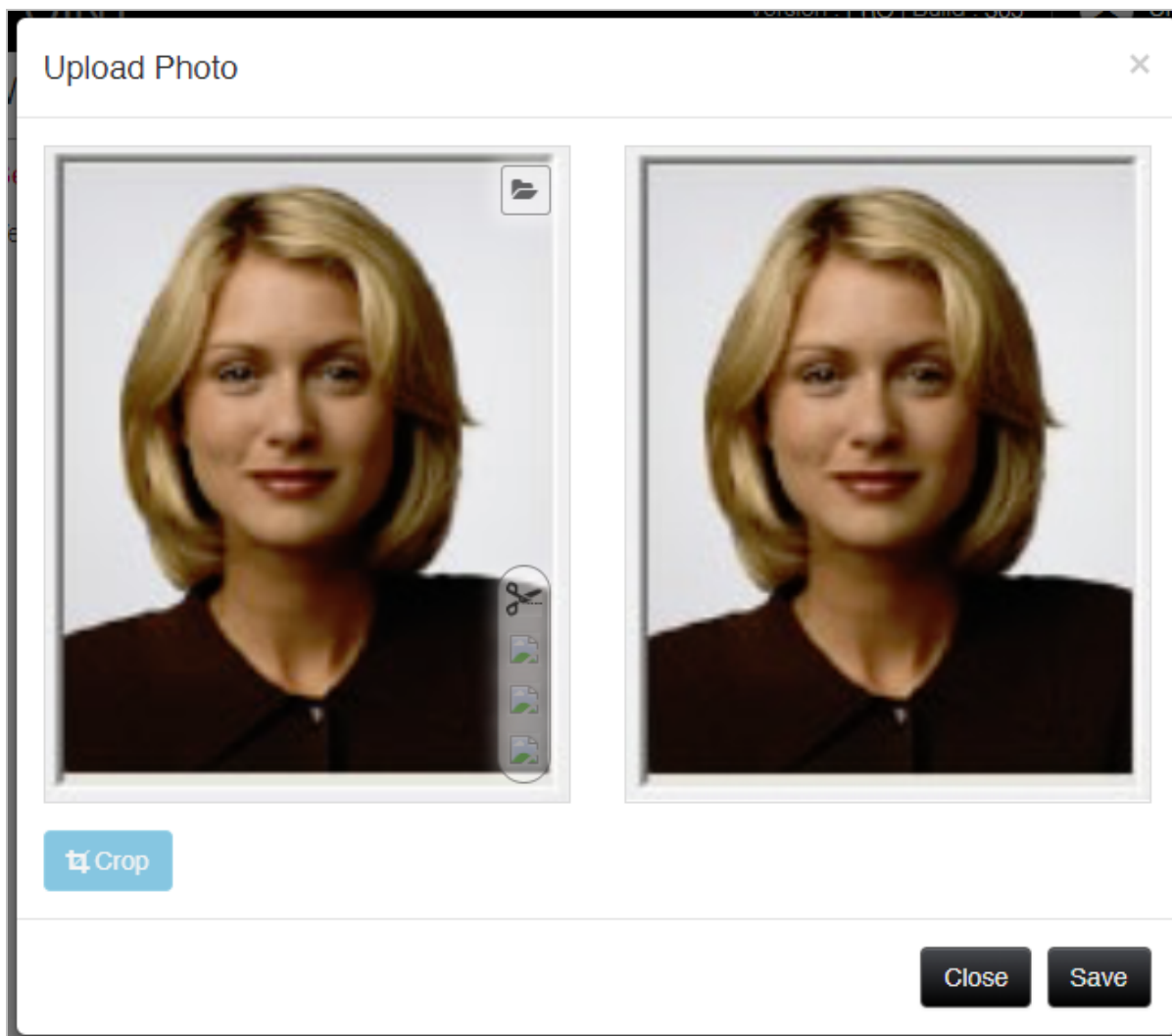
Last Name* Aaron	First Name* Abigail	Middle Name 	Customer [08] Umbrella Corporat	
Department [08] Umbrella Corporat	Data 1 	Date Added 02/14/2019 8:54 PM	Last Modified 03/18/2019 4:03 PM	
D.O.B. 03/13/2019 	Date 1 	Date 2 		

> Additional Fields

Cardholder Editor / Cardholder Information

3. Clicking on the **Photograph** field will open the **Photo Upload** screen where you can add or change the photograph.
- click on the **Folder icon** in the top-right corner of the left photo frame.
 - browse to your photo file and select it
 - you can grab the photo and reposition it, zoom in/out, ...
 - click the **Crop** button to crop and select it.

- the photo will pop to the right frame.
- click **Save** to upload the photo in the cardholder screen.



Cardholder Editor / Upload Photo
(hover/tap to open thumbnail)

4. Clicking the [> Additional Fields section](#) (expandable section) allows you to modify the following fields ...
- Personal data fields (phone, home phone, address, city, state, zip)
 - Elevator Settings (VIP, Vertigo, Has Disability, Split Group)
 - Trace Enabled (when checked the cardholder activity is set to separate color from other activity)

Cardholder Editor / Additional Info
(hover/tap to open thumbnail)

- 11

- Card Reversed cbx (reserved for special use)
- PIN Exempt cbx (exempts the card from PIN)
- Duress Enabled cbx (makes card a duress card)
- Passback Exempt cbx (exempt from passback violation)
- Active Date (set future active date for card to start working)
- Expire Mode (optional-set mode: date, date&time, usage count, none)
- Expiration Value (will match the mode, such as date or the number of usages allowed).

NOTE: You can add another Card by clicking the **Add Card** button.

* a door is 'authorized' for a card if the door is included in the **Authorized Doors List** of the assigned Access Group.

▼ Card/Badge Settings Add Card ☐ Select All

▼ Card 1 🗑️ 👁️ 🖨️ 📄

Card Description ¹² *	Card1 Technology	Facility Code *	ID Code *
Card 1	26 Bit Wiegand	99	5047

PIN1 / Additional Information

☐ Card Disabled

Access Profile

Badge Design

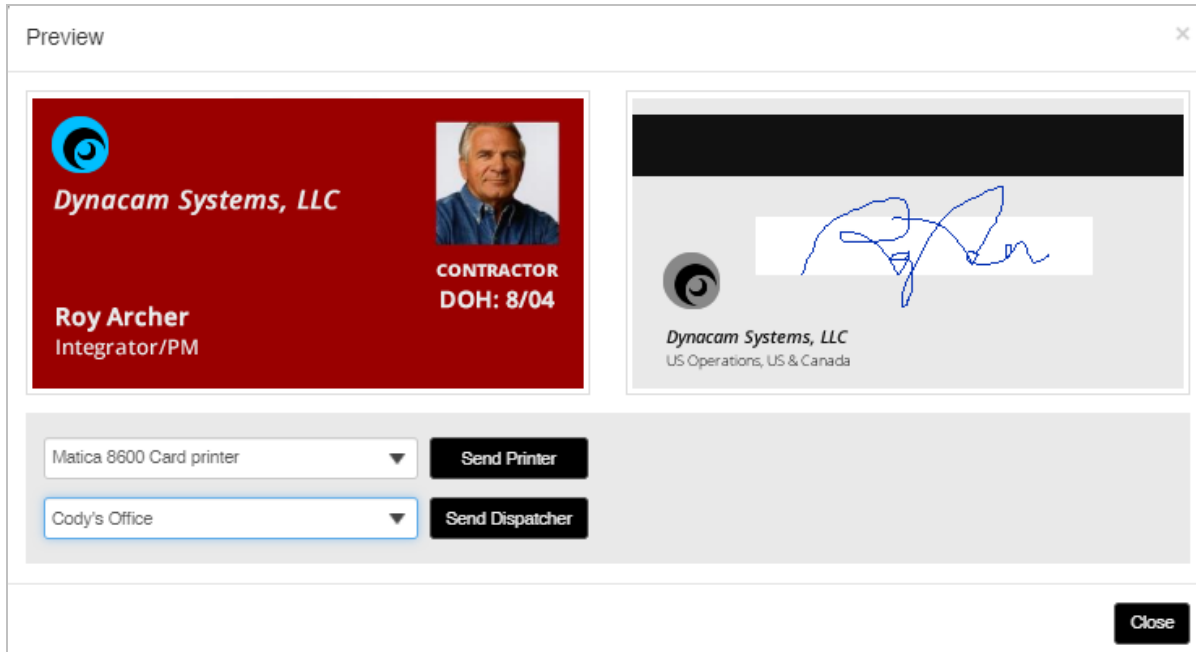
☐ Additional Fields

Access Information Add Loop

Cardholder / Card-Badge Settings
(hover/tap to open thumbnail)

- To Preview or Print a Badge you must have already assigned and saved the Badge Template to the card.
 - Select the template from the Badge Designs field if the badge template is not assigned.
 - Click the Save button to save the cardholder.
 - In the Card Toolbar, you can click the Print icon (printer) to print the badge without previewing it.

- In the Card Toolbar, you can click the Preview icon (eyeball) to preview the badge.
The screen will show both sides of the badge if applicable.
You can print from the Preview dialog box.
- In the Preview screen, select a printer and click Send Printer to print the badge at an online card printer.
- In the Preview screen, select a dispatcher and click Send Dispatcher to send the badge to a Dispatcher queue. A dispatch user will need to open the Print Dispatcher engine and assign the badge to an online card printer.



Cardholder Badge Preview & Print
(hover/tap to open thumbnail)

7. In the [Access Information section](#), you can configure access permissions for the selected card you are editing. You can add more than one loop to a card. The card will not have access to doors on the loop until an access group is assigned.
 - Select Loop (shows the loop that is assigned/selected)
 - Authorized Loops (lists all authorized loops on the card)
 - Access Group 1 through 4 (assign the desired access groups in these fields)

NOTE: You can add more Loops by clicking the **Add Loop** button.

Access Information ➕ Add Loop

Select loop
CC Test Environment

Authorized Loops
CC Test Environment

Access Group 1
** UNLIMITED ACCESS **

Access Group 2
** NO ACCESS GROUP **

Access Group 3
** NO ACCESS GROUP **

Access Group 4
** NO ACCESS GROUP **

▶ Card 2 🗑️ 👁️ 🖨️ ☑️

▶ Card 3 🗑️ 👁️ 🖨️ ☑️

Access Information (permissions)
(hover/tap to open thumbnail)

8. Clicking the [> Activity History section](#) (expandable section) allows retrieve cardholder activity history. The following fields are included ...
- **Start Date/Time:** select the starting date/time
 - **End Date/Time:** select the ending date/time
 - **Event Types:** Select at least one event type.
Types include: Access Granted, Duress, Passback Violations, Invalid Attempts
 - **GET HISTORY** clicking the button retrieves the selected events that occurred between the start and end date range.

▼ **Activity History**

Start Date & Time 📅 End Date & Time 📅 Event Type None selected Get History

Cardholder Activity History Report
(hover/tap to open thumbnail)

9. **BUTTONS** at bottom of page include ...

- **Cancel** - cancel pending changes and return to last saved state.
- **Delete** - delete the entire cardholder
- **Save** - save the pending changes

Access & Schedules

Editing Access Groups

This topic describes how to change the programming of an existing Access Group, which includes adding or removing authorized doors and assigning or changing time schedules.

FEATURED TOPICS

[About Access Groups](#)

[Open Access Group Editor](#)

[How to Edit Access Groups](#)

[Next Steps](#)

About Editing Access Groups

This section contains information that helps the user understand how access groups work.

- You can [SKIP TO INSTRUCTIONS](#) in the next section if needed.
- You can use the [Add Access Group Wizard](#) to add a new access group.

PREREQUISITES TO EDITING ACCESS GROUPS

- The user's login account must have the appropriate permissions to change access group programming.
- The **Access Group** that you want to change must already exist in the system or you will need to create it.
- The **Time Schedules** you need for each door must be created before they can be assigned.
- If you have not yet created the Time Schedules or Access Group, you can do so from the [Wizards](#).
- (optional) If you will be assigning a custom schedule to the crisis mode field, you must create it first.

NOTE: see the "Editing Access Groups " on the previous page and other subsections sections of this topic if you are new to access groups.

IMPORTANT CRISIS MODE OPERATION: if you do not assign a *schedule* to the **crisis mode field** in the access group, the access privileges will continue to operate/behave according to the normally assigned schedules. If you assign a *schedule* to the **crisis mode field**, then all doors in the group will revert to the designated *crisis schedule* until crisis mode is reset or deactivated for the loop/cluster the access group belong in.

TERMS

- **Access Control:** is the function of controlling access to a door or entry point at specified times or days. The system will **grant access** to a valid/active* card/credential at 'authorized entry points' (doors, turnstiles, etc.) during the *active* (green) portion of a time schedule. The system will **deny access** to invalid/inactive cards/credentials at entry points during the *inactive* portion of the time schedule.
- **Access Group:** an *Access Group* is the group of doors that a cardholder is permitted to access or open at designated times. **MORE:** Each door in an access group is linked to a time schedule which controls when a card/credential is granted or denied access. Once an *Access Group* is created, it can be assigned to any **access card** (credential) during cardholder enrollment in the *Cardholder Editor Page* or *Card Wizard*.
- **Custom Access Group:** is an *Access Group* that is created or defined by an user or the system administrator.

- **System Default Access Group:** is a predefined *Access Group* that is in the system by default and cannot be changed or deleted by anyone. There are two predefined *Access Groups* -- i.e., "*** Unlimited Access ***" and "*** No Access ***".
MORE: "Unlimited Access" grants access to all doors at all times. "No Access" denies access to all doors at all times.
- **Time Schedule:** a *Time Schedule* is a set of incremental *time periods* that cover a 24-hour period, which are configured to be *active* or *inactive* (green vs. red/gray) at specified times. *MORE:* a *schedule's* time periods can be divided into *15-minute intervals* (or *1-minute intervals*), depending on the format chosen for the loop/cluster). These incremental *time periods* are either active (green) or inactive (red/gray). And when a schedule is assigned to a card, they control when a card/credential is granted or denied access to the 'authorized doors' that belong to the access group. Once a *Schedule* is created, it can be assigned to any **door** within an access group, or elsewhere in the system to door groups, i/o groups, ...
- **Custom Schedule:** is a *Time Schedule* that is created by the system admin or user, which defines the *active* and *inactive* time periods. *MORE:* Typically 'active' means unlock/grant access and 'inactive' means lock/deny access.
- **System Default Schedule:** is a predefined *Time Schedule* in the system for default use. There are two predefined *Time Schedules*; i.e., "***Always***" and "***Never***". *MORE:* "Always" means all time periods are active/on (green). "Never" means all time periods are inactive/off (red/gray).
- **Crisis Mode:** is a *system-wide state* that can be activated on-command by an user in a critical or emergency situation.
- **Crisis Mode Schedule:** is simply the *time schedule* that is assigned to the crisis mode field in any part of the system programming - including Access Groups, etc. - which the system will use during an 'active crisis mode'. *MORE:* The crisis schedule can be a *custom schedule* or use one of the *default system schedules* ("always" or "never").

* Any cardholder or any card/credential can be made inactive system-wide by configuring/enabling the 'inactive' or 'deactivated' options in the Cardholder programming. While a cardholder is inactive or a card/credential is inactive, access is denied system-wide.

HOW ACCESS GROUPS WORK

Access Groups are created for each loop/cluster. If you want a card to have access to doors that are on different loops, you must create separate access groups for the doors on each loop/cluster. Then during enrollment, the user can assign each loop/cluster to the access card and choose the appropriate access groups that you made in each loop/cluster. You can assign up to four (4) Access Groups per Loop/Cluster.

When you create the *Access Group*, you must choose the doors you want to be in the authorized set and assign the desired *Time Schedule(s)* to them. The same time schedule can be assigned to all doors -OR- you can assign different time schedule(s) to each individual authorized door.

As defined in the Terms, an *Access Group* is a select set of "authorized doors" that have schedules assigned to control when the access card is permitted to enter the door. Of course the authorized doors are within the same hardware loop/cluster. If the cardholder needs access to doors that are in a different loop/cluster then you must create the schedules and access groups within those other loop/clusters.

- You can add or remove a door to the authorized group at any time. You can also assign different schedules to each door.
- To add a door to an access group, move the door from the *unauthorized group* into the *authorized group* and assign a schedule. The system will grant access to "authorized doors" during the active time periods on the schedule.
- To remove a door from an access group, remove the door from the *authorized group*. The system will not grant access to "unauthorized doors".
- To change when access is granted to any door, you can change which schedule is assigned or you can edit the time schedule and change which time periods are active vs inactive. The system will not grant access to authorized doors during the inactive (red/gray) time periods of the assigned schedule.

When the *Access Group* is saved, the associated Loop/Cluster is updated. The panels must be online to receive the updates. Offline panels will continue to operate using the existing programming.

RULES OF OPERATION

Ultimately, the authorized doors will allow access when the assigned schedule is in it's "active" (green) state. And the authorized doors deny access when the assigned schedule is in it's "inactive" (gray/red) state.

- **ALL DOORS = SAME SCHEDULE:** All the authorized doors in an access group can be assigned to the same schedule, which will provide access to all the doors at the same time periods and days. The cards assigned to this kind of access group will work the same way at all the doors in the group.
- **EACH DOOR = DIFFERENT SCHEDULES:** Each individual door in an access group can be assigned to different schedules, which will provide unique access permissions at each authorized door. The cards assigned to this kind of access group will work differently at each door.
- **SINGLE CARD/MULTIPLE ACCESS GROUPS:** You can add more doors and more schedules to the card by adding multiple access groups.
- **A DOOR CAN BE AUTHORIZED IN MORE THAN ONE GROUP** (overlapping privileges) - this means the same door can have different schedules assigned to it through different access groups. So cardholders in the "day-shift group" will have access to the front door during daytime hours only. Cardholders in the "night-shift group" will have access to that same door at nighttime, but not daytime.

Since it is possible to assign more than one access group to a card, it is possible to assign extended or overlapping access privileges to a cardholder. This may or may not be desirable, depending on the cardholder roles and responsibilities.

ABOUT OVERLAPPING ACCESS PRIVILEGES: Since it is possible to create overlapping access privileges you must take care to evaluate all the privileges when you create access groups, as well as when you create the card. Be aware that the system will grant access to any authorized door if any access group has an "active" schedule when the card is presented to the reader. Likewise, be mindful of only partially removing access to a door by removing one access group when another access group on the card has access to that door, if indeed you want to remove all access to that door. The system will still grant access for the remaining groups. It may be undesirable to allow overlapping access permissions on a card. Consider creating a new access group with the specific access the cardholder needs.

CRISIS MODE SCHEDULE BEHAVIOR

Assigning a schedule to the **Crisis Mode Field** is mandatory. You have several options.

1. If you assign a *default system schedule* (i.e., "Always" or "Never") to the crisis mode field, the Access Group will follow the assigned schedule while crisis mode is active/engaged. The access permissions will return to normal operation when crisis mode is reset or deactivated.
2. If you assign a *custom-schedule* to the crisis mode field, the Access Group will follow the assigned custom schedule while crisis mode is active/engaged. The access permissions will return to normal operation when crisis mode is reset or deactivated.
3. If do not want the access group behavior to change while crisis mode active/engaged, then simply assign the same schedule to the crisis mode field as is assigned to the access group. This way the access permissions will continue to operate as normal during the active Crisis Mode.

The crisis mode schedule tells the hardware/readers how to behave when crisis mode is engaged or activated.

- If the "unlimited access" schedule is assigned as the crisis schedule, all the doors in the loop will unlock when crisis mode is engaged.
- If the "no access" schedule is assigned as the crisis schedule, all the doors in the loop will lock down when crisis mode is engaged.
- If the same schedule is assigned to all doors and to crisis mode, then all doors will function as scheduled.
- You can create a specific schedule for crisis mode in the [Time Schedules Wizard](#).

MODIFYING AN ACCESS GROUP

In the *Access Group Editor*, you can modify or delete an existing *Access Group*.

- A. Modifying the access group will change the access permissions in the access control panel. Any changes made to the access group should take effect when the group is saved. All cards/cardholders that are assigned to the updated group will be immediately affected when the changes are saved/loaded to the panel.
- B. Deleting an access group removes it from the access control panels that belong to the selected Loop (location). Deleting an access group does not delete the schedules or doors from the system. The doors and schedules remain in the system, but they are no longer assigned to that access group.

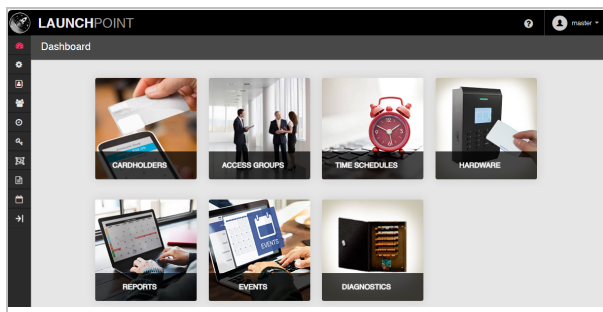
IMPORTANT NOTICE ABOUT UPDATING PANELS: Online panels should receive the updated changes when the access group is saved (or deleted from the system). Offline panels continue using the known access rules until the panels are brought back online and loaded with the new changes. Once the data is loaded to the panels, all changes are effective immediately for associated cards.

1. enter comments and service notes.
2. delete the entire access group.

How to Open Access Group Editor

There are two ways to open the *Access Groups Page* ...

- **Side Menu:** select "Access Group" menu icon or option.
- **Dashboard:** select 'Access Group' Tile (under Configure section)



Click/tap thumbnail to enlarge.

LAUNCHPOINT

Version : PRO | Build : 305

click to close

X

SG OPERATOR

Access Group

Select Loop or Cluster

CC Test Environment

Add New

Select Access Group

** NO ACCESS GROUP **

** UNLIMITED ACCESS **

All 24/7/365

General Hours

Access Group Name *

General Hours

Select Crisis Mode Access Group *

** NO ACCESS GROUP **

☐ Access Group Disabled

Save

Delete

Activation Date &Time

Expiration Date &Time

☐ Additional Fields

Assign Doors

Unauthorized Readers - Click Edit Schedule to add door to group

Unauthorized Readers/Doors	Time Schedule	Action
Authorized Readers/Doors Information		
Authorized Readers/Doors	Time Schedule	Action
Cont: 001, Brd: 1, Sect: 1-0	Day Shift General Employees 8am-5pm	<div>Edit Schedule</div> <div>Remove</div>
Cont: 001, Brd: 1, Sect: 2-0	Management	<div>Edit Schedule</div> <div>Remove</div>

Powered by Galaxy Control Systems

The *Access Group Page* will be empty until the user chooses a loop/cluster.

How to Edit Access Groups

Be aware that all changes must be saved and loaded to the access control panels. The changes will automatically load if the services are running and the panels are online.

NOTICE: the **Delete** button - will delete the selected access group; but user will be prompted to confirm or cancel the choice to delete before the record is deleted.

CAUTION: Access cards that are assigned to a deleted **Access Group** will stop working in the system for the doors that belonged to the deleted access group. If the card was only assigned to one access group, then the card will no longer work in the system even if it is not expired.

STEPS

1. Select the Loop/Cluster (Location) that the Access Group belongs to.
2. Select the Access Group name - you can edit the name as desired. This will propagate throughout the system. Although, typically you will not need to edit the group name.
3. Assign the Crisis Mode Access Group- this affects how all the doors on the Loop behave during crisis mode.
4. (optional) Access Group Disabled (checkbox)- this option affects whether the access group (and associated cards) will work.
 - > When checked, the access group will not work in the system.
 - > When unchecked, the access group will work.
5. (optional) Activation Date/Time - sets a future activation date for the access group.
 - > It will not work in the system until the date elapses. Associated cards are likewise impacted.
6. (optional) Expiration Date/Time - sets a future expiration date for the access group.
 - > It will not work in the system after the date elapses. Associated cards are likewise impacted.
7. Additional Fields cbx - shows/hides additional fields.
 - > When checked, the addit. fields show.
 - > When unchecked, the the addit fields are hidden.
8. (optional) Notes, Comments, Service Comments - enter information at user discretion.
9. Access Group Number - system assigned number - is assigned when user enters the name.
10. (optional) Extended Group (checkbox) - sets the extended access group option.
 - > When checked, the group is treated as an extended group.
 - > When unchecked, the group is treated as a normal group.
11. Assign Doors (dropdown section) - show/hide the available doors (authorized and unauthorized).
12. Unauthorized Doors List - lists all the doors in the Loop that are "unauthorized" (i.e. no assigned schedule).
 - > You must assign a schedule to move the door into the Authorized Doors list.

13. Authorized Doors List - lists all the doors in the Loop that are "authorized" (i.e. have a schedule).
 - > *You must remove the schedule to move the door into the Unauthorized Doors list.*
 - > *You can click the "Edit Schedule" link to choose a different schedule.*See the [Schedules Editor](#) or [Add Schedules Wizard](#) if you need to prepare a schedule.
 14. Click the **SAVE** button to save your work.
 15. Note: Clicking the **Add New** button lets you open the Wizard to add a new access group.
-

Next Steps

Once you have created your needed access groups, you can assign them to a card in the *Access Permissions* section of the Card-holder Editor or Card Wizard.

Editing Time Schedules

This topic covers configuring an existing Time Schedules.

FEATURED TOPICS

[About Editing Schedules](#)

[Open Schedules Editor](#)

[How to Edit Time Schedules](#)

[How to Edit Special Days \(Holidays\)](#)

[Next Steps](#)

About Editing Schedules

In the **Time Schedule Editor**, you can modify or delete an existing schedule or special day (holiday).

- You can [ADVANCE /SKIP AHEAD TO INSTRUCTIONS](#) in the next section as appropriate.
- Use the [Add Time Schedules to Wizard](#) to add a new access group.

PREREQUISITES & NOTES

- The user must have permission to edit schedules and special days.
- The **time schedule** you wish to edit must already exist in the system.
- If you have not added the schedule, see the [Time Schedule Wizard](#).
- A schedule will not function in the system if it does not have the **time periods** properly configured for each day.
- Special Days (holidays) are optional.

Crisis Mode Notice: Typically, crisis mode uses a default system schedule (always or never). However, if you are creating a custom schedule for use in crisis mode field, you should take care to reserve the schedule for crisis mode use only. Do not cross up custom crisis schedules with normal scheduling of doors or other hardware.

TIME SCHEDULES EXPLAINED ...

Time Schedules are created at the Loop/Cluster level in the system. This means they can be assigned to any access group (authorized door) within the same loop/cluster - - which is done through the access group programming. They cannot be used on access groups or doors in other loop/clusters.

Schedules have two states, "active" (green) and "inactive" (not green).

- During the "active"(green) state, a valid card can be granted access.
- During the "inactive"(gray/red) state, a valid card will be denied access.

The schedule is not assigned directly to the access card. Instead it is assigned to a door in an access group. The access group is assigned to the card. This way the cardholder can present the card to a door and the schedule will determine if the cardholder has access.

See [Access Groups Explained](#) for more info on access groups.

When the schedule is saved, it is added to the panels in the Loop. An offline panel must be brought online to update the schedules.

HOW SPECIAL DAYS WORK ...

When creating a time schedule, you can decide whether the schedule will include holidays/special days.

The **Special Days/Holidays** can be programmed to affect a half-day, a whole-day, or any portion of the day that is needed.

- **Half-Day Example:** If you want a half-day (close-early), you could make the special day "active" in the morning, but "inactive" in the afternoon. When this day type is assigned to the calendar day, it will override the normal schedule and access will be denied for the afternoon hours.
- **Whole-day Example:** If you want a whole day closed, you would make the special day "inactive" (gray/red) all day. Whenever this day type occurs on the yearly calendar, it will override the normal schedule and access will be denied instead of granted for that whole day. The system will return to the normal schedule on the next day or first day after the .

HOW ACCESS IS GRANTED ...

Once the schedule is created, it must be assigned to a door/reader in an access group. Then the access group is assigned to the card/cardholder. This will allow the cardholder to gain access at the "authorized doors" during the "active" (green) days and times of the assigned schedule.

The access card is denied access to all "unauthorized" doors (doors with no schedules). The access card is also denied access at "authorized" doors during any days or times that the assigned schedule is "inactive" (not green).

Bottom line, the door must be **authorized** and the schedule must be **active** (in the assigned access group) to grant access to a card.

HOW A TIME SCHEDULE IS MODIFIED ...

Modifying the schedule will change the access permissions in the access control panel. Any changes made to the schedule should take effect when the schedule is saved. All cards/cardholders that are assigned to the affected access group will be immediately affected when the changes are saved/loaded to the panel.

Deleting a time schedule removes it from the access control panels in the same Loop (location). Deleting a schedule does not delete the access group, but it will render any assigned doors to the unauthorized status.

The access groups remain in the system, but they are no longer assigned to the deleted schedule. Access cards also remain in the system and assigned to the access group, but they will be no longer have access to any unauthorized door.

IMPORTANT NOTICE ABOUT UPDATING PANELS: Online panels should receive the updated changes when the schedule is saved or deleted from the system. Offline panels continue using the known schedules until the panels are brought back online and loaded with the new changes. Once the data is loaded to the panels, all changes are effective immediately for associated cards.

In the Time Schedule Editor, you can change the following things ...

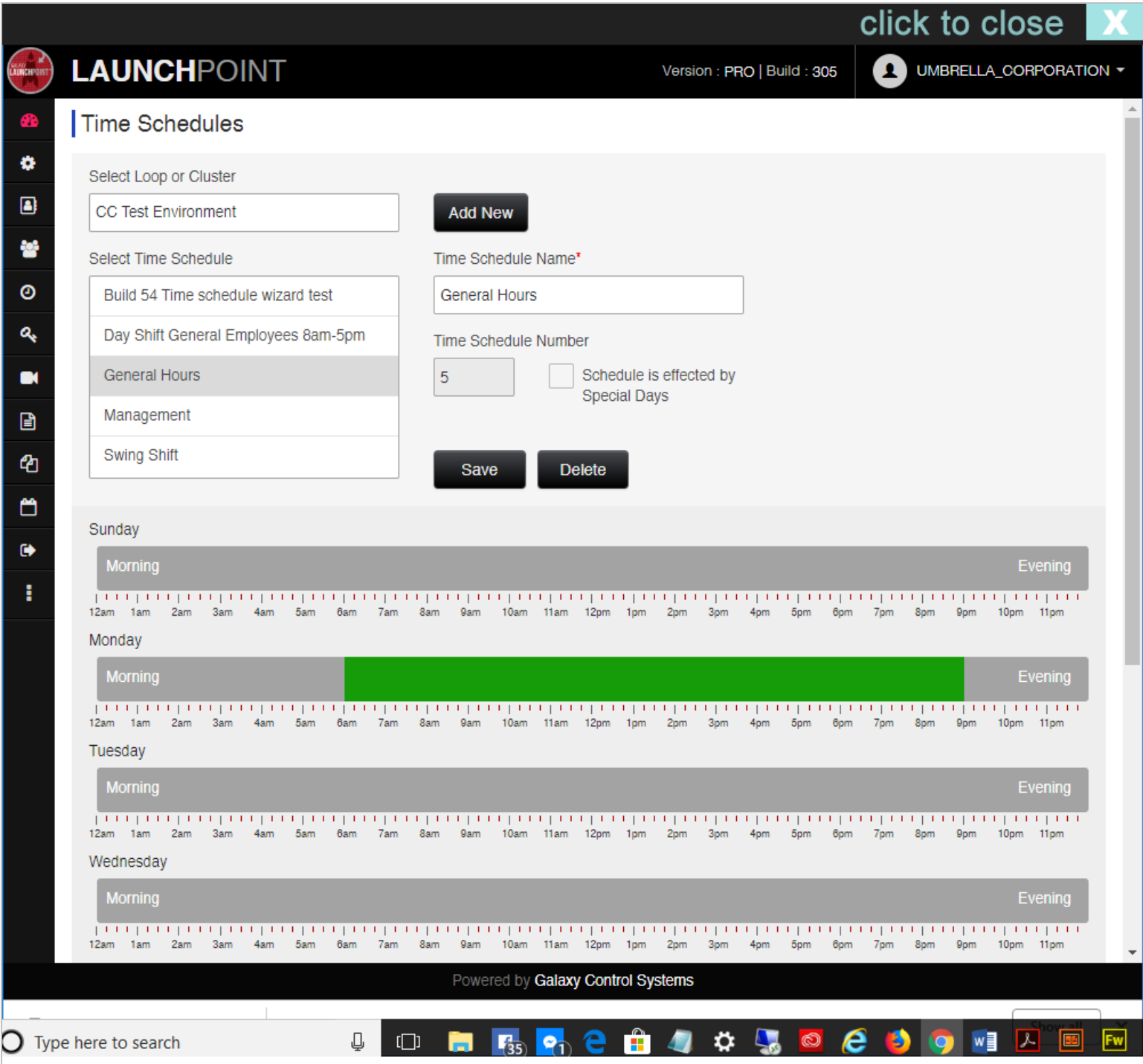
1. change the **Schedule Name** (the name change is effective system-wide)
2. change the start and end times for the **active**(green) and **inactive**(gray) **Time Periods**
3. change which **Special Days** affect the schedules
4. delete the entire **Schedule**

These changes are effective system-wide when the schedule is saved.

TIME SCHEDULE SCREEN OVERVIEW

This section describes the capabilities of the **Time Schedule Editor** which support editing the **time periods** and **special days** (holidays).

If you need to add a new *time schedule*, see the [Time Schedules Wizard](#).



Click/tap to enlarge image or reduce image.

Prerequisites and Notes

- The **time schedule** you wish to edit must already exist in the system.
- If you have not added the schedule, see the [Time Schedule Wizard](#).

- A schedule will not function correctly in the system if the **time periods** are not properly configured for each day.
- Special Days (holidays) are optional.

Navigation Controls and Buttons ...

This wizard essentially has one screen. It makes a difference whether you are adding a new schedule (add new) or if you are selecting an existing schedule to edit.

- **Add New** - opens the Time Schedules Wizard where you can add the name of the new schedule.
- **Save** - saves the schedule and any modifications.
- **Delete** - deletes the selected schedule from the system.
- **Affected by Special Days** (cbx control) - shows/hides the **time period controls** below the week days.

TIP: Adding special days (holidays) is up to the discretion of the system subscriber. If your schedule needs to work the same way all the time (365-days a year) then do not configure special days. This could be true of a schedule that is assigned to hardware or to emergency personnel who may be immune to holidays.

In the Add Time Schedule Wizard, you can enter the following information ...

1. choose an existing Loop/Cluster
2. enter a time schedule name *
3. show/hide the time periods for special days (holidays) **
4. configure the start and stop times for each week day.
5. configure the start and stop times for time schedules.

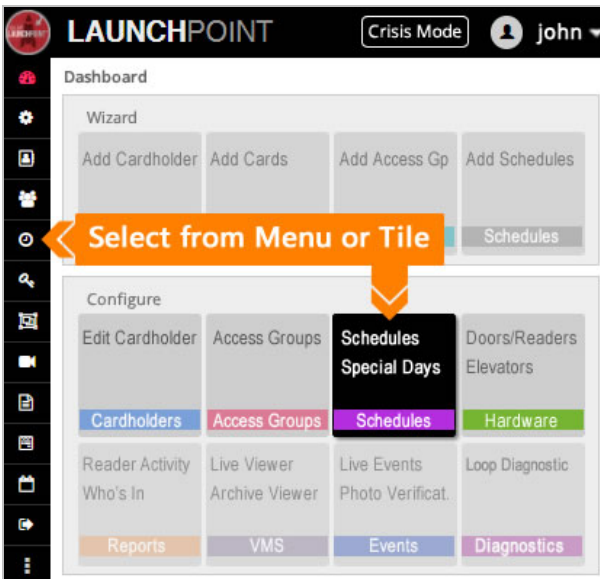
* A system number will be assigned to the schedule when you exit the Schedule Name field.

** Configuring special days is optional - up to subscriber discretion.


How to Open Time Schedules Editor

There are two ways to open the *Time Schedules Page* ...


- **Side Menu:** select "Time Schedule" menu icon.
- **Dashboard:** select 'Time Schedule Tile' (under Configure section)















Click/tap thumbnail to enlarge.

**LAUNCHPOINT**

Version : PRO | Build : 305

 UMBRELLA_CORPORATION



Time Schedules

Select Loop or Cluster
CC Test Environment

Add New

Select Time Schedule
Build 54 Time schedule wizard test
Day Shift General Employees 8am-5pm
General Hours
Management
Swing Shift

Time Schedule Name*
General Hours

Time Schedule Number
5

☐ Schedule is effected by Special Days

Save

Delete

Sunday

Morning

Evening

12am 1am 2am 3am 4am 5am 6am 7am 8am 9am 10am 11am 12pm 1pm 2pm 3pm 4pm 5pm 6pm 7pm 8pm 9pm 10pm 11pm

Monday

Morning

Evening

12am 1am 2am 3am 4am 5am 6am 7am 8am 9am 10am 11am 12pm 1pm 2pm 3pm 4pm 5pm 6pm 7pm 8pm 9pm 10pm 11pm

Tuesday

Morning

Evening

12am 1am 2am 3am 4am 5am 6am 7am 8am 9am 10am 11am 12pm 1pm 2pm 3pm 4pm 5pm 6pm 7pm 8pm 9pm 10pm 11pm

Wednesday


Morning

Evening

12am 1am 2am 3am 4am 5am 6am 7am 8am 9am 10am 11am 12pm 1pm 2pm 3pm 4pm 5pm 6pm 7pm 8pm 9pm 10pm 11pm

Powered by Galaxy Control Systems

Type here to search



- Time Schedule Editor

How to Edit Time Schedules

See the "[TIME SCHEDULES EXPLAINED ...](#)" on page 130 if you are new to schedules.

OPEN THE EDITOR

Click the Schedules icon from the left side Menu.



< [Time Schedule menu icon](#)

STEPS

1. Select the **Loop/Cluster** (Location) that the Schedule belongs to.

Time Schedules

Select Loop or Cluster

Select

[01] Cody Test Loop

[02] Cody Test Loop 2

[50] Live Events

[55] Live Events 2

Add New

2. Select the **Schedule Name** (from list view) - the name field will populate

Select Time Schedule

Customer Schedule 1

Hourly Day Shift

Live Schedule

Audit M-F 915-245

Audit Schedule

3. **Schedule name** - you can edit the name as desired. This will propagate throughout the system.

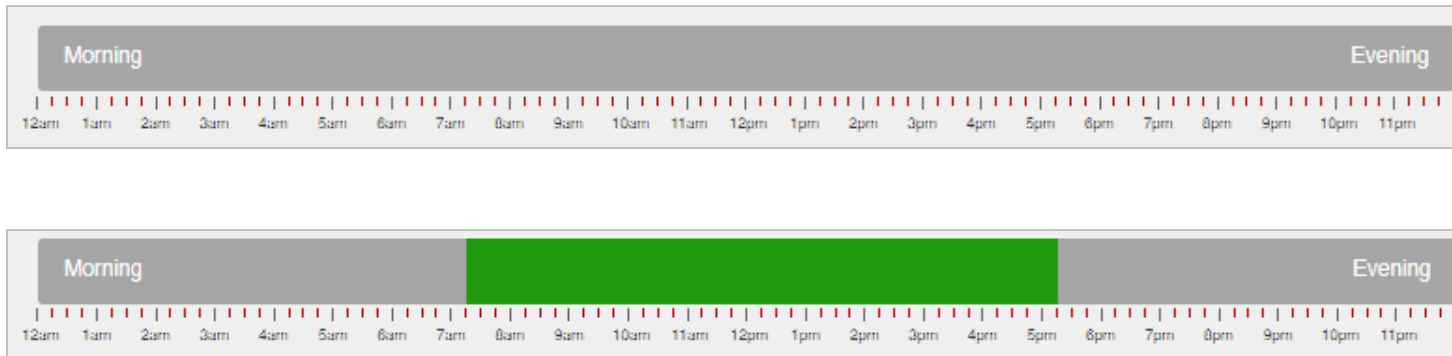
Time Schedule Name

Hourly Day Shift

4. **Schedule Number** - system assigned number - is assigned when user enters the name.
5. **Schedule affected by Special Days** cbx - determines whether schedule will work on holidays.
When checked, the holidays can be configured. The holidays time periods appear.
When unchecked, the holiday time periods cannot be seen or configured.

☐ Schedule is effected by Special Days

6. Click on any **Time Period Bar** to program the active time periods (weekdays Sunday thru Saturday)
 If the Time Bar is all gray, click it if you want to add a time period.
 If the Time Bar has some green, click it if you want to change the time periods.
 Green = active/on. Gray = inactive/off.



7. In the *Set Time Schedule* window, you can add or change the **Start Times** and **Stop Times** for the **Time Period** of the selected weekday (M-F, S/S) ...

a. for the *Start Time*, choose the **hours** and **minutes** > this sets the time when the active period begins.

The screenshot shows the 'Set Time Schedule' window for Tuesday. It has two rows of time period settings. The first row shows '07 am' to '12 pm'. The second row shows '01 pm' to '05 pm', with '05 pm' highlighted. There are buttons for adding (+), removing (X), closing, and saving.

- b. for the *Stop Time*, choose the **hours** and **minutes** > this sets the *Active Time Period* on the chosen weekday.
- c. (optional) you can add another set of **start/stop times** to the same weekday by clicking the **Green Plus button** - as needed.
- d. (optional) you can remove a set of **start/stop times** by clicking the **Red X button** - as needed.
- e. click the **SAVE** button to save your time periods for the selected weekday.
clicking the Close button will exit the *Set Time Schedule* window without saving any changes.

8. Repeat step 6 and 7 for each day's time period bar.

9. Click the **SAVE** button to save your schedule. .

10. Continue to the [next section](#) if you "checked" that this [Schedule is Affected by Special/Holidays](#).

OTHER BUTTONS

Add New button lets you open the Schedules Wizard to add a new schedule.

Delete button will delete the entire schedule. User will be prompted to confirm this choice.

Associated cards will no longer work at doors that were assigned to a schedule that is deleted, but the access group will remain intact.

Configure Holiday Day Types (Special Days/Holidays)

In the system, a **Special Day or Holiday** is simply a calendar day (date) that uses a *different schedule* than the normal days. The Holiday or Special Day must be programmed by the system administrator. However your schedule will not deviate on those days unless you configure the day-type hours for that Holiday.

For example: On a normal day your building is open 8am to 5pm. But on a Holiday your building may operate on different hours.

So when you configure your schedule, you also need to create the Day Types you will need to use.

- closed all day (nothing is active)
- open a half-day (active morning only)
- open a half-day (active afternoon only)
- open extended hours (active until 10pm)

OPEN THE SCHEDULE EDITOR

Click the Schedules icon from the left side Menu.



< Time Schedule menu icon

Time Schedules

Select Loop or Cluster

[50] Live Events

Add New

Select Time Schedule

Customer 1 Edge add test sch M-F 915-245

Hourly Day Shift

Live Events test schedule

Live Events Test schedule add NEWNAME

Sch Audit test 2

Time Schedule Name

Hourly Day Shift

Time Schedule Number

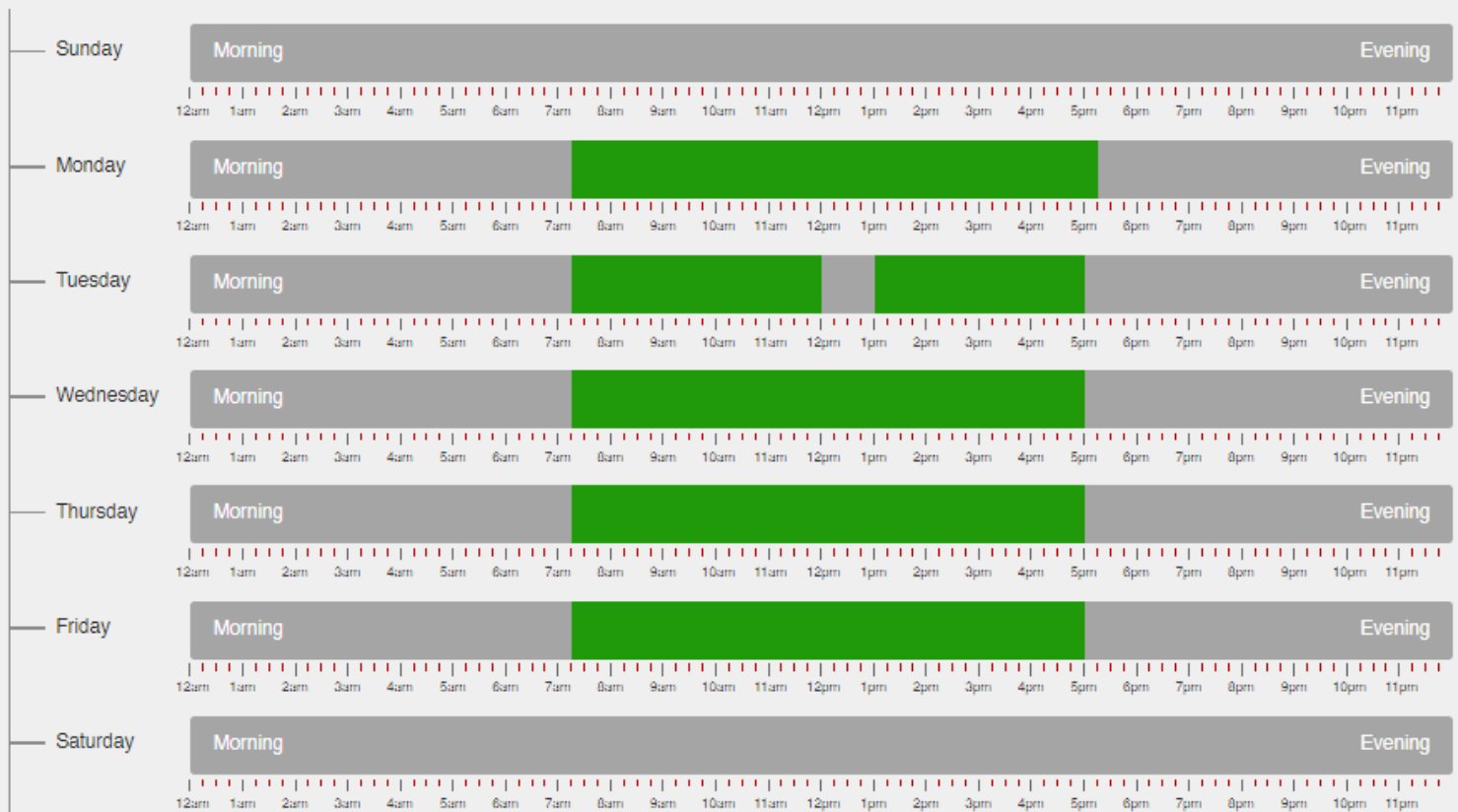
4



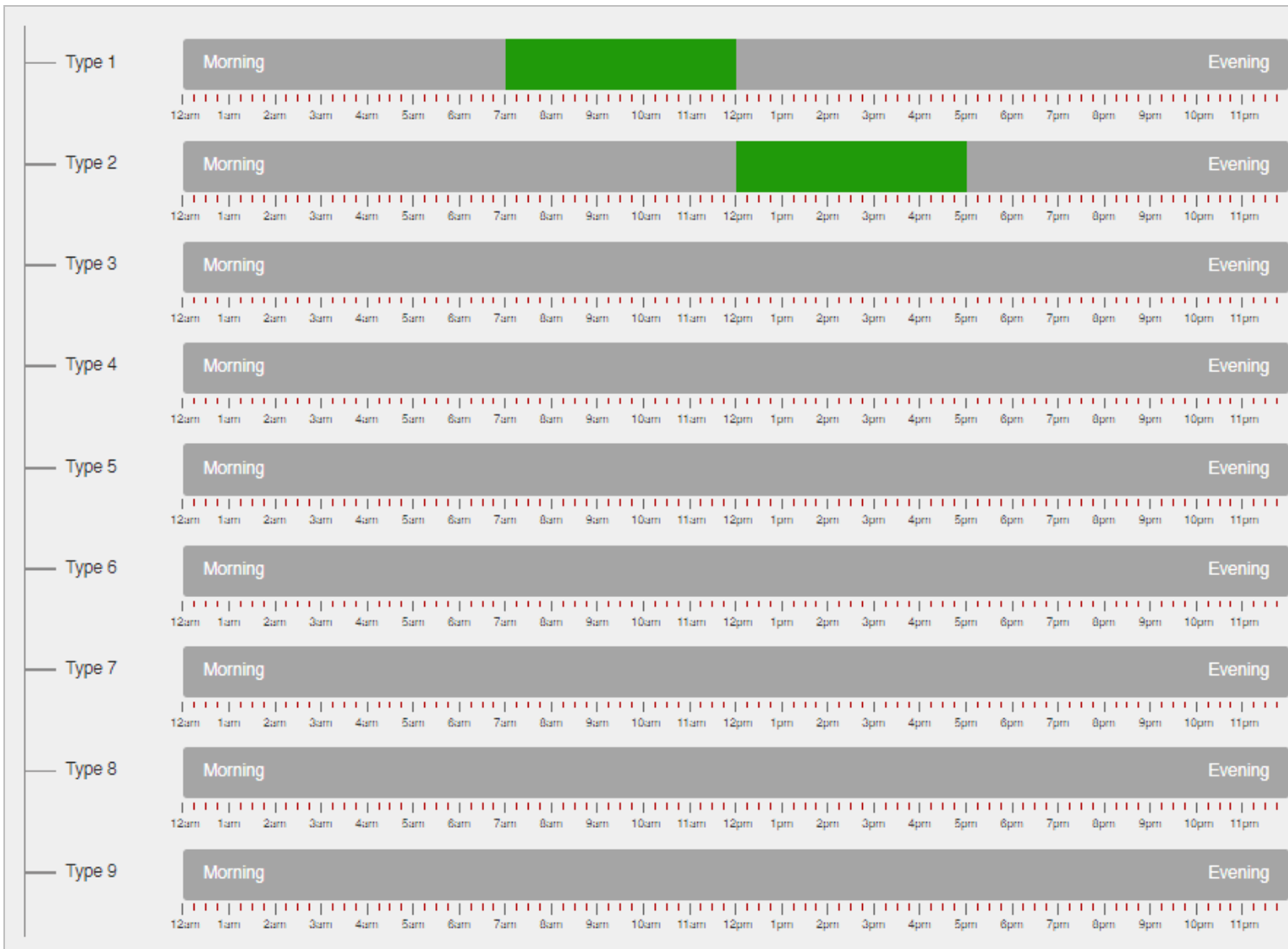
Schedule is effected by
Special Days

Save

Delete



- ◀ Schedule Editor (top half of page)



- ◀ Special Days (bottom half of page)

STEPS

1. If needed, **Select the Loop/Cluster** (Location) and the **Schedule Name** (from list view)
2. Place a checkmark in the **Schedule affected by Special Days** checkbox.
When checked, the holiday day-types will appear and you will need to configure them - in the way you want them to affect your schedule.
When unchecked, the holiday day-type time periods cannot be seen or configured.
3. Click on a **Holiday Type 1 thru 9** to open the *Set Time Schedule* window.

Set Time Schedule

Setting For Type 2

12 pm : 00 To 05 pm : 00

Close Save

12am 1am 2am 3am 4am 5am 6am 7am 8am 9am 10am 11am 12pm 1pm 2pm 3pm 4pm 5pm 6pm 7pm

Morning

12am 1am 2am 3am 4am 5am 6am 7am 8am 9am 10am 11am 12pm 1pm 2pm 3pm 4pm 5pm 6pm 7pm

4. When the *Set Time Schedule* window opens, you can add or remove time periods as needed.
 - a. click the **Green Plus** (*Add*) to add a new active time period to the *Holiday Type*.
 - b. click the **Red X** (*Delete*) to remove any unwanted time periods from the *Holiday Type*.
 - c. Remember if you want the *Holiday Type* to be closed/locked all day, then you do not want to add any active time periods.
5. Choose a **Start Time** and **Stop Time** (Hours/Minutes) in the *Set Time Schedule* window.
 The time between the start and stop time will be green.
 Green = "active"(open/unlock, or grant access). Gray = "inactive"(closed/locked, or deny access)



- 6. Click the **SAVE** button to save your time period for the Holiday Type.
Clicking **Close** will exit the window without saving any changes to the Holiday Type.
- 7. Repeat these steps for each Day Type you need to create.
- 8. When you are finished, click the **SAVE** button to save your schedule.

Next Steps

Once you have created the needed Schedules, you can assign them to a door in the [Access Group programming](#) or to other places - such as a crisis mode field if you made a crisis schedule.

One Time Scheduled Action

This topic describes how to create Scheduled Actions in the One Time Schedule screen.

FEATURED TOPICS

[Create a Scheduled Action](#)

Delete a Scheduled Action

Remove multiple Scheduled Actions

Create a Scheduled Action

The ***One-Time Schedule page*** allows a user to create a *Scheduled Action* for a selected Door/Reader, Input, or Output device. When scheduling the action, you can choose the frequency or behavior of the action.

RULES OF OPERATION

The following ***scheduled actions*** can be configured from the *One-Time Schedule Page*.

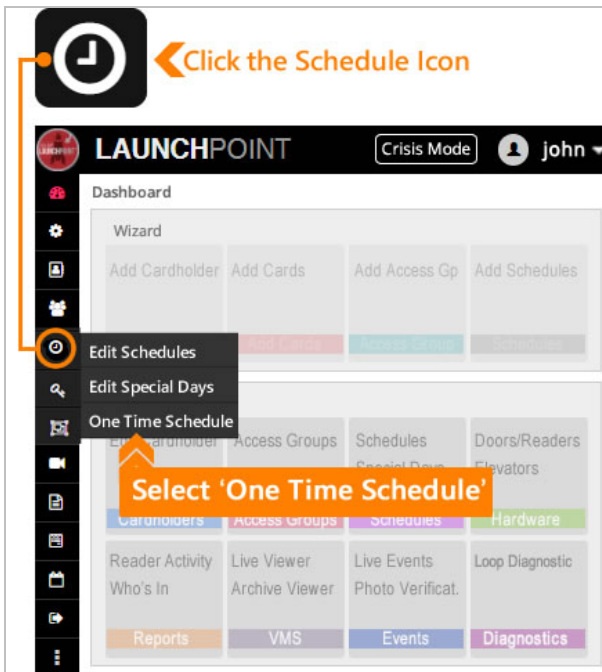
- Create a Door Action (*lock, unlock, enable, disable*)
- Create an Input Action (*shunt, unshunt, enable, disable*)
- Create an Output Action (*on, off, enable, disable*)
- Assign a Behavior (frequency) (one-time-only; every #hours; every #minutes; or on select weekdays)
- Assign a date and time for the action to happen.
- Remove or delete an action or multiple actions.

PREREQUISITES

- The user login account must have the appropriate security-level to open the page.

OPEN THE ONE-TIME SCHEDULE PAGE

You can open the *One-Time Schedule Page* from the side menu by clicking the Schedule icon.



CREATE A SCHEDULED ACTION

To create a *Scheduled Action* you must choose a device and set the frequency for the schedule "behavior".

Action Frequency (Behaviors droplist)

- one-time-only
- repeat every # hours
- repeat every # minutes
- repeat on selected weekdays

Device Actions

- Door/Reader = Lock/Unlock, Disable/Enable, Relay-2 ON/OFF, Pulse
- Inputs = Shunt/Unshunt, Disable (service mode)/Restore
- Outputs = Turn ON/OFF, Disable/Enable

STEPS

1. Select the desired **Loop/Cluster** at the top left of the page.
2. Select the desired **Device Type** (Readers/Doors, Inputs, or Outputs).

3. Select the **Device** - (this list is filtered to show only the devices in this Cluster of the Type you chose in the prior step).
4. Select the **Action** - (this list is filtered based on the Device Type you chose).
5. Select the **Date and Time** that you want the action to happen using the calendar feature.
6. Select the **Behavior** - (this is the frequency that you want the action to happen).
7. Click the **[Add to Scheduled Actions]** button to add the item to the Scheduled Actions list.
8. Click the **Save** button to save your changes.

RESULTS: the action you created will be saved.

Closing the page without saving will cancel your changes.

Scheduled Action

Hardware Action

Select Loop or Cluster

L006 Galaxy Control Systems

Select Device Type

Readers

Device

LP Reader 2

Select Action

Unlock Door

Start Date & Time

11/23/2021 11:07 AM

Select Repetition Behavior

One Time Only

Add To Scheduled List

Scheduled Actions

11/23/2021 11:07:00 AM (Tuesday) - Unlock Door

Delete Selected Items

Save

Cancel

Delete a Scheduled Action

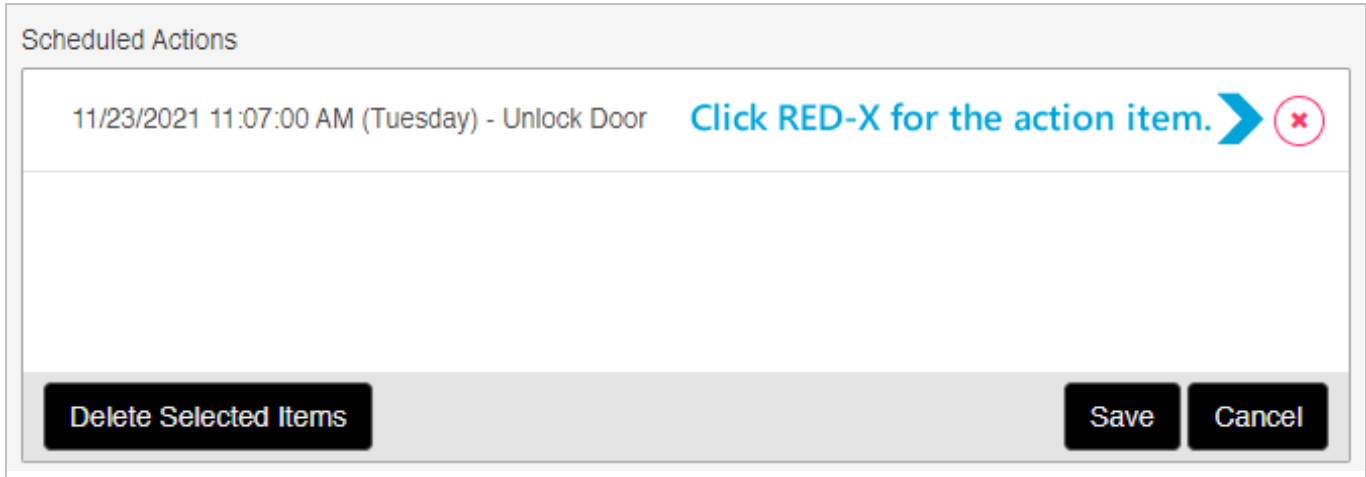
The user can remove a Scheduled Action in LaunchPoint from the *One Time Schedule Page*.

STEPS

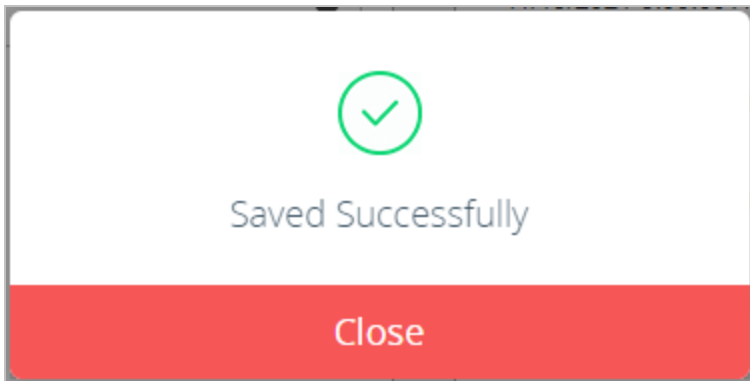
1. From the Menu Bar, click on the Schedules icon and choose *One Time Schedule* option.

RESULT: The *Scheduled Actions list-view* will display the Actions that are currently scheduled.

2. Click the **Red X** beside the desired *Scheduled Action* to delete it from the list-view.



3. Clicking the **Save** button will save your changes.
 - Click the **Save** to save your changes.
 - Click the **Cancel** to cancel your changes.
4. When you save, LaunchPoint should display a success confirmation.



Remove multiple Scheduled Actions

The user can remove multiple Scheduled Actions at the same time from the *One Time Schedule Page*.

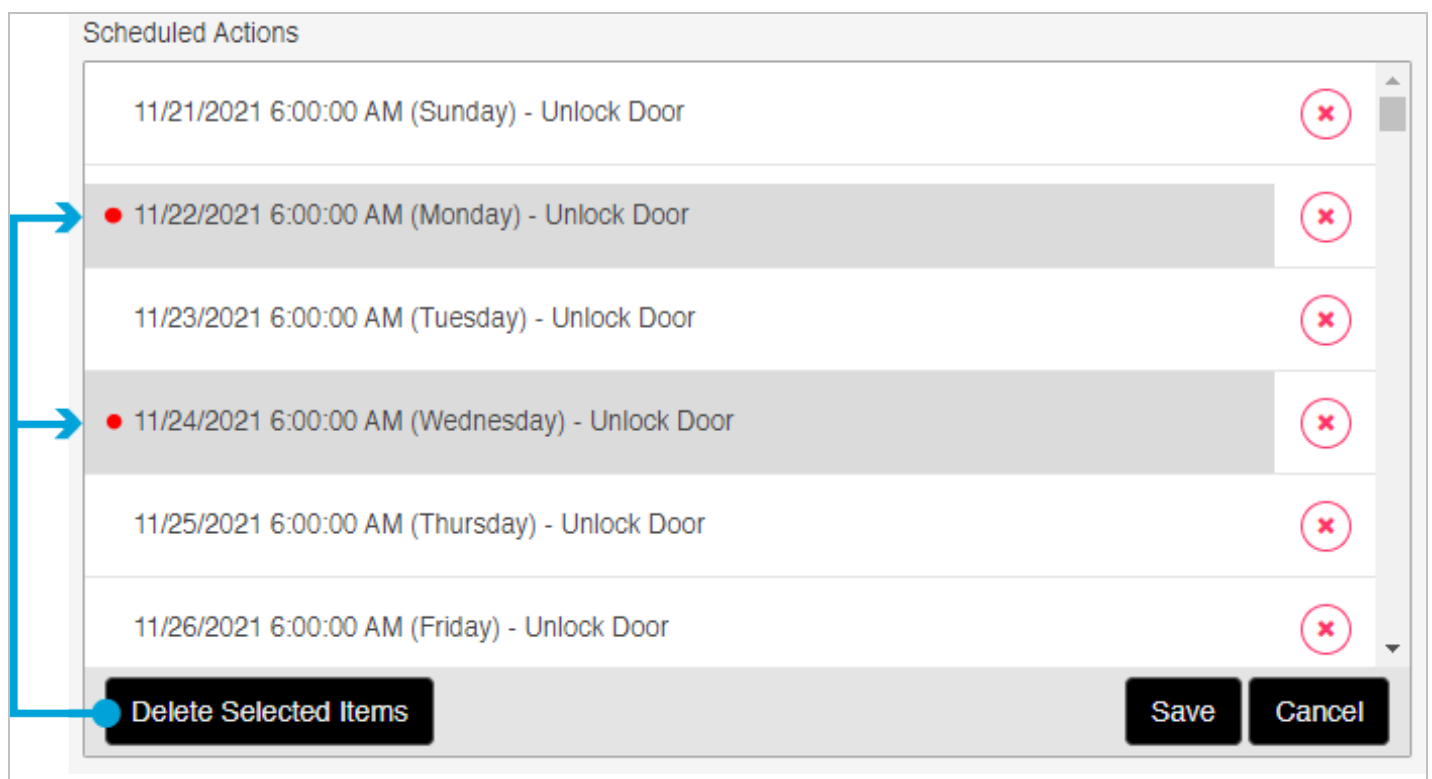
STEPS

1. From the Menu Bar, click on the Schedules icon and choose *One Time Schedule* option.

RESULT: The *Scheduled Actions list-view* will display the Actions that are currently scheduled.

2. Select more than one action by single-clicking on each item you want to delete.

RESULT: Each action item will be highlighted gray when selected.

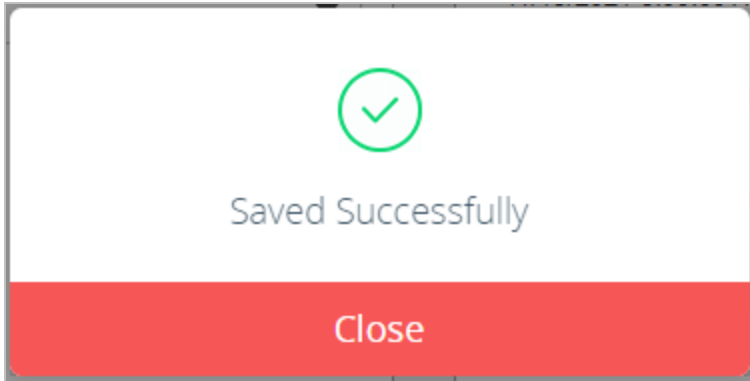


3. Click the **Delete Selected Item** to delete the selected items from the system.

4. Click the **Save** button to save changes.

- Click the **Save** = to save your changes.
- Click the **Cancel** = to cancel your changes.

5. When you save, LaunchPoint should display a success confirmation.



Hardware & Diagnostics

Access Readers

This topic covers functionality related to Access Reader Properties, including configuring door timers, sending user commands to control doors, and view video from linked cameras, as well as retrieving and exporting reader activity history.

FEATURED TOPICS

[Configure Readers](#)

[Send User Commands](#)

[View Reader Activity](#)

[Export Activity Report](#)

Configure Readers

The Reader page allows the user to configure properties of a selected Door/Reader, and more.

RULES OF OPERATION

The following actions can be done from the Reader page.

- **Change Timers** a selected door (*unlock time & reclose time*) .
- **Assign Unlock Schedule** to a door.
- **Send User Commands** to a selected door (Pulse, Lock, Unlock).
- **View Reader Activity History** for a selected reader.
- **Export Reader Activity** for a selected reader (*Excel/PDF*).

PREREQUISITES AND NOTES

- The user login account must have the appropriate security-level to open the Reader Properties page.
- The user login account must have permissions to issue user commands.
- The door unlock schedule must be created before it can be assigned.
- Reader email events require a working email address and the email output feature to be registered in the system licensing.
- External software must be installed to view reports in exported formats.

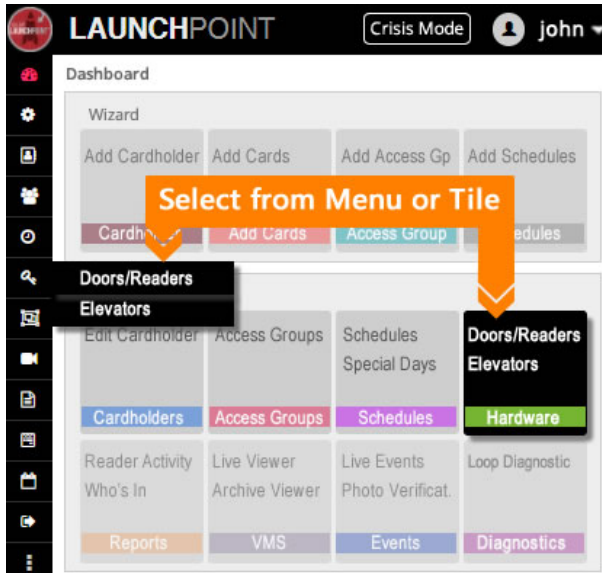
OPEN THE READER PAGE

There are two ways to open the Reader Properties page .

- **Side Menu:** select "Hardware" menu icon and select Doors/Readers.
- **Dashboard:** select 'Hardware' Tile (under Configure section) and select Doors/Readers.



← Hardware icon (from sidebar menu)



STEPS

1. Select the desired **Loop/Cluster** at the top left of the page.
2. Select the desired **Reader/Door**.
3. (optional) Edit the **Door/Reader Name** - as needed.
4. (optional) Assign a **Door Unlock Schedule** (*the schedule must have already been created*)
5. (optional) Set the **Unlock Time** as desired (5 seconds is the default)
6. (optional) Set the **Reclose Time** as desired (15 seconds is the default)
7. (optional) Enter an **Email** as desired (valid email required).
8. Click the **Save** button to save any changes.

RESULTS: the changes you made will be saved.

Closing the page without saving will cancel your changes.

Door/Reader Properties

Select Loop or Cluster

[50] Live Events

Select Door/Reader

Cluster: 050, Cont: 001, Brd: 1, Sect: 1-0

Reader ID: 7

Cluster: 050, Cont: 001, Brd: 1, Sect: 2-0

Reader ID: 8

Door/Reader Name *

Cluster: 050, Cont: 001, Brd: 1, Sect: 1-0

Reader ID : 7

Door Status

Door Open

Lock status

Locked

Automatic Unlock Schedule *

** NEVER **

Last access event

Valid Access (7/12/2021 05:52:36 AM)

Accessed By : Joe Smith

Unlock Time

0 : 5

Minutes Seconds

Reclose Time

0 : 15

Minutes Seconds

Email

cmoble@galaxysys.com

Save

Pulse

Lock

Unlock

Relay 2 off

☐ View History

Send User Commands to Door

User commands can be sent to only one door at a time from the Reader Properties page.

STEPS

1. Select the desired **Loop/Cluster**.
2. Select the desired **Reader/Door**.
3. Send the **User Command** as desired ...

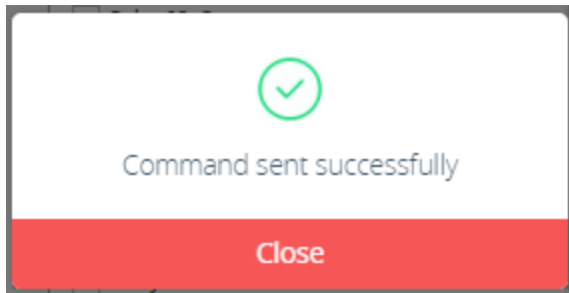
Pulse

Lock

Unlock

Relay 2 off

- a. Click the **Pulse** button = to send a *Pulse command* (momentarily unlock) the door. *The door uses the configured door timers to relock.*
 - b. Click the **Lock** button = to send a *Lock command* the door.
 - c. Click the **Unlock** button = to send an *Unlock command* the door.
 - d. Click the **Relay 2 Off** button = to send a *Relay Off command* the Relay-2.
4. When you send the command, LaunchPoint should display a success confirmation.



IMPORTANT: Lock and Unlock commands stay in effect until the door schedule changes the state. If the door uses a custom schedule, the door will remain in the user-issued state until the next time the schedule changes. Therefore, you must manually return the door to the appropriate lock/unlock state that is normally expected if you do not want to wait for the schedule to change.

View Reader Activity History

User can view the *Reader Activity History* for one reader at a time from the Reader Properties page. The activity history can be viewed online or exported to an Excel file or PDF file.

STEPS

1. Select the desired **Loop or Cluster**.
2. Select the desired **Reader**.
3. Enable (check) the **View History** checkbox to open the *Activity History Page*.
4. Enter the **Start date/time**.
5. Enter the **End date/time**.

6. Select at least one **Event Type**.

- a. "check" will include the event type in the report.
- b. "uncheck" will exclude or omit the event type from the report.
- c. the **Select All checkbox** can be used to toggle on/off all the events.

When checked, the report will include all the activity that occurred at the reader within the start and stop dates.

7. Click the **Get History** button to retrieve the data.

RESULT: the list of events that fall between the start and stop times is displayed.

Unchecked event types are omitted.

☒ View History

Start Date & Time

End Date & Time

Event Type

Date/Time	Event Type	Cardholder Name	Card Data	Video
07/12/2021 05:52 AM	Door Open Too Long			
07/12/2021 05:52 AM	Valid Access	Smith, Joe (Card 1)		
07/12/2021 05:52 AM	Valid Access	Mama, Joe (Card 1)		
07/12/2021 05:52 AM	Valid Access	Mama, Joe (Card 1)		

Page 1 22 Per Page

MANAGE PAGE SIZES

The user can control how many events display per page.

1. At the bottom of the page, set the **Number of Events** per page [22, 55, 99, ...]
2. Use the **Page #** droplist to select which page to display.
3. Click the **GO** button to advance to the selected page.

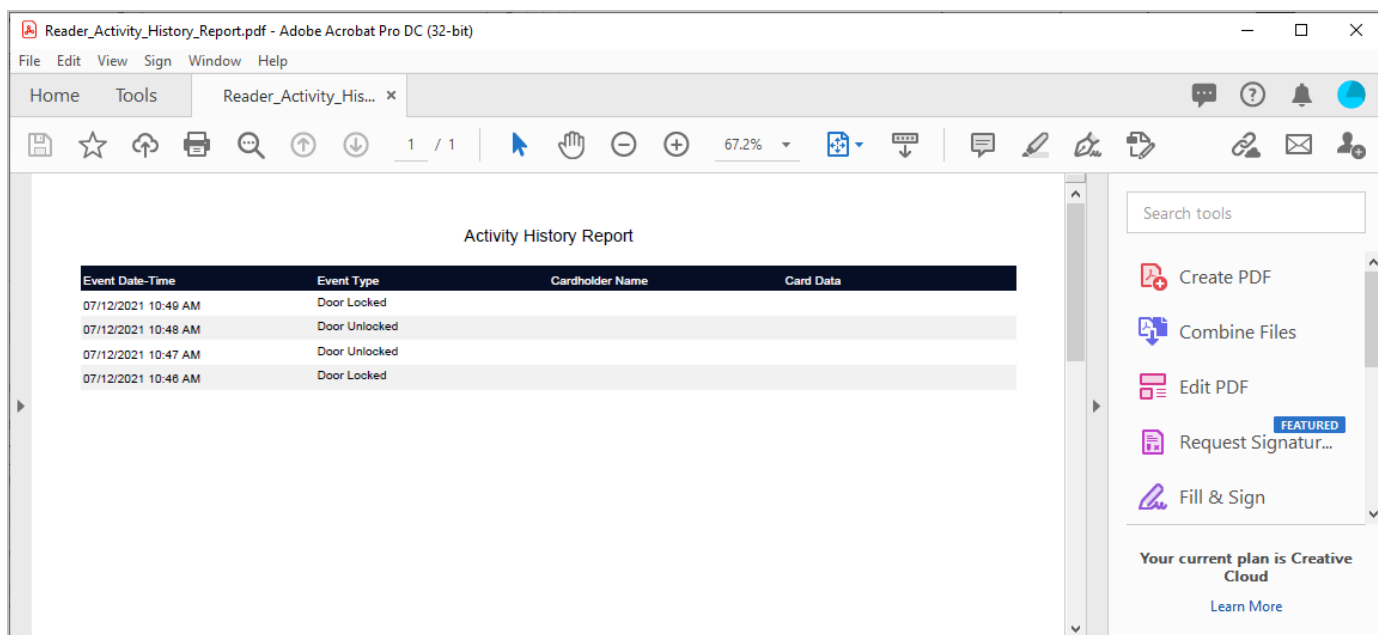
Export Activity History Report

The user can export the *Activity History Report* to Excel or PDF output.

STEPS

1. Select the desired **Loop or Cluster**.
2. Select the desired **Reader**.
3. Enable (check) the **View History checkbox** to open the Activity History page.
4. Enter the **Start date/time**.
5. Enter the **End date/time**.
6. Select an **Event Type** as desired.
 - "check" will include the event type in the report.
 - "uncheck" will exclude or omit the event type from the report.
 - the **Select All checkbox** can be used to toggle on/off all the events.
When checked, the report will include all the activity that occurred at the reader within the start and stop dates.
7. Click the **Get History** button to retrieve the data.
8. Click one of the following buttons to export the report ... or the **PDF** button to export the report to a file.
 - a. Click the **PDF** button to export the report to PDF file.

RESULT: the *Activity History Report* will open in the *PDF Viewer* that is installed on your computer.



- b. Click the **Excel** button to export the report to Excel file

RESULT: the Activity History Report will be generated in an ".XLSX" format and downloaded in your browser. The exported file can be opened from your browser's downloads folder.

The screenshot shows the LaunchPoint Activity History Report interface. At the top, there are filters for 'Start Date & Time' (07/11/2021 10:42 AM), 'End Date & Time' (07/13/2021 10:42 AM), and 'Event Type' (Locked, Unlocked). A 'Get History' button is on the right. Below the filters, there is a 'Choose type of export' section with 'Excel' and 'PDF' buttons. A table displays the activity history with columns: Date/Time, Event Type, Cardholder Name, Card Data, and Video. The table contains four rows of data. At the bottom, a red banner indicates 'Powered by Galaxy Control Systems'. Below the table, a notification bar shows 'Reader_Activity_Hi....xlsx' and 'Excel Report is downloaded' with a 'Show all' button.

Date/Time	Event Type	Cardholder Name	Card Data	Video
07/12/2021 10:49 AM	Door Locked			
07/12/2021 10:48 AM	Door Unlocked			
07/12/2021 10:47 AM	Door Unlocked			
07/12/2021 10:46 AM	Door Locked			

NOTICE: the Excel software may need to be installed, running, and logged-in before the report is exported. If you encounter error messages, try launching excel before you export the report.

IMPORTANT: before you leave or close the LaunchPoint Activity page, go ahead and open/review your exported file to verify your event history was really exported. Some errors may not be noticeable until you attempt to open the file and look at the contents. If the file is empty, re-export the report.

Elevator Readers

This topic covers functionality related to Elevator Readers/Floors, including sending user commands to control floors and schedules, to view video from linked cameras, and retrieve and export activity history.

FEATURED TOPICS

[About Elevator Page](#)

[How to View Video](#)

[Send User Commands](#)

[View Reader Activity Report](#)

[Export Activity Report](#)

About the Elevators Page

The *Elevator Reader Page* allows the user to view video and retrieve/export activity history for an elevator reader, as well as send user commands to a selected floor.

Configuration: Elevator Floors (floor relays) are configured or mapped in the main system programming screens.

RULES OF OPERATION

The following operations can be done from the Elevator Reader page.

- **View Video** (*Live or Search*) for a selected reader.
- **Send User Commands** to a selected floor
(Pulse Floor, Early On, Early Off, Cancel Early On, Cancel Early Off, Refresh Status).
- **View Reader Activity History** for a selected reader.
- **Export Reader Activity** (*Excel or PDF*) for a selected reader.

The user cannot change the elevator programming, schedules, floor mapping, or elevator reader properties from LaunchPoint.

PREREQUISITES AND NOTES

- The user login account must have the appropriate security-level to open the Reader Properties page.
- The user login account must have permissions to issue user commands.
- The floor mapping and any elevator schedules must be created before commands can be issued.
- External software must be installed to view reports in exported formats.

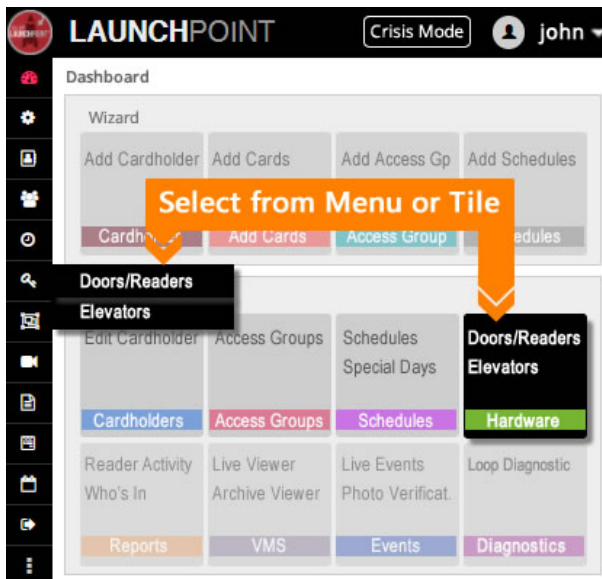
OPEN THE ELEVATORS PAGE

There are two ways to open the Elevators page .

- **Side Menu:** select "Hardware" menu and select Elevators.
- **Dashboard:** select 'Hardware' Tile (under Configure section) and select Elevators.



◀ Hardware icon (from sidebar menu)



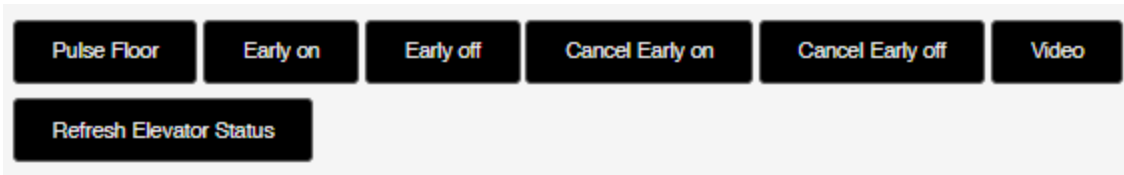
◀ Dashboard (thumbnail)

How to View Video from Elevators Page

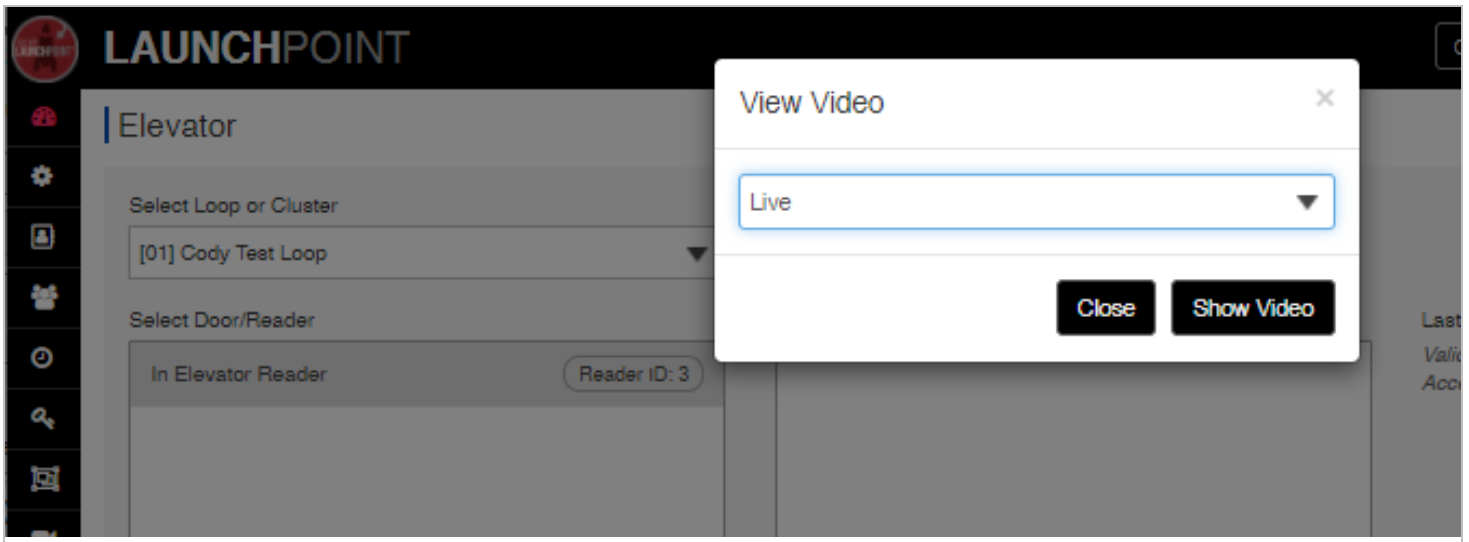
User can view video from the *Elevator Page* by clicking the Video button.

STEPS

1. Select the desired **Loop/Cluster** - *at the top left of the page.*
2. Select the desired **Reader** - *in the reader list.*
3. Click the **Video** button - *at the end of the row of command buttons.*




4. In the *View Video popup*, choose "Live" or "Search" from the droplist.



Notice: if you see the "Contact System Administrator" message, your session may have timed out. Close the message and re-login to LaunchPoint. Reopen the *Elevator Page* and select the **Video** button.

5. Click **Show Video** to open the VMS login page.
6. Sign into the *VMS Webpage* with valid login credentials.


Note: the login page will display for the brand of VMS System you have.



OpenEye[®]
The Cloud Video Platform

Email

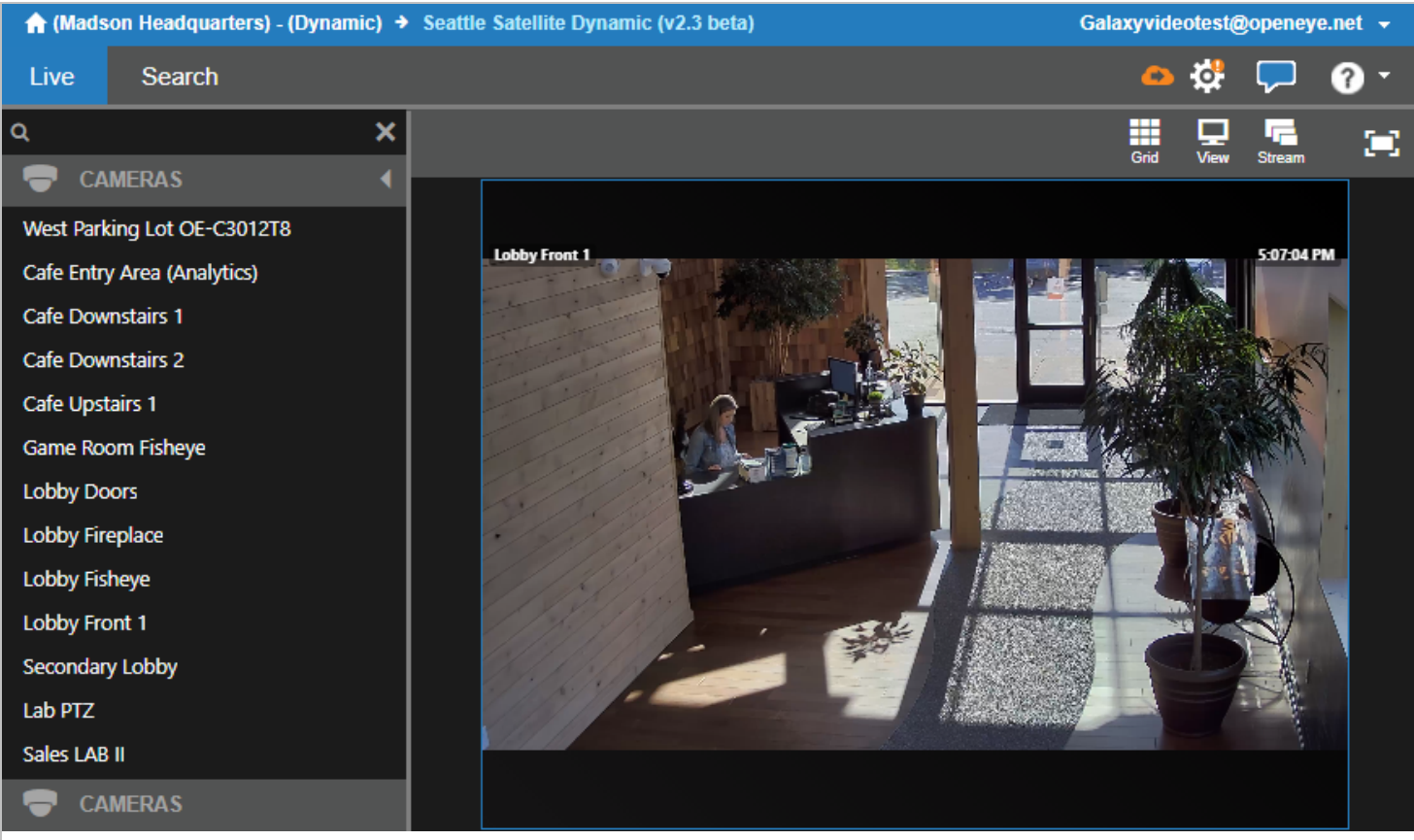
Password

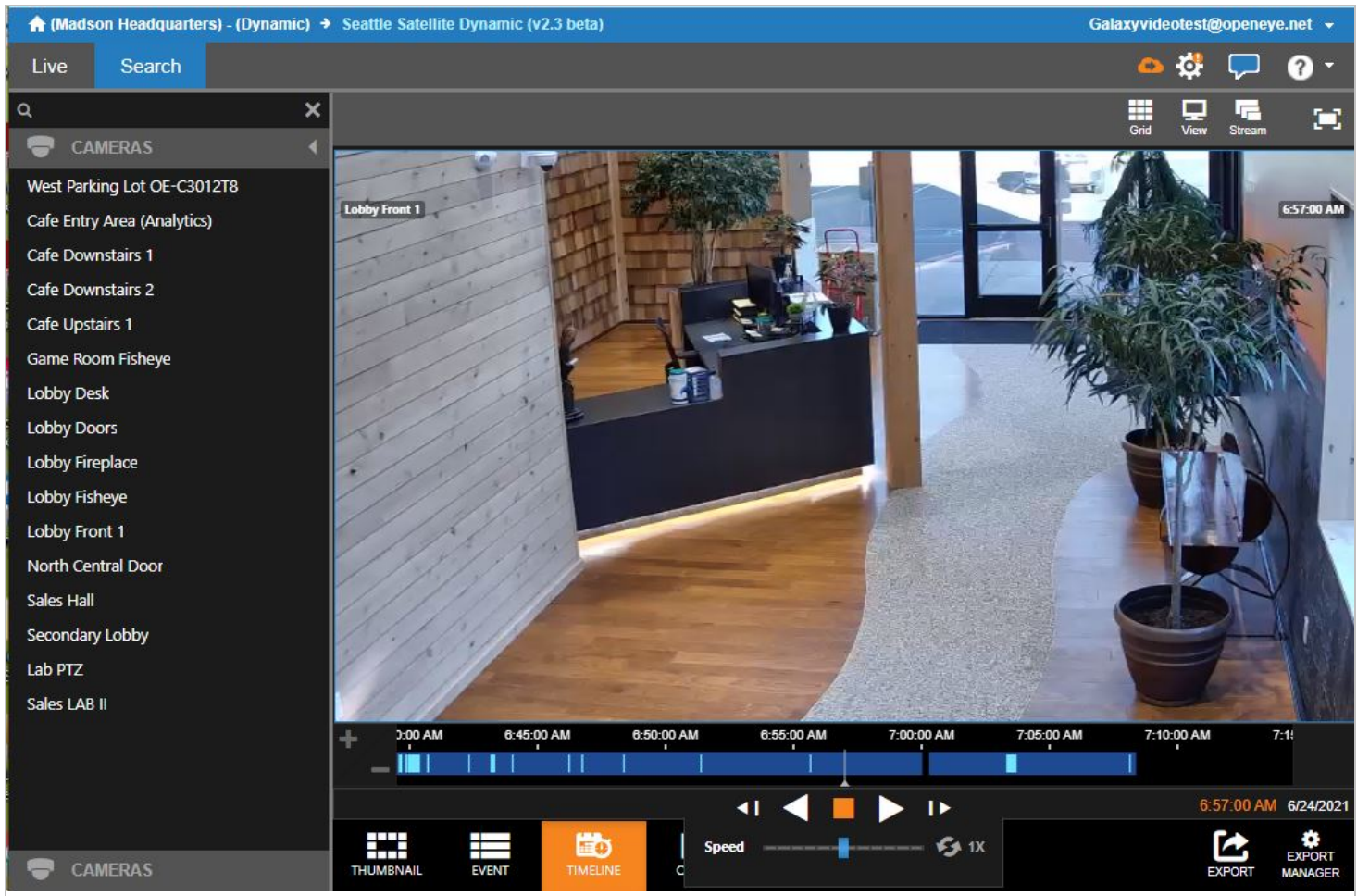
[Forgot password?](#)

[BACK](#) [LOG IN](#)

7. The VMS Camera will display *live video* (or recorded), based on your selection.



(Fig. 1 "Live" video feed)



(Fig. 2 "Search" recorded video playback)

Send User Commands to Relay (Floor)

User commands can be sent to elevator relays (floors) from the Elevator page.

STEPS

1. Select the desired **Loop/Cluster**.
2. Select the desired **Reader/Door**.
3. Select (check) the **Floor Relay(s)** that you want to command.

Note: *Relay status* is reflected by the color of the text.

Red Relay text = OFF. Black Relay text = ON.

Elevator

Select Loop or Cluster

Select Door/Reader

In Elevator Reader

Reader ID: 3

Select Floor/Relay

☐ Floor 01 - On
☒ Floor 02 - On
☐ Floor 03 - Off
☐ Floor 04 - Off
☐ Floor 05 - Off
☐ Floor 06 - Off
☐ Floor 07 - On
☐ Floor 08 - On

Last access event

Valid Access (6/28/2021 11:23:13 AM)

Accessed By : CM CM

Pulse Floor

Early on

Early off

Cancel Early on

Cancel Early off

Video

Refresh Elevator Status

4. Send the **User Command** as desired ...

- Pulse Floor
- Early on / Early off
- Cancel Early on / Cancel Early off
- Refresh Elevator Status

Pulse Floor

Early on

Early off

Cancel Early on

Cancel Early off

Video

Refresh Elevator Status

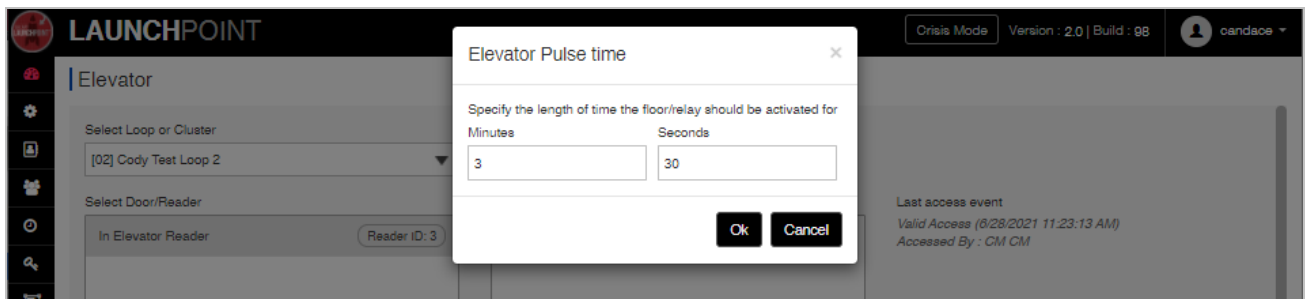
(See each command below)

PULSE FLOOR

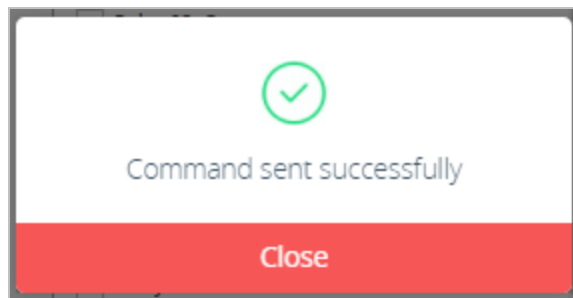
This command sends a pulse (momentary unlock) to the selected relay.

- Clicking the **Pulse Floor** button will send a **Pulse command** the selected relay.
 - In the *Elevator Pulse Time popup*, enter the **amount of time** (mm/ss) you want the pulse to last.
 - Click the **OK button** to issue the pulse command.

Clicking Cancel will close the window without sending a pulse.



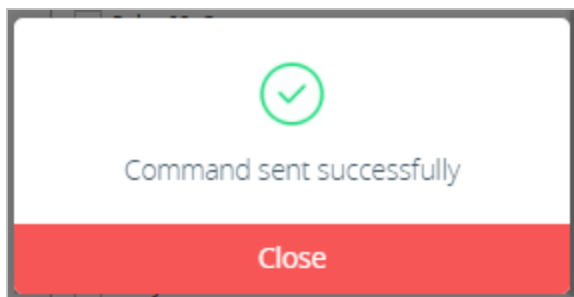
- Click Close to close the Command Success message.



EARLY ON / EARLY OFF

These commands allow the user to turn the selected relays on (or off) before their assigned schedule takes effect - i.e., turns relays on or off early.

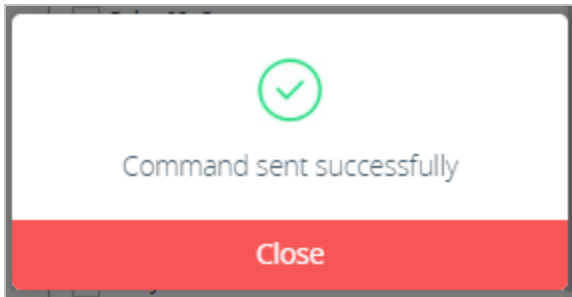
- Click the **Early On** button = to send a **Early On** the selected relays.
Use this command on relays that are OFF, to turn them on early.
- Click the **Early Off** button = to send an **Early Off** the selected relays.
Use this command on relays that are ON, to turn them off early.



CANCEL EARLY ON / CANCEL EARLY OFF

These buttons will cancel the Early On or Early Off command you previously issued. You must select the relay to issue the command.

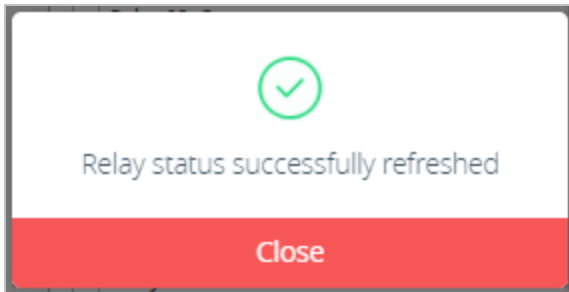
- d. Clicking **Cancel Early On** sends ***Cancel Early-On*** to selected relays.
Use this command to remove an *Early On* command.
- e. Clicking **Cancel Early Off** sends a ***Cancel Early-Off*** to selected relays.
Use the command to remove an *Early Off* command.



REFRESH ELEVATOR STATUS

The Elevator page is not live. This command refreshes the Elevator page to ensure you are seeing the correct relay statuses.

- d. Clicking **Refresh Elevator Status** sends a ***Refresh command*** to the page/relays.
Use this command to update the relay list and see the current status of all relays.



View Reader Activity History

User can view the *Activity History* for one reader at a time.

The history can be viewed online or exported to an Excel file or PDF file.

STEPS

1. Select the desired **Loop or Cluster**.
2. Select the desired **Reader**.
3. Enable (check) the **View History checkbox** to open the Activity History page.
4. Enter the **Start date/time**.
5. Enter the **End date/time**.
6. Select the **Event Types** as desired.
 - a. "**check**" will include the event type in the report.
 - b. "**uncheck**" will exclude or omit the event type from the report.
 - c. the **Select All checkbox** can be used to toggle on/off all the events.

When checked, the report will include all the activity that occurred at the reader within the start and stop dates.

7. Click the **Get History** button to retrieve the data.

☒ View History

Start Date & Time

End Date & Time

Event Type

Date/Time	Event Type	Cardholder Name	Card Data	Video
07/12/2021 05:52 AM	Door Open Too Long			
07/12/2021 05:52 AM	Valid Access	Smith, Joe (Card 1)		
07/12/2021 05:52 AM	Valid Access	Mama, Joe (Card 1)		
07/12/2021 05:52 AM	Valid Access	Mama, Joe (Card 1)		

Page 1

22 Per Page

MANAGE PAGE SIZES

The user can control how many events display per page - 22, 55, 99.

1. At the bottom of the page, set the Number of Items per page
2. Use the page droplist to select a page to display.

3. Click the **GO** button to advance to the selected page.
-

Export Activity History Report

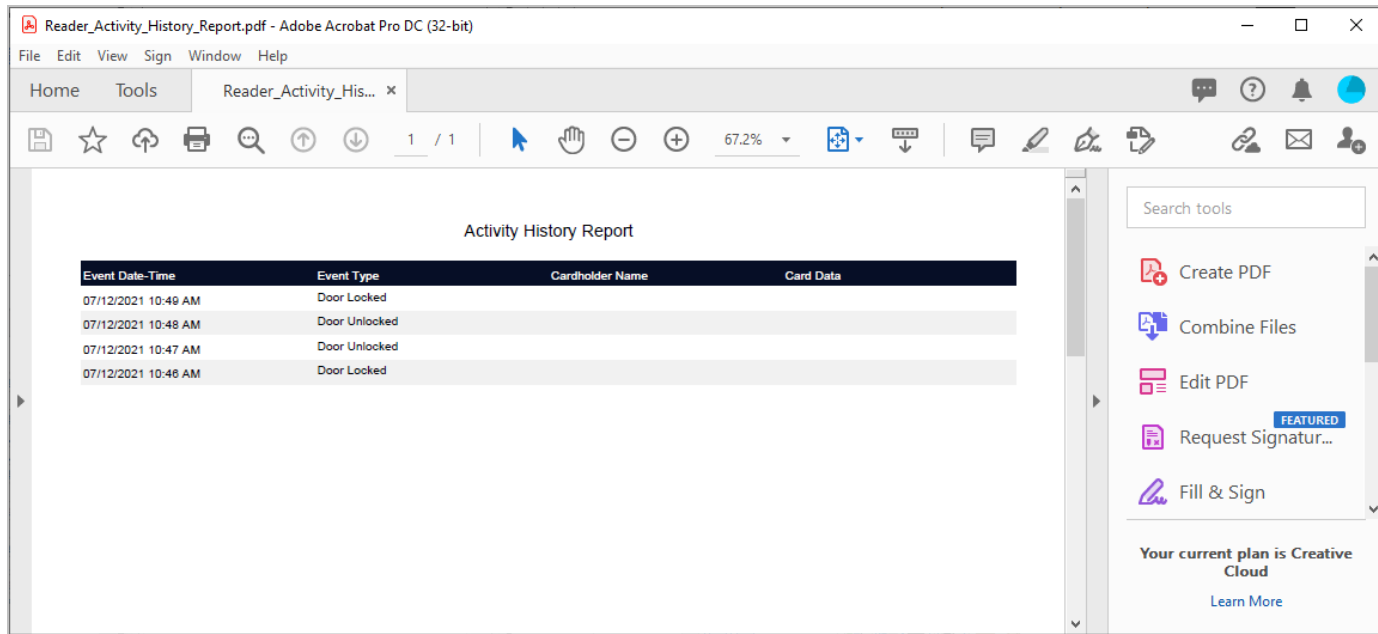
The user can export the *Activity History Report* to Excel or PDF output.

STEPS

1. Select the desired **Loop or Cluster**.
2. Select the desired **Reader**.
3. Enable (check) the **View History checkbox** to open the Activity History page.
4. Enter the **Start date/time**.
5. Enter the **End date/time**.
6. Select an **Event Type** as desired.
 - a. "**check**" will include the event type in the report.
 - b. "**uncheck**" will exclude or omit the event type from the report.
 - c. the **Select All checkbox** can be used to toggle on/off all the events.

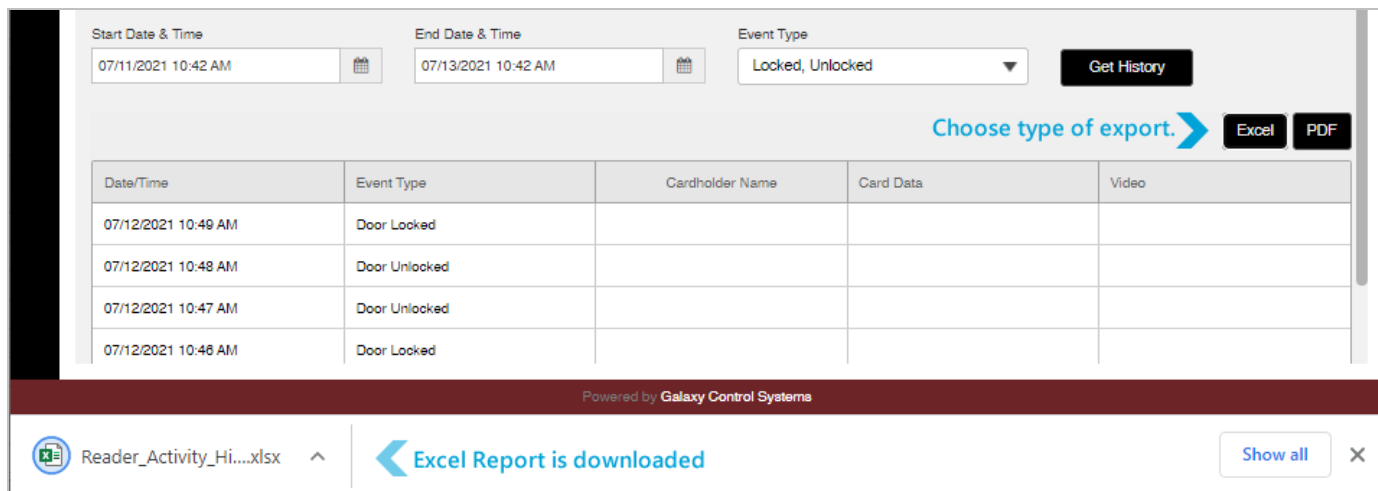
When checked, the report will include all the activity that occurred at the reader within the start and stop dates.
7. Click the **Get History** button to retrieve the data.
8. Click one of the following buttons to export the report ... or the **PDF** button to export the report to a file.
 - a. Click the **PDF** button to export the report to PDF file.

RESULT: the Activity History will open in the *PDF Viewer* that is installed on your computer.



- b. Click the **Excel** button to export the report to Excel file

RESULT: the Activity History will be generated in an ".XLSX" format and downloaded via your browser. The exported file can be found in the browser's *Downloads* folder.



NOTICE: the Excel software may need to be installed, running, and logged-in before the report is exported. If you encounter error messages, try launching excel before you export the report.

IMPORTANT: Go ahead and open/review your exported file to verify your event history was really exported before you leave the LaunchPoint Activity page. Some errors may not be noticeable until you attempt to open the file and look at the contents.

Loop Diagnostics

This topic covers how to execute **diagnostic commands** in the *Loop Diagnostics Page* and related information.

FEATURE TOPICS

[Loop Diagnostics Overview & Prerequisites](#)

[How to Open Diagnostics Page](#)

[How to Send a Diagnostic Command](#)

[Available Commands \(Diagnostic use\)](#)

- [Get Card Count](#)
- [Get Hardware Information](#)
- [Get Logging Information](#)
- [Activate Crisis Mode](#)
- [Reset Crisis Mode](#)
- [Send a PING Command](#)

Loop Diagnostics Overview & Prerequisites

The **Loop Diagnostics** page allows an user to send *diagnostic commands* to all online controllers within a chosen Loop/Cluster.

PREREQUISITES & NOTES

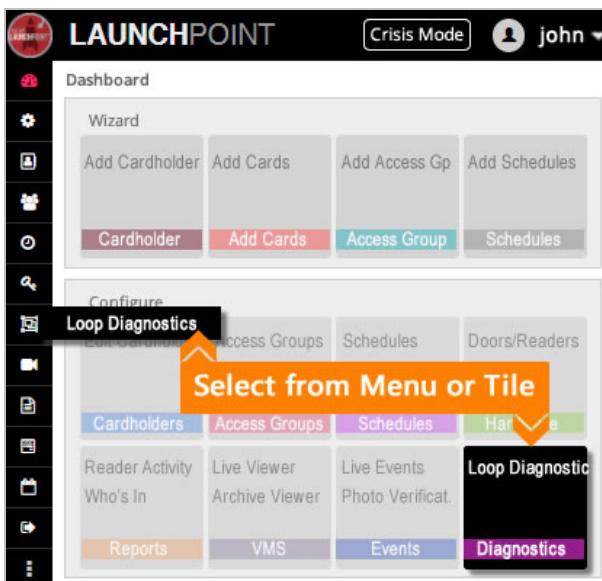
- The user login account must have the appropriate security-level to open the Loop Diagnostics screen.
- The user login account must have permissions to issue user commands.

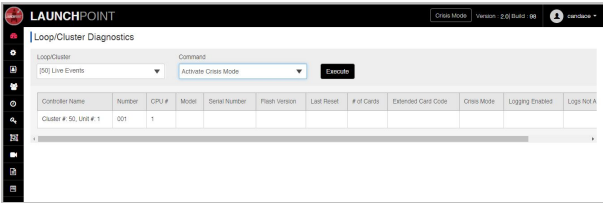
NOTICE: Controllers cannot receive diagnostic commands while they are offline (shaded red). Controllers must be online to respond to diagnostic commands.

How to Open the Diagnostics Page

There are two ways to open the *Loop Diagnostics Page* ...

- **Side Menu:** select "Loop Diagnostics" menu icon or option.
- **Dashboard:** select 'Diagnostics' Tile (under Configure section)





When the *Loop Diagnostics Page* opens, it will be empty until the user sends a command to a loop/cluster. (Offline controllers will not return data, but they will display in the list shaded red.)

Send a Diagnostic Command

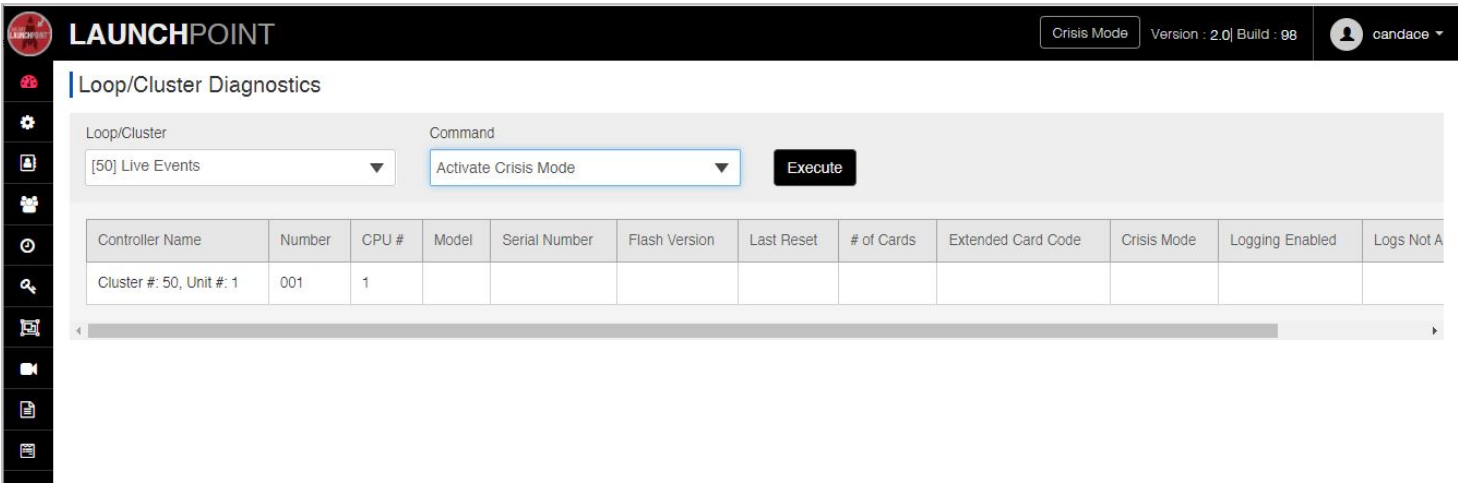
The user can open the *Loop Diagnostics Page* from the Side Menu or the Dashboard Tile.

STEPS

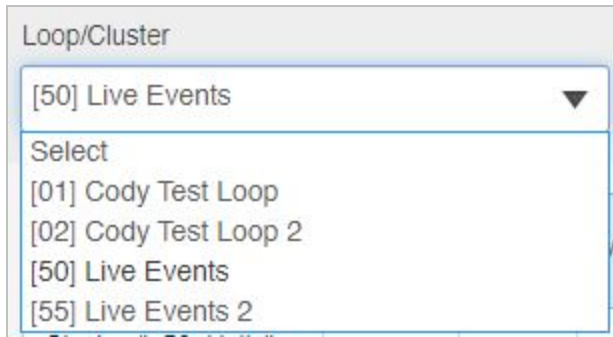
1. Click the **Crisis Mode** button on the LaunchPoint page header .



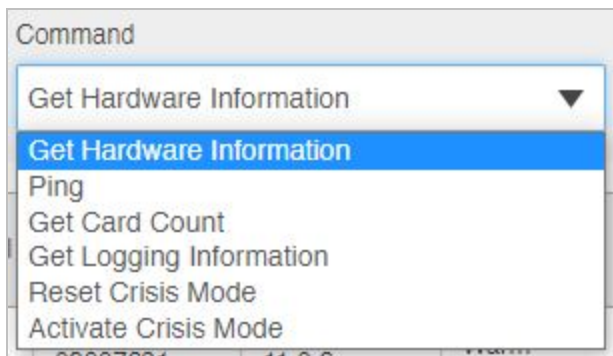
2. When the *Loop Diagnostics* window opens, no data will be showing.



3. Select the **LOOP/CLUSTER** you want to operate on.



4. Select the **COMMAND** you want to send.



5. Click the **EXECUTE** button to send the command to the chosen loop/cluster.



6. Click **Close** to dismiss the Success popup message.

Notice that offline panels (*shaded in red*) will not respond to user commands.

The screenshot shows the LaunchPoint web application interface. At the top, the browser address bar displays 'ccdev.accessonthegeo.com/cc/LoopClusterDiagnostics.aspx'. The page header includes the 'LAUNCHPOINT' logo, a 'Crisis Mode' button, and version/build information: 'Version : 2.0 | Build : 97'. The user is logged in as 'candace Customer 1'.

The main section is titled 'Loop/Cluster Diagnostics'. It features two dropdown menus: 'Loop/Cluster' set to '[01] Cody Test Loop' and 'Command' set to 'Get Card Count'. An 'Execute' button is visible.

A modal dialog box is displayed in the center, indicating 'Command sent successfully' with a green checkmark icon and a 'Close' button.

Below the modal, a table displays diagnostic data for various controllers. The table has the following columns: Controller Name, Number, CPU #, Model, Serial Number, Flash Version, Last Reset, # of Cards, Extended Card Code, Crisis Mode, Logging Enabled, Logs Not Acked, and Log Not sent.

Controller Name	Number	CPU #	Model	Serial Number	Flash Version	Last Reset	# of Cards	Extended Card Code	Crisis Mode	Logging Enabled	Logs Not Acked	Log Not sent
Cluster #: 1, Unit #: 1												
Cluster #: 1, Unit #: 2												
Cluster #: 1, Unit #: 3	001	1	0	03019473					Inactive	Yes	17	0
CPU tied to Bosch Panel	001	1	0	03006346					Inactive	Yes	10	0

RESULT OF SENDING DIAGNOSTIC COMMANDS

The *Loop Diagnostic* page will display the results for each online controller in the selected Loop/Cluster.

The screenshot shows the 'Loop/Cluster Diagnostics' page with 'Loop/Cluster' set to '[55] Live Events 2' and 'Command' set to 'Get Hardware Information'. The 'Execute' button is visible.

The table below displays the results for the selected loop/cluster. Offline controllers are shaded in red.

Controller Name	Number	CPU #	Model	Serial Number	Flash Version	Last Reset	# of Cards	Extended Card Code	Crisis Mode	Logging Enabled	Logs Not Acked	Log Not sent
Cluster #: 55, Unit #: 1												
Cluster #: 55, Unit #: 2	001	1	635	03007597	11.0.6	Warm Reset		NO	Inactive	Yes	7	0
Cluster #: 55, Unit #: 3(Office)												

The offline controllers are shaded in red to indicate that those panels are offline.

See [Available Commands](#) (next) for instructions on each user command.

Available User Commands

This section covers how each of the user commands work.

GET CARD COUNT

Executing a **Get Card Count** command will send a *card count* request to each online panel in the selected Loop/Cluster.
(offline controllers cannot respond)

USER TIP: This command is useful to determine if the expected number of cards are in the controller.

For Example: if you know 50 employees should be in a controller for access permissions to a specific door, and the card count is lower than 50, then you know that some of your cards are not loaded to the controller yet - for some reason.

Things you can do to troubleshoot this situation ...

You should reload all the data to the controller and recheck card count.

FYI: You get a *Not In System* message when a card has not been enrolled in the system (thus you need to enroll the card and give it access).

FYI: You get an *Invalid Access* message when a card is not in the controller for some reason, or is in the controller but doesn't have access to the door (access group) at the time the card is being presented (schedule). Be sure all data has been loaded to the controller, and the Cardholder's *access card* has been given permissions to the loop/cluster, and is assigned to an access group that includes the door in question for the time period (schedule) that is needed (see Cardholder programming (assigning locations and access permissions), Access Group programming, and Schedules programming. Be sure the card and cardholder are active in the Cardholder programming (cardholder information and card data).

RESULT: the "**# of Cards**" field displays the number of cards each controller currently contains in memory.

Loop/Cluster

[50] Live Events ▼

Command

Get Card Count ▼

Execute

Controller Name	Number	CPU #	Model	Serial Number	Flash Version	Last Reset	# of Cards	Extended Card Code
Cluster #: 50, Unit #: 1	001	1	0	03007691	11.0.6	Warm Reset	23	NO

GET HARDWARE INFORMATION

Executing a **Get Hardware Information Command** will retrieve the hardware data from each online panel in the selected Loop/Cluster.

(offline controllers cannot respond - as shown red shading in the image below)

Fields of Interest

- Number - (numeric) controller ID / unit ID
- Model - (numeric) identifies the CPU board model number (600/635).
- Serial Number - (numeric) CPU Board serial number
- Flash Version - the current s28 Flash version running in the CPU
- Last Reset - (status) Warm or Cold Reset, whichever was the last done.
- Extended Card Mode - (yes/no) identifies whether the controller is operating in extended card mode.
- Crisis Mode - status - shows whether crisis mode is active or inactive.
- Red shading means the controller is programmed in the system but is offline currently.

RESULT: the fields in the table display all the data stored in the controller (except *Card Count*).

Loop/Cluster Diagnostics

Controller Name	Number	CPU #	Model	Serial Number	Flash Version	Last Reset	# of Cards	Extended Card Code	Crisis Mode	Logging Enabled	Logs Not Acked	Log Not sent
Cluster #: 55, Unit #: 1												
Cluster #: 55, Unit #: 2	001	1	635	03007597	11.0.6	Warm Reset		NO	Inactive	Yes	7	0
Cluster #: 55, Unit #: 3(Office)												

The offline controllers are shaded in red to indicate that those panels are offline.

GET LOGGING INFORMATION

Executing a **Get Logging Information Command** will retrieve the controller log data from each online panel in the selected Loop/Cluster.

(offline controllers cannot respond)

Fields of Interest

- Logging Enabled - (yes/no)
- Logs Not Acked - (numeric) number of logs not acked.
- Logs Not Sent - (numeric) number of logs not sent.

RESULT: the fields in the table display the logging data from the controller (in last three fields).

Loop/Cluster Diagnostics

Controller Name	Number	CPU #	Model	Serial Number	Flash Version	Last Reset	# of Cards	Extended Card Code	Crisis Mode	Logging Enabled	Logs Not Acked	Log Not sent
Cluster #: 50, Unit #: 1	001	1	635	03007691	11.0.6	Warm Reset		NO	Inactive	Yes	9	0

SEND CRISIS MODE COMMANDS

The user can "Activate Crisis Mode" or "Reset Crisis Mode" for controllers in a selected Loop/Cluster.

(offline controllers cannot respond)

IMPORTANT: See the **Crisis Mode Topic** for instructions about activating Crisis Mode using the **Crisis Mode Button** to issue a Crisis Mode Command to all the loops/clusters in the system simultaneously . Sending a crisis mode command from the Diagnostics page can only be done for one loop/cluster at a time, which may not be as quick as you need in a real crisis situation.

USER TIP: You can use the Diagnostics page to test or verify and diagnose how crisis mode is behaving in your system from the Diagnostics page - which may helpful when validating the implementation of your crisis mode programming .

Fields of Interest

- Controller Name - will be in red text if crisis mode is active.
- Crisis Mode - (status) indicates if Crisis Mode is "active" or "inactive" at a controller

RESULT: When user **Activates Crisis Mode**, the *controller name* is red and Crisis Mode status is "Active".

Only the online controllers in the selected loop are activated - see Crisis Mode topic on how to use the **Crisis Mode Button** to activate crisis mode system-wide.

Loop/Cluster Diagnostics

Loop/Cluster

Command

[50] Live Events

Activate Crisis Mode

Execute

Controller Name	Number	CPU #	Model	Serial Number	Flash Version	Last Reset	# of Cards	Extended Card Code	Crisis Mode	Logging Enabled	Logs Not Acked	Log Not sent
Cluster #: 50, Unit #: 1	001	1	635	03007691	11.0.6	Warm Reset		NO	Active	Yes	29	0

RESULT: When user **Resets Crisis Mode**, the Crisis Mode field returns to "Inactive" status.

Loop/Cluster Diagnostics

Loop/Cluster

Command

[50] Live Events

Reset Crisis Mode

Execute

Controller Name	Number	CPU #	Model	Serial Number	Flash Version	Last Reset	# of Cards	Extended Card Code	Crisis Mode	Logging Enabled	Logs Not Acked	Log Not sent
Cluster #: 50, Unit #: 1	001	1	635	03007691	11.0.6	Warm Reset		NO	Inactive	Yes	48	0

PING CONTROLLERS

Executing a **Ping Command** will send a *ping* to each online panel in the selected Loop/Cluster.

(offline controllers cannot respond).

Fields of Interest

- Number - (numeric) controller ID / unit ID
- Model - (numeric) identifies the CPU board model number (600/635).
- Serial Number - (numeric) CPU Board serial number
- Flash Version - the current s28 Flash version running in the CPU
- Last Reset - (status) Warm or Cold Reset, whichever was the last done.

RESULT: the data for each available field is populated for each controller in the selected loop/cluster.

Loop/Cluster Diagnostics

Loop/Cluster
[50] Live Events ▼

Command
Ping ▼

Execute

Controller Name	Number	CPU #	Model	Serial Number	Flash Version	Last Reset	# of Cards	Extended Card Code	Crisis Mode	Logging Enabled	Logs Not Acked	Log Not sent
Cluster #: 50, Unit #: 1	001	1	0	03007691	11.0.6	Warm Reset		NO	Inactive	Yes	40	0

You can verify the individual controller by the CPU Board serial number

Live Events

The **Live Events Feature** supports the ability to **Monitor Live Events**, **Handle Alarm Events**, and **Send User Commands** - *configuration of event settings and alarm activity is required.*

FEATURED Topics

Operation of Events Page

- Process of Operating Events Page
- Events & Alarm Logging Explained

Configure Event Settings

- Monitor Live Events
- User Commands (Events page)

Handle Alarm Events

- Configure Alarm Events
 - User Commands (Alarms window)
-

Event Overview

This topic provides an Operation Overview of the **Live Events** page including Prerequisites .

FEATURED TOPICS

Overview of Operation

- Process of Operating the Events
 - Events & Alarm Logging Explained
-

Overview of Operation

The *Live Events Page* and *Alarm Events Popup* allow an user to monitor real-time events and alarms that occur from system activity.

System **events** are logged to the *Events Page* whenever readers, doors, inputs, controllers, boards, etc. are actively transmitting events in the system. If any of these system events (or their associated hardware) are

programmatically configured to identify an **alarm event**, then the system will log those alarm events to the *Alarm Events Popup*.

Prerequisites & Notes

- Users must have the appropriate account permissions to view events and alarms (configured by system administrators).
- Users must have permissions and a VMS system login/account to be able to view video from linked cameras.

The Process of Operating the Events Page

This section describes the top-down process of using the Events Page. This will describe what users can do in the Events page.

1. To see **live events**, you must set up the 'event types' and 'devices' you want to include (see *Configure Settings*).
2. To see live **alarm events**, you must set up the 'alarm types' and 'devices' you want to include (see *Configure Alarms*).
3. Once the settings are configured, the events and alarms will start logging/displaying.
4. Event Functions: the user can interact with the individual events to do things like ...
 - **Add Card Button** ('Not In System' events only)
 - **Forgive Passback** *
 - **Disable Cardholder** *
 - **View Photograph** *
 - **View Properties** * (cardholder)
 - **View Video** * from the associated camera

* The *context menu* is dynamic - which means some commands are conditionally disabled based on the type of event selected (i.e., card event vs. door event, schedule event, etc.).

* some options are conditionally available in the context menu based on the type of event - i.e., card/reader event.

5. Alarm Functions: the user can interact with the *Alarm Popup** to do things like ...
 - **Ignore button** (individual alarm)
 - **View Video¹ button** (individual alarm)
 - **Ignore All button** (applies to all alarms)
 - **Acknowledge All button** (entering an *user text message* may be needed - configurable)

Note: Ignoring or acknowledging an alarm will stop the associated *audible alarm beeper*. Acking / ignoring all alarms will stop the alarm beeper for all incoming alarms that are currently displayed. New alarms may start a beeper again.

* the *Alarm Popup* will not open if alarm events are not configured to display in the *Settings* and *Alarm Activity Settings* windows.

1 - the *Video Viewer Login Page* will open only if a camera is linked to the device causing the alarm. User must have a valid VMS login with permissions to view the camera.

6. The *Event Page* will continuously log events and alarms until the page becomes *idle* or *inactive* for too long (meaning **unattended**).

The incoming events and alarms do not count as *user activity* or *attendance* in the page.

- a. User activity is when an user clicks interactive features on the Events page or Alarm window; such as clicking *buttons or menu commands*.
- b. When the page becomes inactive/idle, LaunchPoint will start an *audible countdown timer* (beeper).
 - Choose "Stay Logged In" before the *countdown timer* elapses, or the event and alarm logging will be interrupted.
 - If the user does not choose to *stay logged in*, the page session will become disconnected. The user Login will time-out.

7. The user can close the *Events Page* (browser tab) to stop monitoring the events.

LIVE EVENTS & ALARM LOGGING EXPLAINED

LaunchPoint is able to log real-time incoming **events** and **alarm events** to a *Live Events Page* and *Alarms Popup Window*.

- The *Live Events Page*: allows the user to continuously monitor system activity in a separate browser screen (tab) that uninterrupted by other features and screens.
- The *Alarms Popup Window* (modal): allows the user to continuously monitor incoming alarm events in the same Events page (tab) and manage those alarms from the popup window.

Opening the Events page the First Time ...

When the *Events Page* opens the first time, the user must configure which events and alarms will be monitored.

- Events are set up in the *Settings Window*.
- Alarms are set up in both the *Settings* and *Alarm Activation Windows*.



How does the Events Page work?

The *Live Events Page* opens in a new browser tab and functions independently from other LaunchPoint screens and features. This allows an user to monitor events and alarms while the main *Dashboard Page* remains open for other functions.

In the *Live Events page*, an user can do the following ...

1. continuously monitor **events** and **alarm events** (configurable)
2. send commands using the command buttons and menu options

Note - the context menu is displayed by clicking on an incoming event message in the Event column of the events table.

See more on User Commands for list of commands.

How long will Live Events log to the Event screen?

The *Live Events Page* (browser tab) will continuously log events and alarms until the page becomes idle too long.

LaunchPoint considers activity to be when the user clicks elements within the Events page, such as buttons, options, or user commands.

Page Unattended Alert! LaunchPoint will sound an *audible beeping signal* and displaying a *count-down timer messagebox* that requests the user to "respond" and confirm the page is still being monitored. If the user responds, the live events will resume logging to the Event page. If the countdown timer elapses, the events are stopped and the Events page is closed.

How do Alarm Events display?

When Alarm Events occur, LaunchPoint opens the *Alarm Event popup* (modal window) that displays in the foreground of the Events screen. The incoming Events continue to log in the background.

Alarm Events may also sounds an *audible "beeping" signal* on the computer speakers when an alarm occurs.

- If user resolves an alarm, the correlating beeper will stop.
- If the user ignores-all or acknowledges-all alarms, then all beepers should stop for the current alarms.
- If the beeping restarts that means a new alarm has been detected that is not resolved.

NOTICE! Configuration of *Alarm Activity Settings* is required to choose which Alarm Events you want to see. Therefore it is possible to filter out some of the Loops/Clusters, controllers, or devices in the system.

NOTICE! Computer speakers must be available to play audible feedback. Alarm signals may not be audible if headsets/headphones are connected.

How does a user resolve Alarms?

The user can choose to resolve alarms *individually* or *all together* by using the *ignore* or *acknowledge* buttons.

If the user chooses to acknowledge an alarm, the *Acknowledge Textbox* may open. The user can enter any text about the alarm as needed (configurable).

NOTE: The user can also *View Video* from the camera that is linked to the hardware that is triggering the alarm.

The screenshot shows the 'Alarm Events' window. At the top right is a 'Mute' checkbox. Below it, an event is listed with details: Device: Cluster: 055, Cont: 002, Brd: 1, Sect: 2-0; Event Time: 6/22/2021 6:45:10 PM; Event: Not In System. Below the event are 'Show Video' and 'Ignore' buttons. At the bottom of the window are 'Acknowledge All' and 'Ignore All' buttons. An 'Acknowledge' modal is open, showing a text input field with 'CER' and 'Close'/'Save' buttons. Annotations include: a blue arrow pointing to the 'Mute' checkbox with text 'Check to "mute" incoming alarms (alarms muted for user-selected duration)'; a blue arrow pointing to the 'Show Video' button with text 'Click to launch the VMS Viewer * (view live video from linked camera)'; a blue arrow pointing to the 'Ignore' button with text 'Click to ignore an individual alarm'; a blue box on the left with text '* operator must provide valid login & password open the VMS Viewer. Login must have permissions to view the selected camera.'; a blue arrow pointing to the 'Acknowledge' modal with text 'Type text as appropriate. (only for Acknowledged Alarms)'; a blue arrow pointing to the 'Acknowledge All' button with text 'Click to Acknowledge All pending alarms'; and a blue arrow pointing to the 'Ignore All' button with text 'Click to Ignore All pending alarms'.

Alarm Events ☐ Mute

Device : Cluster: 055, Cont: 002, Brd: 1, Sect: 2-0
Event Time : 6/22/2021 6:45:10 PM
Event : Not In System

Show Video Ignore

Acknowledge

CER

Close Save

Show Video Ignore

Acknowledge All

Ignore All

* operator must provide valid login & password open the VMS Viewer. Login must have permissions to view the selected camera.

Check to "mute" incoming alarms
(alarms muted for user-selected duration)

Click to launch the VMS Viewer *
(view live video from linked camera)

Click to ignore an individual alarm

Type text as appropriate.
(only for Acknowledged Alarms)

Click to Acknowledge All pending alarms

Click to Ignore All pending alarms

How many events display in the Events screen?

The event screen (browser tab) will display a up to 500 events in the browser window.

The user can adjust how many Events to display per page and then chose which page to see as the buffer fills up.

Which events can you display?

You must configure the *Events Page* to display the events you want to see in the *Settings window*.

Checked = display the event when it occurs.

Unchecked = do not display the event even if it occurs.

Event Types

- **Activity** = is any type of activity in the system that occurred at the selected reader(s).
 - **Alarm** = is any type of system alarm that occurred at the selected reader(s).
 - **Not in System** = is a not-in-system that occurred at the selected reader(s).
-
-

HOW TO VIEW LIVE EVENTS

See the "[LIVE EVENTS & ALARM LOGGING EXPLAINED](#)" on [page 183](#) section if you are new to the Event Viewer.

OPEN THE EVENT VIEWER

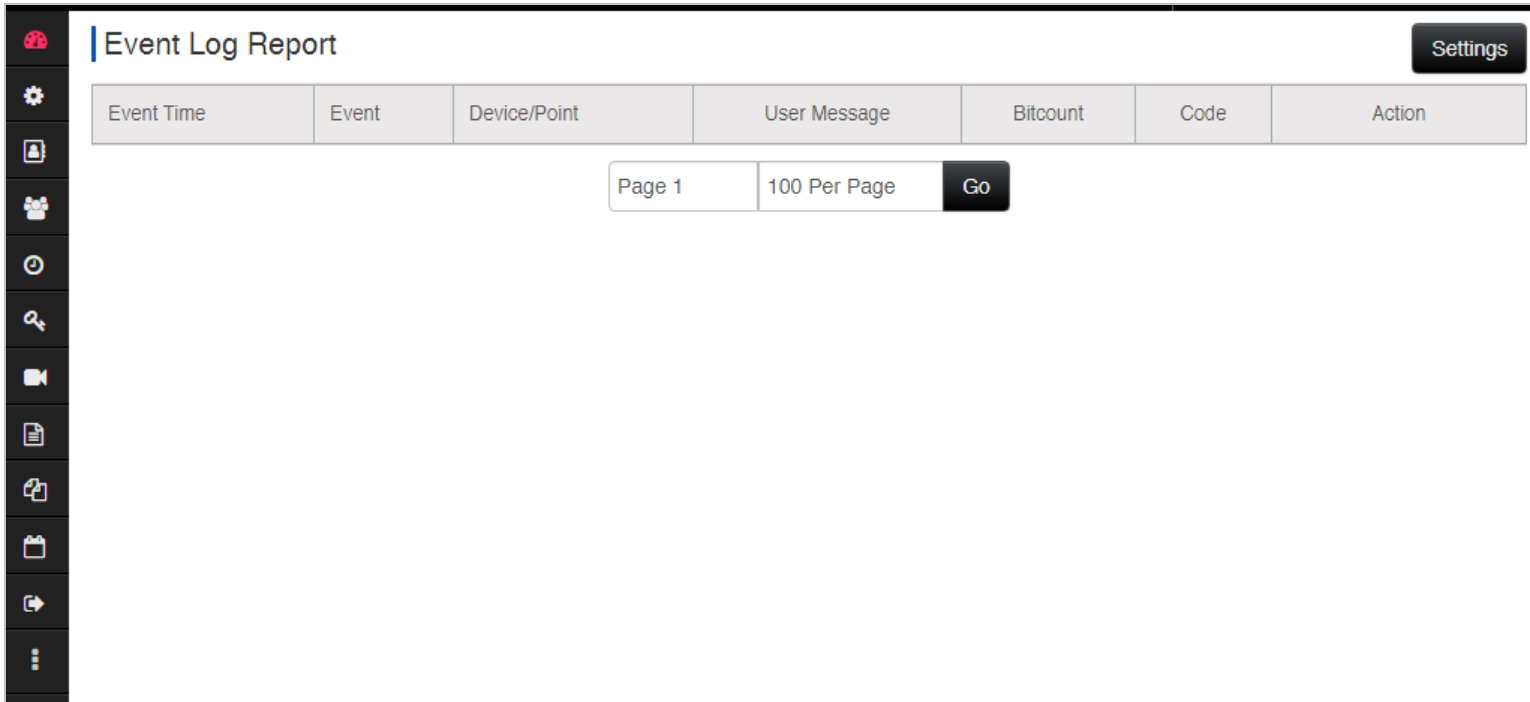
To open the Event Log Viewer, go to the Dashboard screen and click the **View Events** tile, under the Configure section.

Or open the Event Log Viewer from the left side Menu.

Click on thumbnails to open and close them.



← Events Log menu icon



[← Event screen](#)

HOW TO VIEW LIVE EVENTS

1. Click the **Settings** button in the Event screen.
2. Select any combination of Readers you want to see events for.
3. Select any Event Types you want to see.
there are several types, including activity events, alarm events, and not in system.
4. Click **Save** button to save your choices and close.
5. In the Eventscreen, choose the *number of events* you want to display per screen.
there are 3 choices ... 100, 250, 500.
6. Click the **Go** button to pull the Log Report.

Monitoring Events

This topic covers monitoring Live Events and sending User Commands - including configuring settings.

FEATURED TOPICS

[Configure Events \(Settings\)](#)

[Monitor Live Events](#)

[User Commands](#)

Configure Events (Settings)

The first time the *Live Events Page* is opened, you must configure which events to monitor. This is done in the Settings window (modal).

The Settings window lets the user choose which *hardware devices** to monitor and configure which *event messages* to see in the *Live Events Page*.

- **Checked** = monitor the device* and its events when they occur.
- **Unchecked** = do not monitor this device or event.

* Hardware devices include readers/doors, inputs, controllers, and third-party alarm panels.

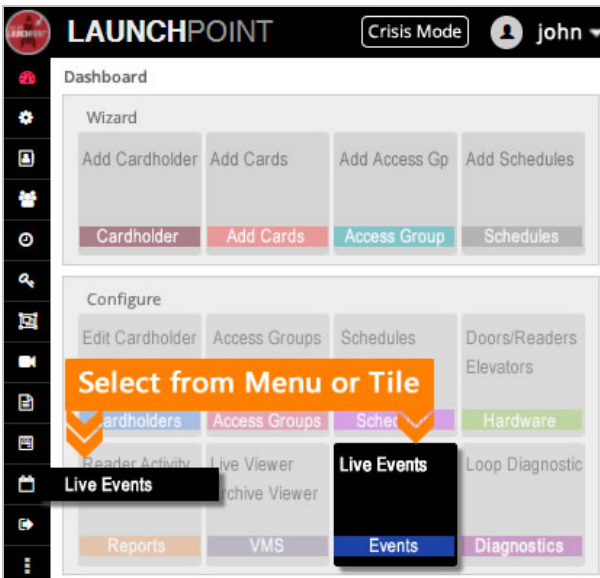
PREREQUISITES & NOTES

- (in the VMS system) User must have a valid *VMS system login/account* and *camera permissions* in order to view video from specific cameras.
- User must have appropriate permissions to view events and alarms.
- You must enable the hardware Device you want to monitor in the [Settings window](#).
- You must enable the Event Types (types of messages) you want to see in the [Settings window](#).
- If you want to monitor armed inputs, you must configure the Alarm Events in the Alarm Activation window - See [Alarm Events topic](#) for more information.

OPEN THE EVENTS PAGE

There are two ways to open the *Live Events Page* ...

- **Side Menu:** select "Live Events" option.
- **Dashboard:** select 'Events' Tile (under Configure section)



OPEN THE SETTINGS WINDOW

When the *Live Events Page* opens, the user can click the **Settings button** at the top-right corner of the Events page.



Note: No events will display if the user has never configured the event settings. After settings are configured, the appropriate incoming events will display as they happen in the system.

CONFIGURE EVENT SETTINGS

The Settings window allows user to choose which *hardware devices* to monitor and which *event types* to display.

STEPS

- To open Settings window, click the **Settings button** in the Event page (top-right corner).
 - The *hardware devices* are listed are in column-1 and the *event types* are in column-2.
 - When you choose a hardware device, you must also pick the corresponding event types to see.

The screenshot shows a 'Settings' window with two columns. Column 1 is titled 'Col.1 Select desired hardware.' and contains four dropdown menus: 'Select Reader' (22 selected), 'Select input' (2 selected), 'Select Controller' (2 selected), and 'Select Alarm panel' (All selected (2)). Column 2 is titled 'Col.2 Pick corresponding event types.' and contains four dropdown menus: 'Select Event Type' (All selected (3)), 'Select Input Event Type' (Alarm Event), 'Select Controller Type' (Alarm Event), and 'Select Alarm Event Type' (Alarm Event). At the bottom, there is a note '"Check" = display/include' and two buttons: 'Close' and 'Save'.

2. Select (check) any **Hardware Devices** from the 1st column that you want to monitor.
 - Each droplist all the hardware devices in your system (i.e., readers, inputs, controllers, alarm panels).
 - Use the "Select All" option to toggle the checkboxes (all on or all off).

DEVICE DROPLISTS

- **Readers** = list of all individual readers from every controller unit in the system.
- **Inputs** = list of all individual inputs from every controller unit in the system.
- **Controllers** = list of all the controllers in the system.
- **Alarm Panels** = list of alarm panels in the system.

3. Select (check) any **Event Types** from the 2nd column that you want to see events from.
 - Each droplist in the 2nd column pairs with the corresponding droplist in the 1st column. Each droplist contains a list of the events that pertain to the corresponding hardware in the 1st column.
 - Use the "Select All" option to toggle the checkboxes (all on or all off).

EVENT TYPE DROPLISTS

- **Reader Events** = check the desired types to see events from the selected readers/doors. [choices are - activity events, alarm events, and 'not in system' events]
- **Input Events** = check the *alarm event* to see events from inputs.
- **Controller Events** = check the *alarm event* to see controller events - such as controller online/offline, board online/offline, tamper, low battery, etc.
- **Alarm Panels** = check the *alarm event* to see events from alarm panels in the system.

4. Click **Save** button to save your choices and close.
(the Close button will close the window without saving your changes.)
5. **RESULT:** the system event messages that you selected should start logging from the hardware you chose.

EVENT MESSAGES

- **Invalid Access Attempt** = access denied - card presented does not have access to this door.
- **Valid Access** = access granted - card presented has valid access to this door.
- **Door Open too Long** = the door contact was not closed before the reclose within timer expired.
- **Door Forced** = door contact was opened without having a valid access granted.
See the main system programming guide for all types of events that are possible.
- **Not in System** = access card presented to the reader is not in the system.
See User Commands for more information on the Add button.

> Note: to see NIS events, the "Not in System" Event Type must be "checked" in the [Settings window](#).

Live Events							Alarm Activation Settings	Settings
Event Time	Event	Device/Point	User Message	Bitcount	Code	Action		
7/7/2021 2:16:18 PM	Not in System	Cluster: 055, Cont: 002, Brd: 1, Sect: 2-0	2 06 94 68 (26 bits)	26	33985640	<button>Add</button>		
7/7/2021 2:16:16 PM	Invalid Access Attempt	Cluster: 050, Cont: 001, Brd: 1, Sect: 1-0	Cluster50add Cluster50Add (Card 1)		50			
7/7/2021 2:16:07 PM	Door Open Too Long	Cluster: 050, Cont: 001, Brd: 1, Sect: 2-0			50			
7/7/2021 2:16:05 PM	Invalid Access Attempt	Cluster: 055, Cont: 002, Brd: 1, Sect: 2-0	48793 Jessica (Card 1)		55			
7/7/2021 2:16:00 PM	Valid Access	Cluster: 050, Cont: 001, Brd: 1, Sect: 1-0	iphone_edge_add iphone_edge_add (Card 1)		50			
7/7/2021 2:15:47 PM	Valid Access	Cluster: 050, Cont: 001, Brd: 1, Sect: 2-0	iphone_edge_add iphone_edge_add (Card 1)		50			
7/7/2021 2:15:40 PM	Invalid Access Attempt	Cluster: 055, Cont: 002, Brd: 1, Sect: 1-0	48793 Jessica (Card 1)		55			
7/7/2021 2:15:40 PM	Door Open Too Long	Cluster: 050, Cont: 001, Brd: 1, Sect: 2-0			50			
7/7/2021 2:15:20 PM	Valid Access	Cluster: 050, Cont: 001, Brd: 1, Sect: 2-0	Smith Test (Card 1)		50			
7/7/2021 2:15:10 PM	Door Open Too Long	Cluster: 050, Cont: 001, Brd: 1, Sect: 1-0			50			
7/7/2021 2:15:03 PM	Valid Access	Cluster: 055, Cont: 002, Brd: 1, Sect: 1-0	LeTestAdd LeTestAdd (Card 1)		55			
7/7/2021 2:15:03 PM	Valid Access	Cluster: 050, Cont: 001, Brd: 1, Sect: 2-0	Smith Joe (Card 1)		50			
7/7/2021 2:14:55 PM	Valid Access	Cluster: 050, Cont: 001, Brd: 1, Sect: 2-0	Smith Test (Card 1)		50			
7/7/2021 2:14:52 PM	Valid Access	Cluster: 050, Cont: 001, Brd: 1, Sect: 1-0	Smith John (Card 1)		50			

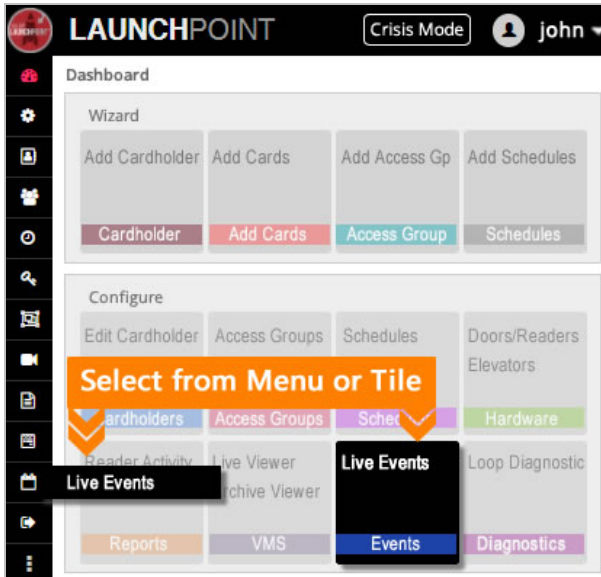
Monitoring Live Events

The **Live Events Page** allows the user to monitor live incoming events in a real-time capacity.

Events are continuously logged to the Events Page until user closes the page or the page connection times out.

STEPS

1. Open the Live Events page from the side menu or dashboard tile.



2. When the Events page opens, the live events will begin displaying based on the configured settings.

Live Events							Alarm Activation Settings	Settings
Event Time	Event	Device/Point	User Message	Bitcount	Code	Action		
7/7/2021 2:16:18 PM	Not in System	Cluster: 055, Cont: 002, Brd: 1, Sect: 2-0	2 06 94 68 (26 bits)	26	33985640	<button>Add</button>		
7/7/2021 2:16:16 PM	Invalid Access Attempt	Cluster: 050, Cont: 001, Brd: 1, Sect: 1-0	Cluster50add Cluster50Add (Card 1)		50			
7/7/2021 2:16:07 PM	Door Open Too Long	Cluster: 050, Cont: 001, Brd: 1, Sect: 2-0			50			
7/7/2021 2:16:05 PM	Invalid Access Attempt	Cluster: 055, Cont: 002, Brd: 1, Sect: 2-0	48793 Jessica (Card 1)		55			
7/7/2021 2:16:00 PM	Valid Access	Cluster: 050, Cont: 001, Brd: 1, Sect: 1-0	Iphone_edge_add Iphone_edge_add (Card 1)		50			
7/7/2021 2:15:47 PM	Valid Access	Cluster: 050, Cont: 001, Brd: 1, Sect: 2-0	Iphone_edge_add Iphone_edge_add (Card 1)		50			
7/7/2021 2:15:40 PM	Invalid Access Attempt	Cluster: 055, Cont: 002, Brd: 1, Sect: 1-0	48793 Jessica (Card 1)		55			
7/7/2021 2:15:40 PM	Door Open Too Long	Cluster: 050, Cont: 001, Brd: 1, Sect: 2-0			50			
7/7/2021 2:15:20 PM	Valid Access	Cluster: 050, Cont: 001, Brd: 1, Sect: 2-0	Smith Test (Card 1)		50			
7/7/2021 2:15:10 PM	Door Open Too Long	Cluster: 050, Cont: 001, Brd: 1, Sect: 1-0			50			
7/7/2021 2:15:03 PM	Valid Access	Cluster: 055, Cont: 002, Brd: 1, Sect: 1-0	LeTestAdd LeTestAdd (Card 1)		55			
7/7/2021 2:15:03 PM	Valid Access	Cluster: 050, Cont: 001, Brd: 1, Sect: 2-0	Smith Joe (Card 1)		50			
7/7/2021 2:14:55 PM	Valid Access	Cluster: 050, Cont: 001, Brd: 1, Sect: 2-0	Smith Test (Card 1)		50			
7/7/2021 2:14:52 PM	Valid Access	Cluster: 050, Cont: 001, Brd: 1, Sect: 1-0	Smith John (Card 1)		50			

NOTE: User commands are available from the User Command menu. See below.

SETTING THE 'NUMBER OF EVENTS' PER PAGE

1. In the Events page, choose the *number of events* you want to display per screen.
there are 3 choices ... 100, 250, 500.

2. In the Page Number field you can select which page you want to advance to.
3. Click the **Go** button to advance to the selected page.

OPERATOR COMMANDS

While the *Live Events Page* is open and active, the user can issue **User Commands** - described below.

There are two places to find user commands ...

- A. **Command Menu:** this is a *popup menu* that displays when the user clicks on the **Event column** of any incoming event message.

CAUTION: Be sure you are clicking the correct event, because the incoming event messages are continually popping in, which may move the position of your intended event.

NOTICE: the user commands are dynamically enabled/disabled based on the *event type* chosen.

- B. **Action Column:** this last column can display a *button* or a *link* that performs a command operation - such as View Video (link) or the Add Card (button). These options only display on the appropriate event types.

NOTICE: the Show Video option is available in the *Command Menu* if the Action column has a button or other option occupying that space. If the Action column is free, you may see a View Video link in the Action column - both Show Video command option and View Video action link will open the VMS login page.

The screenshot shows the 'Live' events page with a table of incoming messages. A blue callout box points to the 'Event Col.' header with the text 'Click on an event message.' A context menu is open over the 'Event' column, listing commands: 'Forgive Passback', 'Disable Cardholder', 'View Photograph', 'Properties', and 'Show Video'. A blue callout box points to the 'Add' button in the 'Action' column of the first row with the text 'Click Command button to add card from a Not in System message.' Another blue callout box points to the 'Choose Operator Command' button with a right arrow.

Event Time	Event	Device/Point	User Message	Bitcount	Code	Action
7/7/2021 2:16:18 PM	Not in System	Cluster: 055, Cont: 002, Brd: 1, Sect: 2-0	2 06 94 68 (26 bits)	26	33985640	Add
7/7/2021 2:16:16 PM	Invalid Access Attempt	Cluster: 055, Cont: 001, Brd: 1, Sect: 2-0	Cluster50add Cluster50Add (Card 1)		50	
7/7/2021 2:16:07 PM	Door Open Too Long	Cluster: 055, Cont: 001, Brd: 1, Sect: 2-0	48793 Jessica (Card 1)			
7/7/2021 2:16:05 PM	Invalid Access Attempt	Cluster: 055, Cont: 001, Brd: 1, Sect: 2-0	edge_add Iphone_edges_add (Card 1)			
7/7/2021 2:16:03 PM	Invalid Access Attempt	Cluster: 055, Cont: 001, Brd: 1, Sect: 2-0	edge_add Iphone_edges_add (Card 1)			
7/7/2021 2:15:40 PM	Invalid Access Attempt	Cluster: 055, Cont: 001, Brd: 1, Sect: 2-0	48793 Jessica (Card 1)		55	
7/7/2021 2:15:40 PM	Door Open Too Long	Cluster: 055, Cont: 001, Brd: 1, Sect: 2-0	LeTestAdd LeTestAdd (Card 1)		50	
7/7/2021 2:15:20 PM	Valid Access	Cluster: 050, Cont: 001, Brd: 1, Sect: 2-0	Smith Test (Card 1)		50	
7/7/2021 2:15:10 PM	Door Open Too Long	Cluster: 050, Cont: 001, Brd: 1, Sect: 2-0	Smith Test (Card 1)		50	
7/7/2021 2:15:03 PM	Valid Access	Cluster: 055, Cont: 002, Brd: 1, Sect: 1-0	LeTestAdd LeTestAdd (Card 1)		55	
7/7/2021 2:15:03 PM	Valid Access	Cluster: 050, Cont: 001, Brd: 1, Sect: 2-0	Smith Joe (Card 1)		50	
7/7/2021 2:14:55 PM	Valid Access	Cluster: 050, Cont: 001, Brd: 1, Sect: 2-0	Smith Test (Card 1)		50	
7/7/2021 2:14:52 PM	Valid Access	Cluster: 050, Cont: 001, Brd: 1, Sect: 1-0	Smith Joe (Card 1)		50	

STEPS

1. Open the Live Events Page from the dashboard tile or sidemenu.
2. Single-click on any *event message* in the Event column. While live events are logging,

Note: If incoming events are actively logging, the next incoming event could "bump" your intended event down as you are clicking. Be careful to ensure you have selected the intended event.

3. When the *command menu* opens, a list of **user commands** will display.
(the Commands are dynamically enabled or disabled based on which type of event is chosen.)
4. Select (choose) the appropriate command ...

LIST OF COMMANDS IN MENU

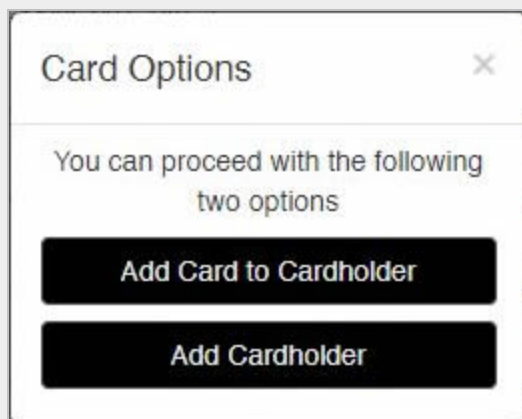
Open the Command Menu by clicking on the Event Column.

- **FORGIVE PASSBACK** = releases a card from a passback violation.
- **DISABLE CARDHOLDER**= disables the cardholder (system-wide) for the selected card.
- **VIEW PHOTOGRAPH** = displays the cardholder photograph in a popup box.
- **PROPERTIES** = opens the cardholder record of the person the card was issued to.
- **SHOW VIDEO** = opens the VMS Page and displays video from the associated camera for the door or device in selected event. (User will be prompted to sign-in to the VMS system.)

-
- **VIEW VIDEO (Action Column)**= this link opens the *VMS Page* and displays video from the associated camera for the door or device in chosen event. (User will be prompted to sign-in to the VMS system.)
 - **ADD (Action Column)**= this button allows user to add a card from a "not-in-systemevent".

More Info on Adding a "Not in System" Card: When a *Not in System event* logs to the Event page, it includes an **ADD button**. Clicking the Add button opens a message-box that lets the user add the card to the system.

- > clicking [Add Card to Cardholder] will add the card to an existing cardholder.
- > clicking [Add a Cardholder] will add the card to a new cardholder.



Alarms & Crisis Mode

Handling Alarms

This topic covers setting up and monitoring **real-time Alarm Events** and as well as **sending User Commands**.

FEATURED TOPICS

[Configure Alarms \(Activity Settings\)](#)

[Monitor Alarm Events](#)

[User Commands](#)

About Alarm Events

An **Alarm Event** is simply a *hardware event* that is elevated programmatically to be a system alarm. The alarm events are produced by hardware activity from inputs that are being monitored.

Alarm Events are not events from a third-party alarm panel. Events from third-party alarm panels are logged in the Live Events Page and are configured in the *Settings Window*.

The user must configure which hardware device(s) to see alarms from. This is done in the *Alarm Settings Window* (modal). See the next section.

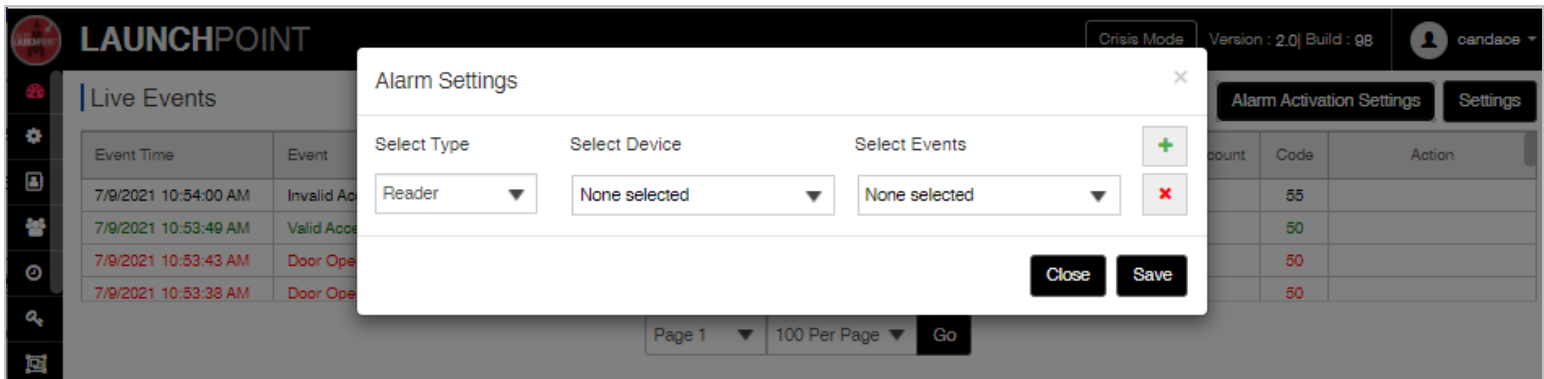
Once the Alarm Settings are configured, the user can handle the incoming alarm events as they occur. Alarm events display in a popup window (modal) in the foreground of the Events page. User cannot interact with the incoming events while the Alarm Events popup is open. User must resolve the alarms to return to the Events page.

Configure Alarms (Activation Settings)

Configuring alarm events is done in the *Alarm Settings Window* (modal).

The Alarm Settings window allows the user to build **alarm sets** to monitor selected hardware for specified events.

The user will choose a device type, then select the individual devices, and finally pick which events to see. The user can add as many alarm sets as needed.



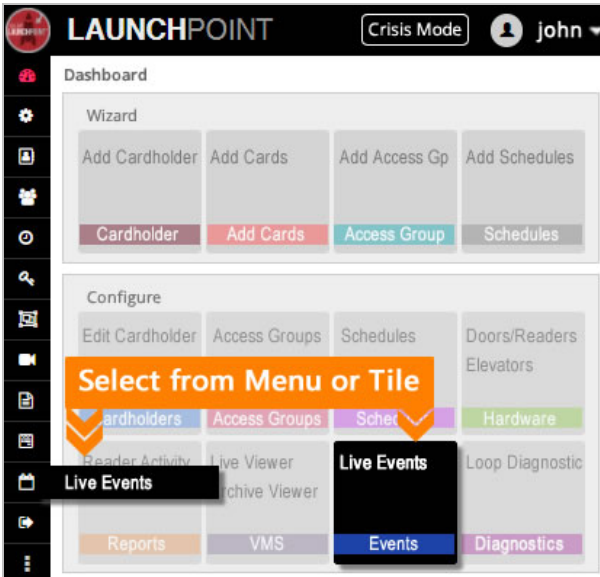
PREREQUISITES & NOTES

- Users must have the appropriate account permissions to view events and alarms (configured by system administrators).
- Users must have permissions and a VMS system login/account to be able to view video from linked cameras.
- You must enable the Hardware Types and Devices (readers, inputs, controllers, alarm panels) you want to monitor from the Alarm Activation Settings window.
- You must enable the actual event messages you want to see in the Alarm Activation Settings window.

OPEN THE EVENTS PAGE

There are two ways to open the *Live Events Page* ...

- **Side Menu:** select "Live Events" option.
- **Dashboard:** select 'Events' Tile (under Configure section)



OPEN THE ALARM SETTINGS WINDOW

When the *Live Events Page* opens, the user can click the **Alarm Activation Settings** button at the top-right corner of the Events page.



Note: No alarms will display if the user has never configured the alarm sets. After the alarm sets are created, the appropriate incoming alarms will display as they occur in the system.

ALARM SETTINGS

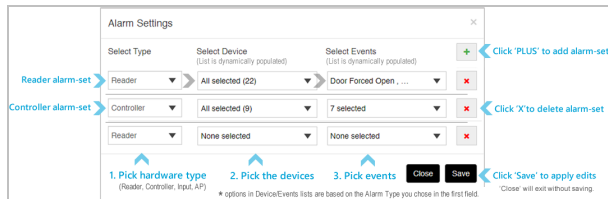
The Alarm Activation Settings window allows user to choose which **hardware** to monitor and which **alarm types** to display.

STEPS

1. Click the **Alarm Activation Settings** button in the Event page (top-right corner) to open the window.
(The Alarm Settings window (modal) will open.)
2. Click the **Plus** button in the *Alarm Settings window* to add an alarm-set.
(An alarm-set will be added to the screen.)
3. Select (check) a **Hardware Type** that you want to create an alarm-set for (1st droplist).
The choice you make in the Type field controls how the *Device* and *Events* lists are populated.

"TYPE" DROPLIST

- **Readers** = populates the *Device* and *Events droplists* to show choices for readers.
- **Inputs** = populates the *Device* and *Events droplists* to show choices for inputs.
- **Controllers** = populates the *Device* and *Events droplists* to show choices for controllers.
- **Alarm Panels** = populates the *Device* and *Events droplists* to show choices for alarm panels (3rd party).



4. Select (check) any **Hardware Devices** that you want to monitor (2nd droplist).
 - The **Device droplist** is populated based on the *Hardware Type* you chose in the 1st field (prior step).
For example: All the readers in your system are listed if you chose "Reader" in the *Type field*.
 - Use the "Select All" option to toggle the checkboxes (all on or all off).

"DEVICE" DROPLIST

- **Readers** = list of all the readers in the system.
- **Inputs** = list of all inputs in the system.
- **Controllers** = list of all the controllers in the system.
- **Alarm Panels** = list of all alarm panels in the system.

5. Select (check) any **Events** that you want to see (3rd droplist).
 - The **Events droplist** contains a list of events that correlate to the chosen Devices.
For example: Reader events are listed if you chose "Reader" in the *Type field*.
 - Use the "Select All" option to toggle the checkboxes (all on or all off).

"EVENTS" DROPLIST

- **Reader Events** = "check" the specific reader/door events - [e.g. *Door Forced, Invalid Access, etc.*]
- **Input Events** = "check" the specific input events - [e.g. *Armed Alarm, Armed Secure, etc.*]
- **Controller Events** = "check" the specific controller events - [e.g. *Board Offline, Tamper, Low Battery, etc.*]
- **Alarm Panels** = "check" the specific AP events - [e.g. *Point Bypassed, Trouble, A/C Fail, etc.*]

6. To add another alarm-set, repeat steps 2 thru 5 - as many times as needed.

7. Click the **Save button** to save your alarm-sets when ready.

The Close button in the Settings window will close the window without saving your changes.

8. Close the *Save Success* popup message to begin monitoring alarms.

9. RESULT: alarm event messages that you selected will start logging based on your alarm settings.

EVENT MESSAGES

- **Invalid Access Attempt** = access denied - card presented does not have access to this door.
- **Valid Access** = access granted - card presented has valid access to this door.
- **Door Open too Long** = the door contact was not closed before the reclose within timer expired.
- **Door Forced** = door contact was opened without having a valid access granted.
See the main system programming guide for all types of events that are possible.
- **Not in System** = access card presented to the reader is not in the system.
See User Commands for more information on the Add button.
> Note: to see NIS events, the "**Not in System**" **Event Type** must be "checked" in the [Settings window](#).

Live Events							Alarm Activation Settings	Settings
Event Time	Event	Device/Point	User Message	Bitcount	Code	Action		
7/7/2021 2:16:18 PM	Not in System	Cluster: 055, Cont: 002, Brd: 1, Sect: 2-0	2 06 94 68 (26 bits)	26	33985640	<button>Add</button>		
7/7/2021 2:16:16 PM	Invalid Access Attempt	Cluster: 050, Cont: 001, Brd: 1, Sect: 1-0	Cluster50add Cluster50Add (Card 1)		50			
7/7/2021 2:16:07 PM	Door Open Too Long	Cluster: 050, Cont: 001, Brd: 1, Sect: 2-0			50			
7/7/2021 2:16:05 PM	Invalid Access Attempt	Cluster: 055, Cont: 002, Brd: 1, Sect: 2-0	48793 Jessica (Card 1)		55			
7/7/2021 2:16:00 PM	Valid Access	Cluster: 050, Cont: 001, Brd: 1, Sect: 1-0	Iphone_edge_add Iphone_edge_add (Card 1)		50			
7/7/2021 2:15:47 PM	Valid Access	Cluster: 050, Cont: 001, Brd: 1, Sect: 2-0	Iphone_edge_add Iphone_edge_add (Card 1)		50			
7/7/2021 2:15:40 PM	Invalid Access Attempt	Cluster: 055, Cont: 002, Brd: 1, Sect: 1-0	48793 Jessica (Card 1)		55			
7/7/2021 2:15:40 PM	Door Open Too Long	Cluster: 050, Cont: 001, Brd: 1, Sect: 2-0			50			
7/7/2021 2:15:20 PM	Valid Access	Cluster: 050, Cont: 001, Brd: 1, Sect: 2-0	Smith Test (Card 1)		50			
7/7/2021 2:15:10 PM	Door Open Too Long	Cluster: 050, Cont: 001, Brd: 1, Sect: 1-0			50			
7/7/2021 2:15:03 PM	Valid Access	Cluster: 055, Cont: 002, Brd: 1, Sect: 1-0	LeTestAdd LeTestAdd (Card 1)		55			
7/7/2021 2:15:03 PM	Valid Access	Cluster: 050, Cont: 001, Brd: 1, Sect: 2-0	Smith Joe (Card 1)		50			
7/7/2021 2:14:55 PM	Valid Access	Cluster: 050, Cont: 001, Brd: 1, Sect: 2-0	Smith Test (Card 1)		50			
7/7/2021 2:14:53 PM	Valid Access	Cluster: 050, Cont: 001, Brd: 1, Sect: 1-0	Smith John (Card 1)		50			

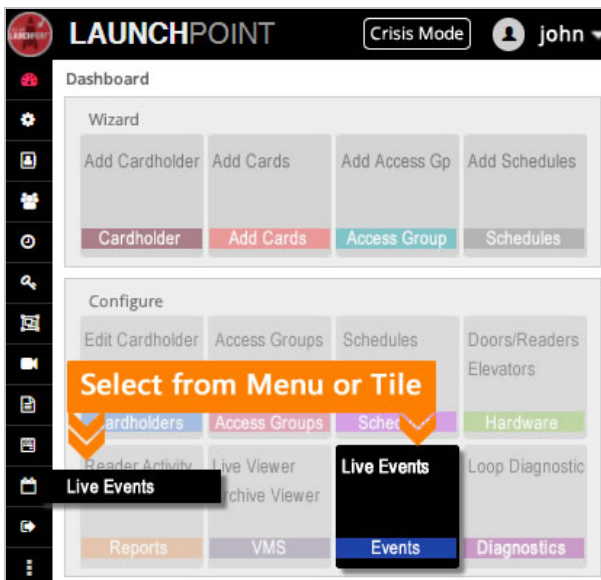
Monitoring Alarm Events

The **Alarm Events** window allows the user to handle incoming alarm events in a real-time capacity.

Alarm events are continuously logged to the Alarm window as they occur.

STEPS

1. Open the Live Events page from the side menu or dashboard tile.



2. The **Alarm Events popup window** will open as soon as alarm events occur in the system.

These pending alarms will continue to fill the alarm queue.

- The user can resolve alarms by *ignoring* or *acknowledging* them.
- Ignoring/Acknowledging an alarm removes it from the active list and silences its audible beeping alert.
- User may be prompted to enter a resolution text in the Acknowledge popup (configurable).

The screenshot shows the 'Alarm Events' window with the following elements and annotations:

- Alarm Events Window:**
 - Header: 'Alarm Events' with a 'Mute' checkbox.
 - Device: Cluster: 055, Cont: 002, Brd: 1, Sect: 2-0
 - Event Time: 6/22/2021 6:45:10 PM
 - Event: Not In System
 - Buttons: 'Show Video' and 'Ignore'.
- Annotations:**
 - 'Click to launch the VMS Viewer * (view live video from linked camera)' points to the 'Show Video' button.
 - 'Check to "mute" incoming alarms (alarms muted for user-selected duration)' points to the 'Mute' checkbox.
 - 'Click to ignore an individual alarm' points to the 'Ignore' button.
 - 'Type text as appropriate. (only for Acknowledged Alarms)' points to the text input field in the 'Acknowledge' popup.
 - 'Click to Acknowledge All pending alarms' points to the 'Acknowledge All' button.
 - 'Click to Ignore All pending alarms' points to the 'Ignore All' button.
- Acknowledge Popup:**
 - Header: 'Acknowledge'
 - Text input field containing 'CER'.
 - Buttons: 'Close' and 'Save'.
- Footer Note:** '* operator must provide valid login & password open the VMS Viewer. Login must have permissions to view the selected camera.'

NOTE: User commands are issued from the User Command buttons. See below.

ACKNOWLEDGE OPERATOR FEEDBACK

An programmable option can be configured to allow or require the user to enter a text message to provide system notes about the alarm.

1. When an *alarm event* comes in, click **Acknowledge All** button. The Acknowledge popup will open.
2. Type the appropriate *text message* into the textbox.

3. Click the **Close button** to clear the queued alarm event(s) and silence their correlating *audible beeping alarms*.
All the alarm events that were queued after the user clicked the Acknowledge button, will be not cleared or silenced.

NOTICE: Any audible alarms for events that were in the queue after the **Acknowledge button** was pressed, will continue sounding.

OPERATOR COMMANDS

While the Alarm Events window is open, the user can issue **User Commands** by clicking the command buttons.

STEPS

1. While alarm events are logging, **click on any command button in the Alarm window**.

Note: As you resolve one alarm, newer alarms could be logging. The user command applies only to the selected or active alarm.

2. Select (choose) the appropriate command button ...

COMMAND BUTTONS

- **IGNORE** = clears only the chosen alarm and silences the associated audible beeper.
- **IGNORE ALL** = clears all alarms currently queued and silences the associated audible beepers.
- **ACKNOWLEDGE ALL** = clears all alarms currently queued and silences the associated audible beepers.
- **SHOW VIDEO** = opens the VMS Page and displays the live video from the associated camera for the device causing the alarm event. (User will be prompted to sign-in to the VMS system.)

3. While alarm events are logging, **click on any command button in the Alarm window**.

NOTICE: As you resolve one alarm, newer alarms could be logging. The user command applies only to the selected or active alarm.

Activating Crisis Mode

This topic covers how to **activate** and **reset** Crisis Mode.

FEATURED TOPICS

[Crisis Mode Overview & Prerequisites](#)

[How to Activate Crisis Mode \(system-wide\)](#)

[How to Reset Crisis Mode \(system-wide\)](#)

[Command Crisis Mode in Diagnostics \(by loop/cluster \)](#)

Crisis Mode Overview & Prerequisites

The **Crisis Mode feature** allows an user to selectively place *some* or *all* of the system *Hardware* and *Groups* into a synchronized state, known as **crisis mode**. System programming applies - see [Prerequisites & Notes](#).

Before crisis mode can be activated, it must be configured in the system programming. This begins with the administrator creating the *crisis mode schedule(s)* and assigning them as to the appropriate hardware or groups (such as readers/doors, i/o groups, access groups, ...). Of course some of the hardware or groups in your system may not have a crisis mode schedule assigned - this is determined by the system administrator.

Recommended: After the system programming is saved, the crisis mode operation should be given a test run which includes walk-testing the system while crisis mode is activated and deactivated.

Once the schedules are assigned, the user can selectively choose which to include in the crisis mode activation .

PREREQUISITES & NOTES

- The *crisis mode schedule(s)* must have already been created and assigned to the appropriate hardware devices such as doors or inputs.
- Crisis mode schedules can be configured to secure or release doors (lock/unlock) - as needed.

- The user login account must have permission to use crisis mode.
- The user login may need the appropriate security level to open/edit the screen.

The following caveats apply ...

IMPORTANT: Users can selectively leave out Clusters/Loops from crisis mode activation by not checking them. Unchecked clusters will not invoke the crisis mode command, even if they have *crisis schedules* assigned. You can see the excluded (unchecked) panels (clusters) in *Crisis Mode Page*.

IMPORTANT: Offline panels cannot respond to crisis mode commands. Offline panels will continue to operate normally, even though crisis mode has been activated for their Cluster. You can find out if panels are offline via the *Loop Diagnostics Page*.

IMPORTANT: Unscheduled hardware or groups are not affected by crisis mode commands. If a crisis mode schedule is not assigned, the hardware or groups will continue operating as normal.

How is crisis mode activated or deactivated (reset)?

The user can **activate** and **deactivate** the *Crisis Mode* by one of two methods ...

1. open the *Crisis Mode Settings window* via the **Crisis Mode button** (in menu header of every page).
2. open the *Loop Diagnostics page* (using the **Crisis Mode options**).

How does crisis mode affect system operation?

Crisis mode only affects *Hardware* and *Groups* that have **crisis schedules** assigned if the Loop/Cluster they belong to a chosen for crisis mode activation.

When **crisis mode** is activated, the *hardware* and *groups* that belong to the selected (checked) Loop/Clusters immediately switch to crisis mode operation based on their **crisis schedules**.

EXCEPTIONS

- Groups/hardware continue normal operation if they do not have a crisis schedule assigned - even if the Loop/Cluster is selected (checked).
- Groups/hardware continue normal operation if the Loop/Cluster is unselected(unchecked) - even if they have crisis schedules.

IMPORTANT: Offline panels cannot respond to crisis mode commands. If a controller is offline it will continue operating as normal even if a crisis mode schedule is assigned. You can determine if panels are online in the Loop Diagnostics page.

Why is crisis mode not activating for part of my system?

The following are reasons why some hardware devices, doors or groups are not activating when crisis mode is issued.

- The panel is offline that contains the hardware in question - verify panel is online in the *Loop Diagnostics Page*.
- The Loop/Cluster containing the hardware or group was not selected (checked) when crisis mode was issued.
- The user account permissions are preventing the crisis mode from activating.
- No crisis mode schedule has been assigned to the hardware or group that is misbehaving.
- The wrong crisis mode schedule is assigned or the schedule is incorrectly programmed in some way.

IMPORTANT: Always use custom crisis mode schedules and do not mix normal operation schedules with crisis schedules, and visa-versa.

How are crisis mode schedules created and assigned?

Crisis mode schedules are made the same way any schedule is made - in the *Schedules screen*. What makes it a schedule a *crisis mode schedule*, is when the schedule is created specifically for use in a **Crisis Mode field** in the system programming.

Crisis mode schedules are assigned by selecting the crisis schedule in the **crisis mode field** of the hardware or group programming screens. This includes Access Group programming screen, Reader Properties Screens, and others.

IMPORTANT: Avoid using crisis schedules for normal operation - and visa versa. Keep normal schedules and crisis mode schedules separate to avoid conflicts in the system operation. It will be impossible to keep track of future changes and if schedules are crossed up, the changes are break your crisis mode operation.

Activating Crisis Mode Button (system-wide)

The user can activate crisis mode by clicking the **Crisis Mode button** in the menu header of any LaunchPoint page.

- The user can simultaneously activate all online controllers system-wide by selecting all loop/clusters.
- The user can selectively activate online controllers in selected loop/clusters simultaneously.

The Crisis Mode button is always visible in the LaunchPoint menu header from every screen or page.

If you have a modal screen or user feedback message open you may need to close it to return focus/-control to the page.



PREREQUISITES & NOTES

- The *crisis mode schedule(s)* must have already been created and assigned to the appropriate hardware devices such as doors or inputs.
- Crisis mode schedules can be configured to secure or release doors (lock/unlock) - as needed.
- The user login account must have permission to use crisis mode.
- The user login may need the appropriate security level to open/edit the screen.

OPEN CRISIS MODE SETTINGS

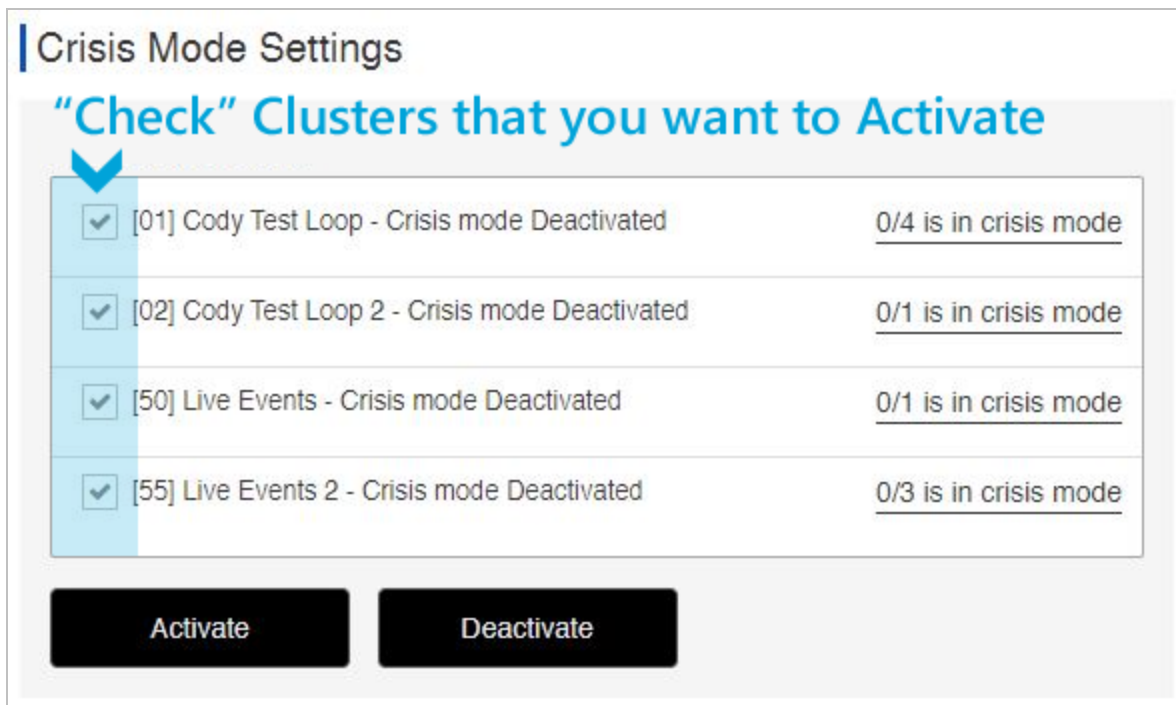


STEPS

1. Click the **Crisis Mode** button on the LaunchPoint page header .



- When the *Crisis Mode Settings* window opens, select (check) the Clusters(s) you want to activate ...

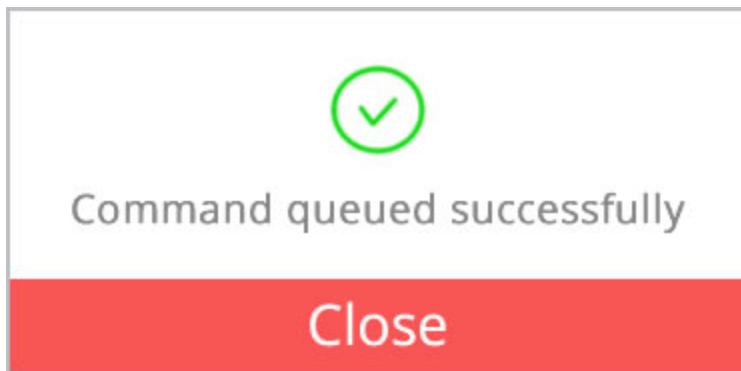


The image shows a 'Crisis Mode Settings' window. At the top, it says 'Crisis Mode Settings' and 'Check Clusters that you want to Activate'. Below this is a table with four rows, each representing a cluster. The first three rows are selected, indicated by a blue highlight and a blue arrow pointing to the first row. The table has three columns: a checkbox, the cluster name, and the crisis mode status. At the bottom of the window are two buttons: 'Activate' and 'Deactivate'.

<input checked="" type="checkbox"/>	[01] Cody Test Loop - Crisis mode Deactivated	<u>0/4 is in crisis mode</u>
<input checked="" type="checkbox"/>	[02] Cody Test Loop 2 - Crisis mode Deactivated	<u>0/1 is in crisis mode</u>
<input checked="" type="checkbox"/>	[50] Live Events - Crisis mode Deactivated	<u>0/1 is in crisis mode</u>
<input checked="" type="checkbox"/>	[55] Live Events 2 - Crisis mode Deactivated	<u>0/3 is in crisis mode</u>

Activate Deactivate

- Click the **Activate** button to activate *Crisis Mode* on the selected clusters/loops.
- Click **Close** to close the popup message.



RESULT OF ACTIVATING CRISIS MODE

The Crisis Mode Settings screen will display the *crisis status* for each Cluster.

- the screen indicates the *Loop/Cluster Name*, the *Crisis Mode Status* of and how many panels are in crisis mode.
- crisis mode will only activate for the selected (checked) loop/clusters.
- offline panels that belong to the activated cluster will not be in crisis mode.
- you can verify which specific panels are activated vs not activated in the [Loop Diagnostics](#) page.

Crisis Mode Settings

Select Loop or Cluster

<input checked="" type="checkbox"/> [01] Main Access Doors - Crisis mode Activated	2/4 is in crisis mode
<input type="checkbox"/> [02] Exterior Gates - Crisis mode Deactivated	0/1 is in crisis mode
<input checked="" type="checkbox"/> [03] Interior Doors - Crisis mode Activated	1/1 is in crisis mode
<input checked="" type="checkbox"/> [03] Inside Security - Crisis mode Activated	1/3 is in crisis mode

Activate Deactivate

This Cluster unchecked.

Deactivating Crisis Mode (system-wide)

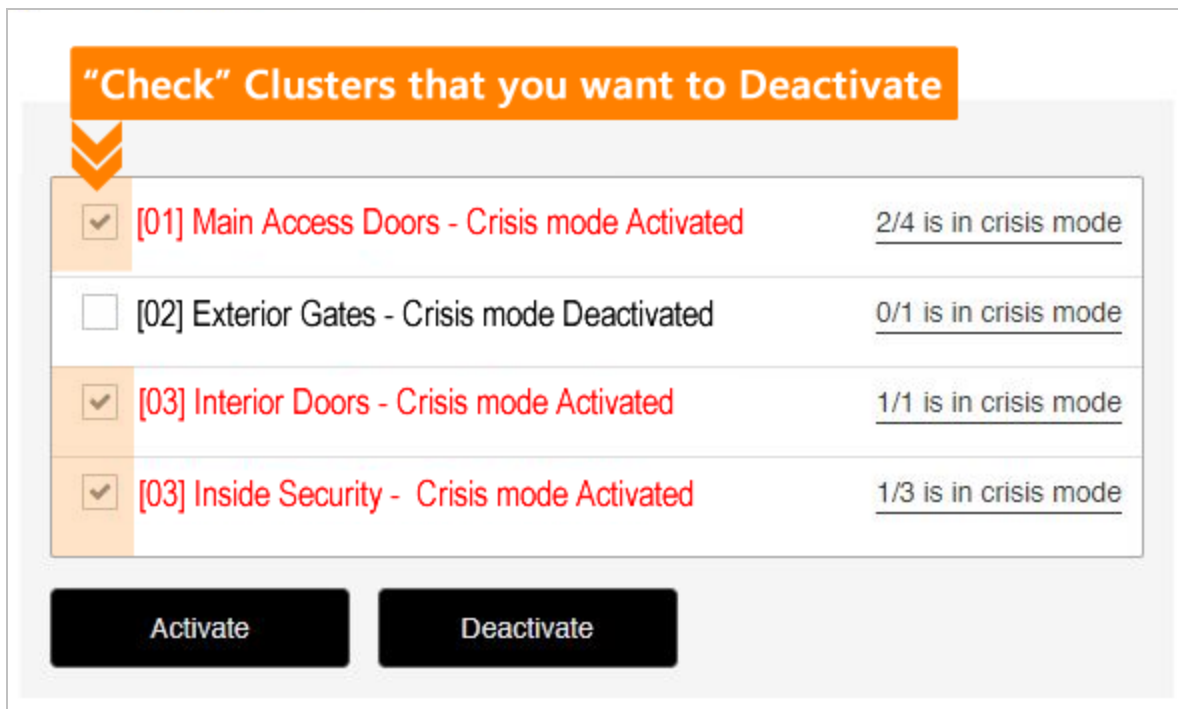
User can deactivate crisis mode from the same *Crisis Mode Settings* window where the mode was activated.

STEPS

1. Click the **Crisis Mode** button on the LaunchPoint page header - as needed.



2. With *Crisis Mode Settings* window open, select (check) the Clusters(s) you want to deactivate (reset).

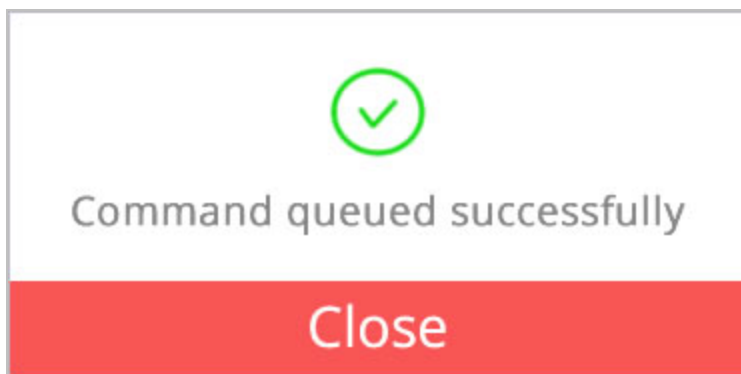


"Check" Clusters that you want to Deactivate

<input checked="" type="checkbox"/>	[01] Main Access Doors - Crisis mode Activated	<u>2/4 is in crisis mode</u>
<input type="checkbox"/>	[02] Exterior Gates - Crisis mode Deactivated	<u>0/1 is in crisis mode</u>
<input checked="" type="checkbox"/>	[03] Interior Doors - Crisis mode Activated	<u>1/1 is in crisis mode</u>
<input checked="" type="checkbox"/>	[03] Inside Security - Crisis mode Activated	<u>1/3 is in crisis mode</u>

Activate **Deactivate**

3. Click the **Deactivate** button to reset *Crisis Mode* for the selected clusters/loops.
4. Click **Close** to close the Success popup message.



VALID CRISIS MODE EXCEPTIONS

The following exceptions will prevent *crisis mode* from activating for hardware or groups within a loop/cluster ...

- a. *Offline controllers** will not activate crisis mode, even if they have a crisis mode schedule assigned.
- b. Clusters that were "unchecked/unselected" will not activate crisis mode, even if they have a crisis mode schedule assigned.
- c. Any doors/groups/devices that do not have a *crisis mode schedule* assigned to them, cannot activate crisis mode.

* While controllers are designed to remain fully operational in an "offline" situation, they cannot detect or respond to user commands while they are offline.

Activate or Reset Crisis Mode from Loop Diagnostics

The user can **activate** or **reset crisis mode** from the *Loop Diagnostics Page*.

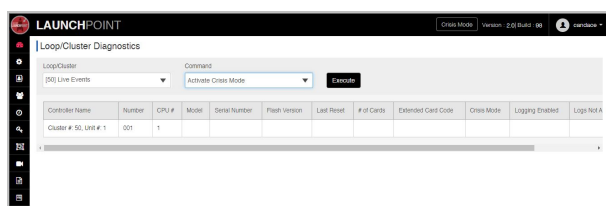
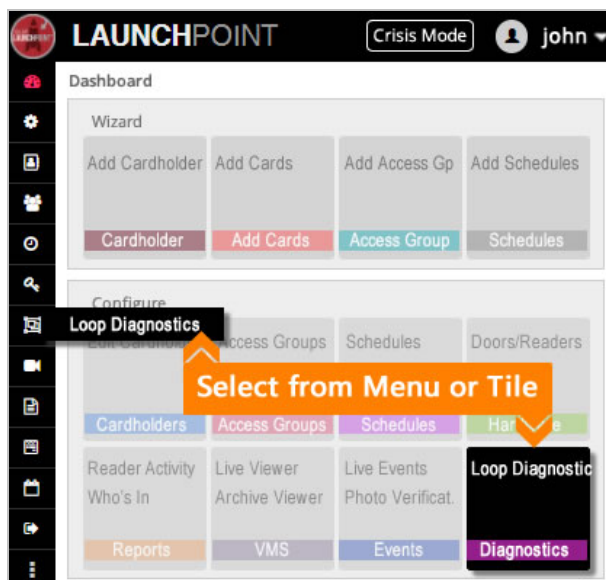
Scope of Crisis Mode functionality: The user can only 'activate' or 'reset' crisis mode at one loop/cluster at a time.

- This individual *Loop/Cluster functionality* gives the user the ability to walk-test the crisis mode programming on an individual basis, and lets the user walk-test the hardware a section at a time.
- Also, this gives the user more granular control over releasing crisis mode in a real crisis situation.

OPEN THE DIAGNOSTICS PAGE

There are two ways to open the *Loop Diagnostics Page* ...

- **Side Menu:** select "Loop Diagnostics" menu icon or option.
- **Dashboard:** select 'Diagnostics' Tile (under Configure section)



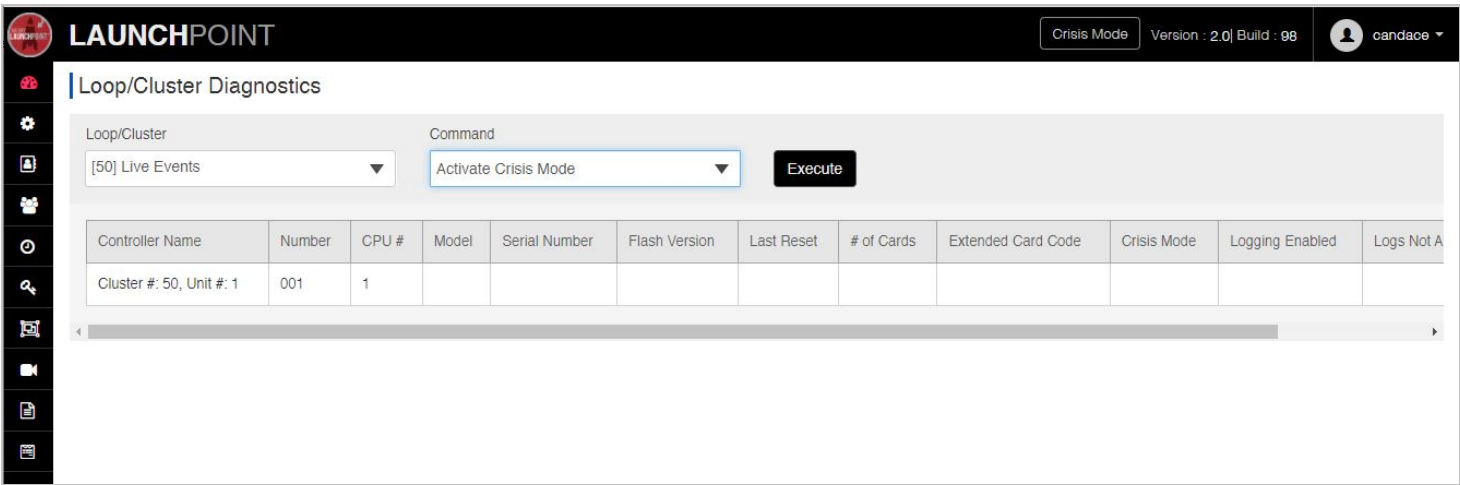
When the *Loop Diagnostics Page* opens, it will be empty until the user sends a command to a loop/cluster. (Offline controllers will not return data, but they will display in the list shaded red.)

- The *crisis mode schedule(s)* must have already been created and assigned to the appropriate hardware devices such as doors or inputs.
- Crisis mode schedules can be configured to secure or release doors (lock/unlock) - as needed.
- The user login account must have permission to use crisis mode.
- The user login may need the appropriate security level to open/edit the screen.

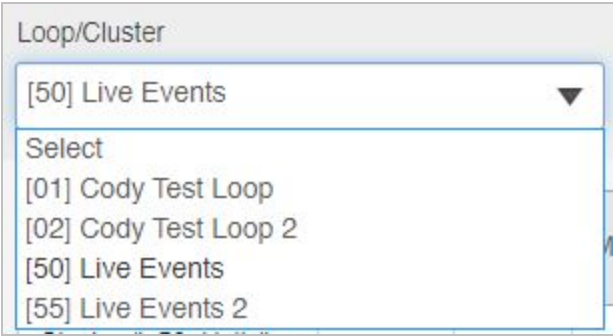
NOTICE: You can only activate or deactivate Crisis Mode on a single Loop/Cluster at a time. If you need to activate or reset crisis mode for multiple or all Loops/Clusters at the same time, use the *Crisis Mode Screen* (i.e., the *Crisis Mode Button* on the menu header).

STEPS

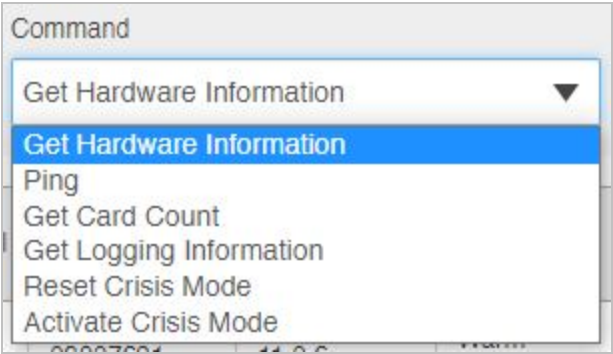
- 1. Click the **Loop Diagnostics** tile on the Dashboard page .
(or select Loop Diagnostics from the side menu)
- 2. When the *Loop Diagnostics* window opens, no data will be showing.



- 3. Select the **LOOP/CLUSTER** you want to operate on.



- 4. Select the **COMMAND** you want to send.



5. Click the **EXECUTE** button to send the command to the chosen loop/cluster.



6. Click **Close** to dismiss the Success popup message.

Notice that offline panels (shaded in red) will not respond to user commands.

The screenshot shows the LaunchPoint web interface. At the top, there's a navigation bar with the "LAUNCHPOINT" logo, a "Crisis Mode" button, and version/build information. Below this is the "Loop/Cluster Diagnostics" section. It features two dropdown menus: "Loop/Cluster" (set to "[01] Cody Test Loop") and "Command" (set to "Get Card Count"). An "Execute" button is to the right. Below these is a table with columns: Controller Name, Number, CPU #, Model, Serial Number, Flash Version, Last Reset, # of Cards, Extended Card Code, Crisis Mode, Logging Enabled, Logs Not Acked, and Log Not sent. The first two rows of the table are shaded red, indicating they are offline. A modal popup is centered over the table, displaying a green checkmark icon, the text "Command sent successfully", and a red "Close" button at the bottom.

5. **RESULT:** Crisis Mode will be activated (or reset) for the individual Loop/Cluster you selected.

Notice the *Controller Name* will appear in red text while crisis mode is ON/active

This screenshot shows the same "Loop/Cluster Diagnostics" interface. The "Loop/Cluster" dropdown is now set to "[50] Live Events" and the "Command" dropdown is set to "Activate Crisis Mode". The "Execute" button is visible. The table below shows a single row for "Cluster #: 50, Unit #: 1". The "Controller Name" is highlighted in red text. The "Crisis Mode" column for this row is "Active".

Controller Name	Number	CPU #	Model	Serial Number	Flash Version	Last Reset	# of Cards	Extended Card Code	Crisis Mode	Logging Enabled	Logs Not Acked	Log Not sent
Cluster #: 50, Unit #: 1	001	1	635	03007691	11.0.6	Warm Reset		NO	Active	Yes	29	0

VALID CRISIS MODE EXCEPTIONS

The following exceptions will prevent *crisis mode* from activating for hardware or groups within a loop/cluster ...

- a. *Offline controllers** will not activate crisis mode, even if they have a crisis mode schedule assigned.
- b. Clusters that were "unchecked/unselected" will not activate crisis mode, even if they have a crisis mode schedule assigned.
- c. Any doors/groups/devices that do not have a *crisis mode schedule* assigned to them, cannot activate crisis mode.

* While controllers are designed to remain fully operational in an "offline" situation, they cannot detect or respond to user commands while they are offline.

Video & Photo Viewers

Photo Verification

This topic covers viewing the cardholder Photo ID from the **Photo Verification Viewer**.

FEATURE TOPICS

[Overview & Prerequisites](#)

[Open the Photo Verification screen](#)

[How to View Photo IDs](#)

Photo Verification - Overview and Prerequisites

The **Photo Verification Viewer** allows the user or attendant to perform Photo Verification and Person Identification at a selected entry point.

Presumably the entry point that the user is attending, has the ability to control the queue of cardholders at the entry point, to allow the user to flag any person in synch with their photo entry.

RULES OF OPERATION

The LaunchPoint *Photo Verification Screen* displays the current Photo ID for the access card presented at the selected reader. The user can quickly verify that photo in the system matches the person who is at the door.

Photo Verification Screen

Current Main Photo Data: A cardholder's *Photo ID Data* displays in the *Photo Verification Screen* when the access card is presented at the selected reader. The Photo ID Data is updated real-time when each card is swiped.

- A *green or red border* indicates whether access was granted (green) or denied (red).
- The *status caption* under the photo also states "Valid Access" (granted) or "Invalid Access" (denied)
- The *identification data* is personnel data that was saved in the Cardholder screen when the person was enrolled.
- "No Photo Available" displays if a photo is not saved in the cardholder record.

NOTICE: The presence or absence of a photograph does not affect the access card is valid or invalid.

The card is granted or denied access based on the access permissions assigned during enrollment. The access groups determine, which doors are authorized and what days and times the card is valid or invalid.

Photo Carousel: the *Photo Carousel* displays at the bottom of the *Photo Verification Screen* and holds the Photo and access timestamp when the

- The user can use the Photo Carousel independently of the Current Photo ID Data.
- Each incoming Photo (and access time stamp) is added to the carousel in sequential order
- The Current Photo Data will be refreshed with data from the next card swipe at the reader.
- That photo will be added to the Photo Carousel.
- Once the page is closed, the queue is emptied. The system does not retain photos from previous sessions.

PREREQUISITES & NOTES

- The *main photograph* must be saved in the Cardholder screen for the photo to appear in Photo Verification screen.
- Any *personal data** that relates to *photo verification* must be saved in the Cardholder Editor screen .
- The user* must select **at least one reader** to see photos appear in the Photo Verification screen.
- The main Photo ID Data area can only display one photo at a time, which is the last card swiped.

- The Photo Carousel will display a queue of the prior photos (cards) presented at the reader.
- The user can independently scroll through the carousel to see previous photos.
- The user cannot control access from the LaunchPoint Photo Verification screen. Access is determined by the access permissions assigned to the card.

* The LaunchPoint User account must have the correct privileges or filters to be able to see cardholder photos, cardholder information and to see/select the readers as needed.

Always Active / Live Photo Updates

The *Photo Verification Tab* remains active as long as the session is open. Photographs continue updating "real-time" in the background, even if the browser tab is not the top window or is not 'in focus'.

NOTE: The user privileges (filters and permissions) can determine which readers are available in the Select Reader droplist. A master user should be able to see all the readers in the list. Contact the system administrator to update the user profile if needed.

When the *Photo Verification Window* first launches, the user must select at least one reader.

The list of readers has checkboxes beside each reader name, which allows the user can select multiple readers. Photos will display in the order they are presented. Photos will not display from readers that are not selected.

The user will only see the last cardholder to present their card to a selected reader.

How to open the Photo Verification screen ...

1. On the *Dashboard*, you can hover over the **Event tile** and select the **Photo Verification** option.
2. On the *Sidebar Menu*, you can click the **Event icon** and select the **Photo Verification** option.
3. When the window opens, the user will see incoming photos.

Result: The *Photo Verification Viewer* allows an **authorized*** user to view the *main photograph* and personnel data for the access card being presented to the reader. If a photograph is not saved, the user will see "No Photograph Available".

* The **LaunchPoint User profile** must have the correct *user privileges* that grant permission to see cardholder data. Contact the system administrator for questions about the user permissions, as needed.



◀ Event Icon (sidebar menu)

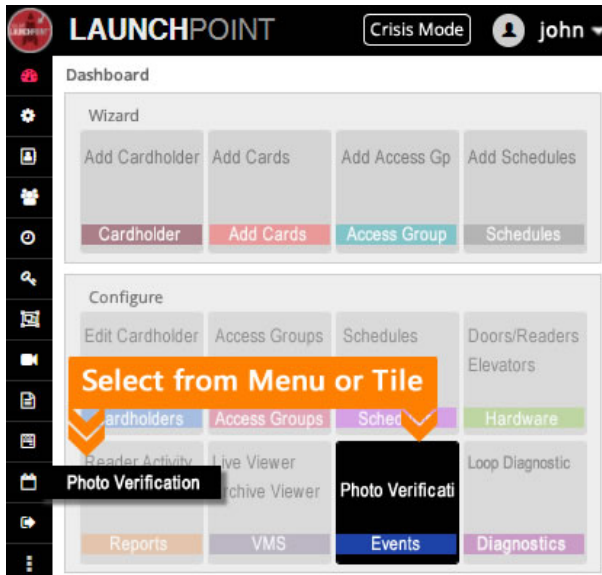


Photo Verification screen
(hover/tap to open thumbnail)

How to View Photo Verification

The *Photo Verification Window* will open in a new browser tab in the same browser window.

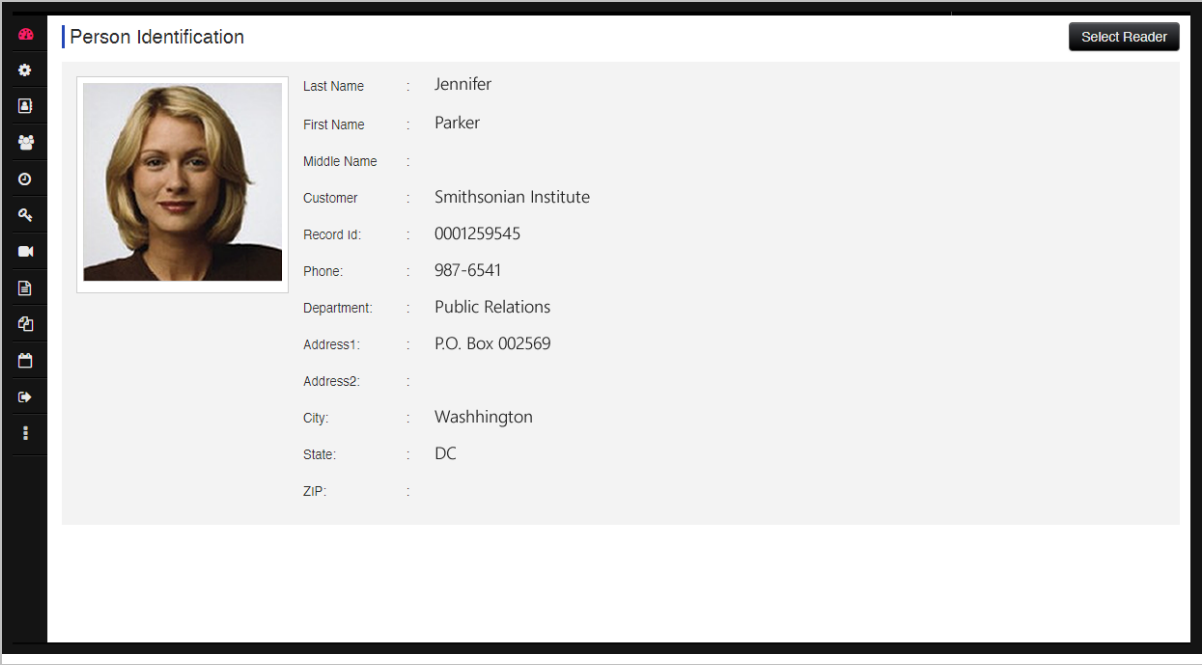
This tab/session will remain active in the background if the user shifts focus to another page or another task.

1. From the sidebar menu or dashboard, select **Events > Photo Verification** option.
2. When the *Photo Verification* window opens, choose the desired Reader as follows ...
 - a. click the **Select Reader** button (top right corner of the screen).
 - b. choose the reader that you want to see photos from.

Select Reader

- 3. When a cardholder presents an *access card* to the chosen reader, the Person Identification information is displayed ...
 - a. the *main photograph* (from the Cardholder screen) will display in the Photo Viewer screen.
 - b. also *personnel data* (from the Cardholder screen) will display in the Photo Viewer screen.


FIGURE-1 Picture of the Person Identification in the Cardholder screen



- 4. When *each cardholder* presents an access card to the chosen reader, their photo and person identification data are displayed in the *Photo Viewer* and also added to the "*Photo Carousel*".

Person Identification

Select Reader



6/24/2021 8:28:51 AM
Valid Access

Last Name : **Smith**

First Name : **Joe**

Middle Name :

Customer : Customer 1

Record Id : 4433

Phone :

Department : Customer 1 Dept 1

Address1 :


Address2 :

City :


State :

ZIP :


Accessed From : Cluster: 050, Cont: 001, Brd: 1, Sect: 1-0




6/24/2021 8:28:51 AM




6/24/2021 8:28:51 AM



6/24/2021 8:28:45 AM



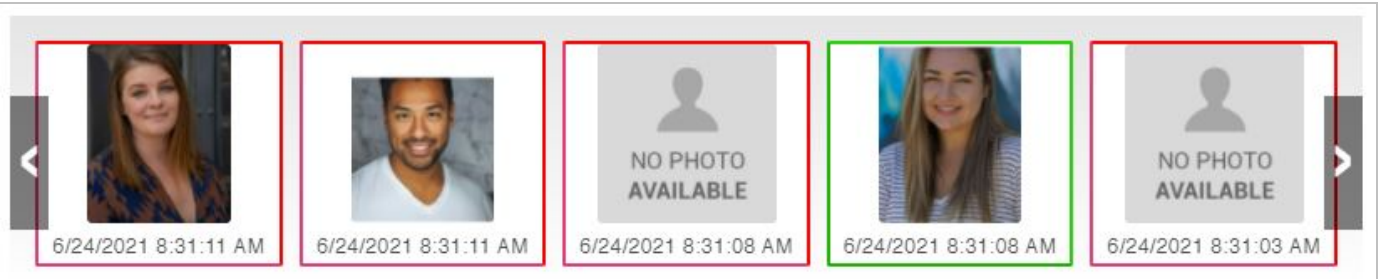
6/24/2021 8:28:45 AM



6/24/2021 8:28:44 AM

5. User can scroll back and forth in the *photo carousel* to see the first thru the last photos.
- A green border = access granted ("Valid Access" is displayed).
 - A red border = access denied (i.e., "Invalid Access" or "Not in System").
 - "NO PHOTO AVAILABLE" = means no photo is in the system for the card presented to the reader.
 (green border/no photo) - a *valid card* that doesn't have a photo on file.
 (red border/no photo) - an *invalid card* that doesn't have access to the door or doesn't have access at the time

presented.
OR it could be an invalid attempt for a card that is not in the system, in which case access will be denied (red border).



6. When you close the window, the **Photo Viewer** session is ended.

NOTE: If the **Photo Viewer** does not display data you expect, verify that (A) a *main photograph* is saved in the *Cardholder Screen*, and that (B) the *personnel data* is saved. Also verify (C) the user chose the correct reader in the Photo View page.

* "Authorized User = the **LaunchPoint User profile** must have the correct *user privileges* assigned that grant permission to see cardholder data. Contact your system administrator for questions about the user permissions, as needed.

Viewing VMS Video

This topic covers viewing video from the Video Management System.

FEATURED TOPICS

- [Overview and Prerequisites](#)
- [View Video \(Live or Recorded\)](#)

See Related Topics

- [Video of Live Events](#)
- [Video of Alarms](#)
- [Video - Elevator page](#)
- [Video - Reader Activity](#)

Overview & Prerequisites

The **VMS Viewer** allows an **authorized user** to View Live video or View Recorded video.

PREREQUISITES & NOTES

- Discovery OWS is the default video management system used by LaunchPoint
 - Your brand of VMS Video plug-in must be installed and configured in the system by the System Administrator.
 - The cameras must be mapped to the appropriate readers/doors, or input device.
 - The LaunchPoint user must have a valid login to the VMS webpage and permissions to view video/cameras (configured by administrator).
 - If user doesn't have proper permissions, LaunchPoint will display an error message when the user tries to view a camera.
 - Contact your integrator for questions about your VMS.
-

How to View Video

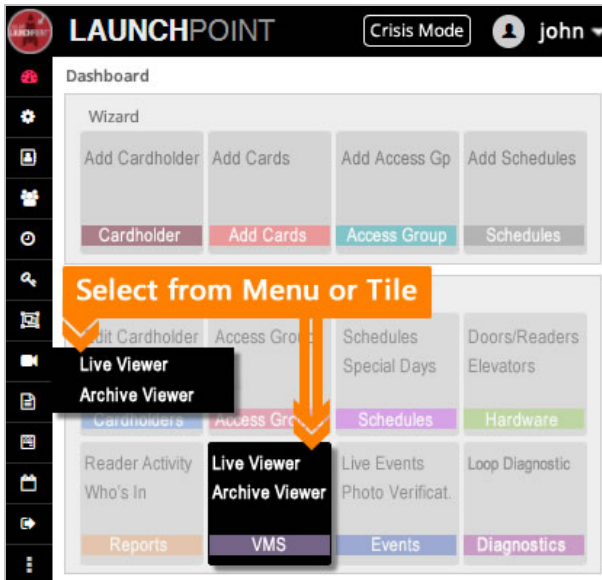
The **VMS Viewer** allows an **authorized user*** to play Live video or Recorded video.

HOW TO OPEN THE VMS SCREEN

There are multiple ways to open the Video Viewer (or VMS Online Video Screen).

- LaunchPoint Dashboard: Hover your mouse-pointer over the VMS Tile and select Live or Archive.
- LaunchPoint Side Menu: Click the VMS Icon and select Live or Archive.
- Alarm Event popup: Click the View Video button.

Click/tap on thumbnails to open and close them.

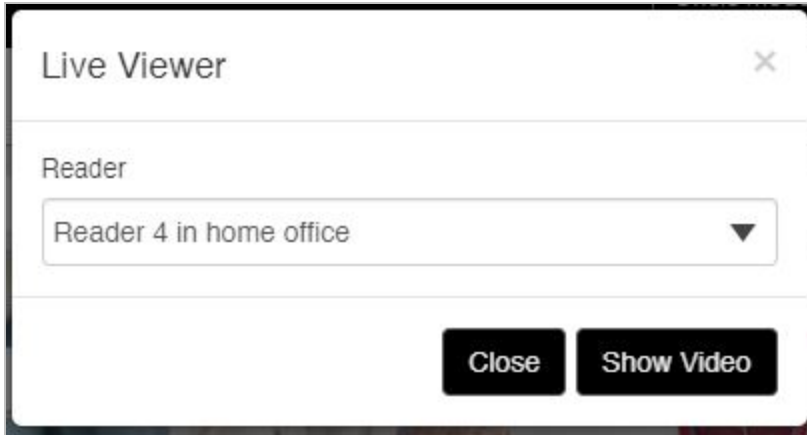


◀VMS icon (from sidebar menu)

NOTE: if the user clicked a View Video button from an event message or alarm event message, the live video will display from the camera that is linked to the selected event.

STEPS

1. From the menu or dashboard, select the **View VMS** option.
 - a. select the **Live viewer** to see live feed.
 - b. select the **Archive viewer** to see recorded / historic video.
2. In the **Video Viewer popup** modal, choose the desired reader.
(or in the Archive popup, choose the reader and the date/time)

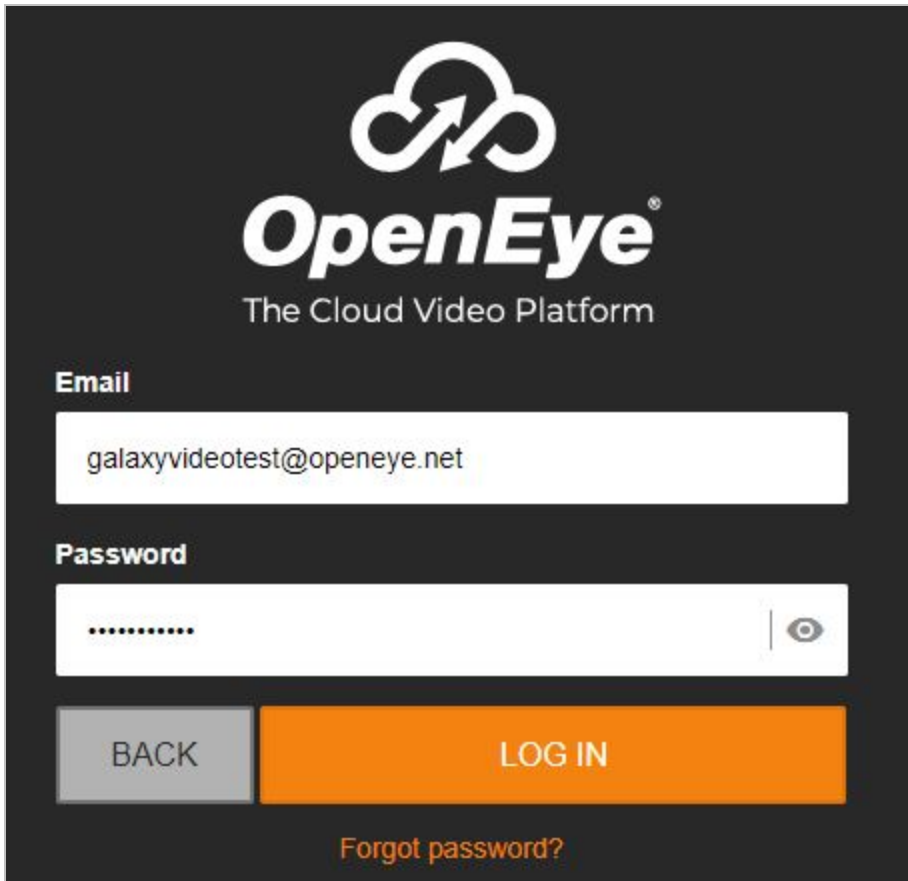
A screenshot of a 'Live Viewer' popup window. The window has a title bar with 'Live Viewer' and a close button (X). Below the title bar, there is a section labeled 'Reader' with a dropdown menu showing 'Reader 4 in home office'. At the bottom of the window, there are two buttons: 'Close' and 'Show Video'.

(Live popup - reader list)

A screenshot of an 'Archive Viewer' popup window. The window has a title bar with 'Archive Viewer' and a close button (X). Below the title bar, there is a section labeled 'Reader' with a dropdown menu showing 'Cluster: 055, Cont: 002, Brd: 1, Sect: 2-0'. Below that, there is a section labeled 'Date' with a text input field and a calendar icon. At the bottom of the window, there are two buttons: 'Close' and 'Show Video'.

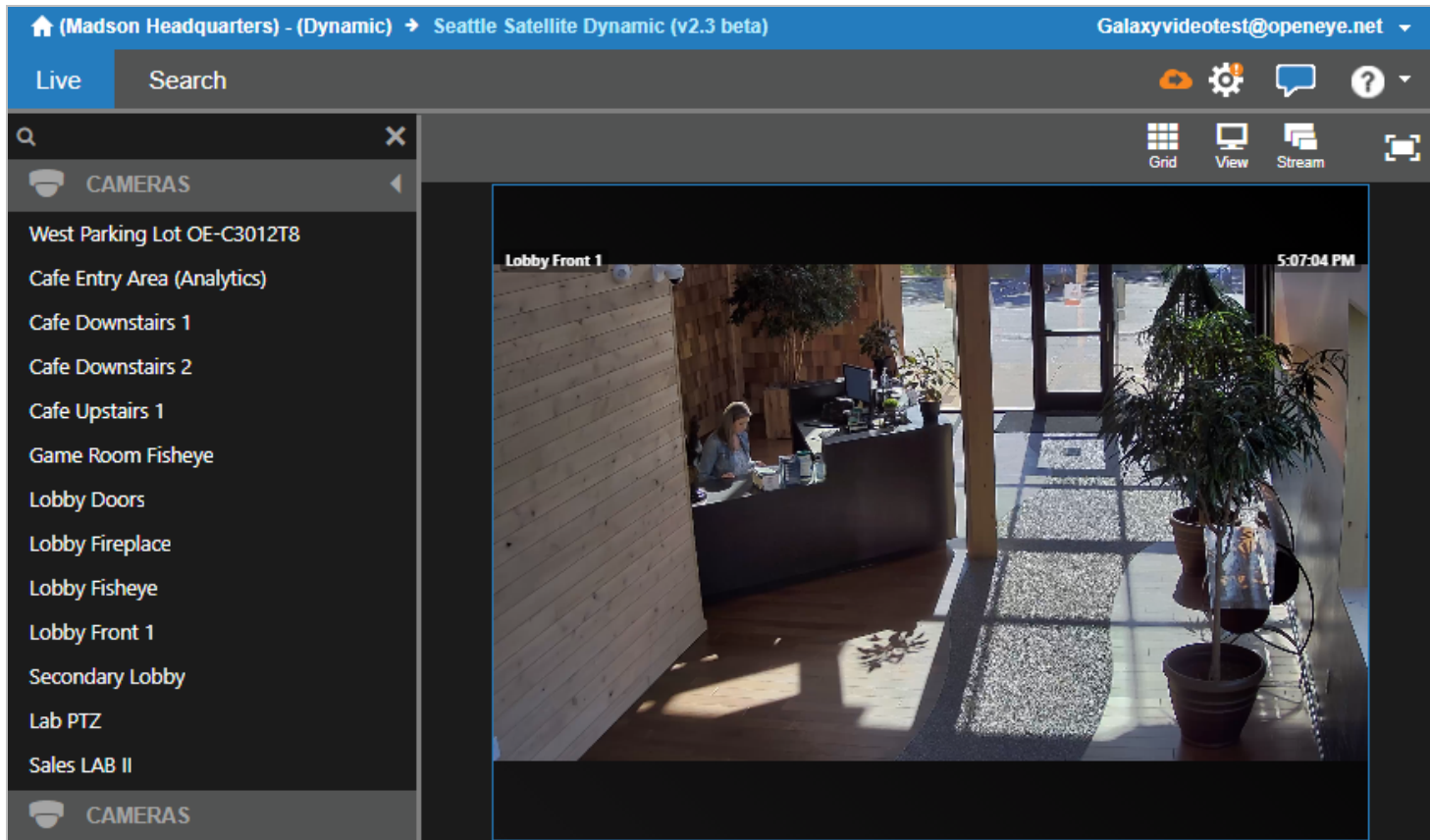
(Archive popup - reader list and date/time field)

3. Click **Show Video** button to launch the VMS Viewer.
4. User must provide the **valid login credentials: name/email and password**.

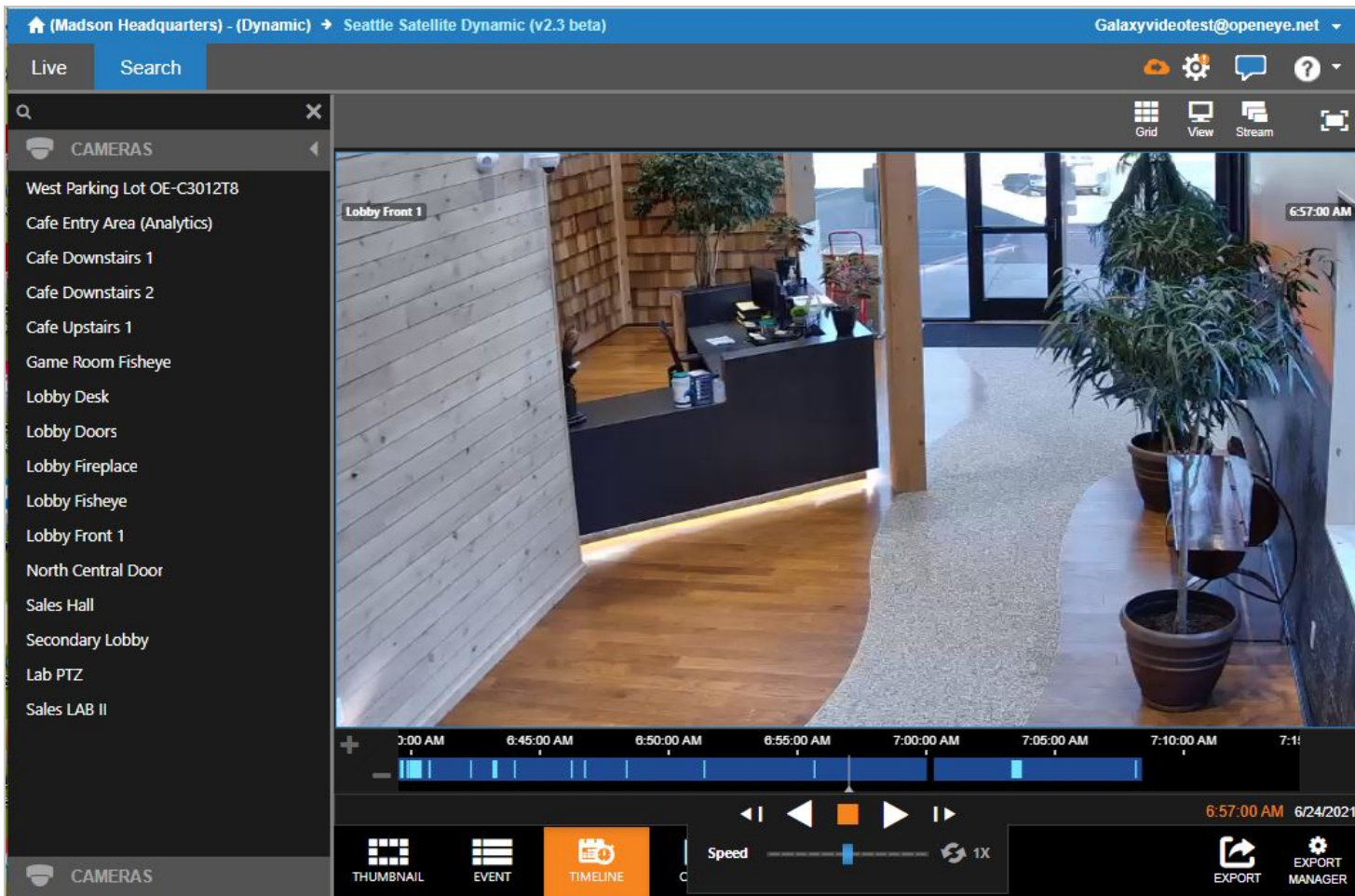
The image shows a login page for OpenEye, 'The Cloud Video Platform'. The page has a dark background. At the top is the OpenEye logo, which consists of a stylized cloud with an arrow forming a circular path. Below the logo is the text 'OpenEye' in a large, bold, white font, and 'The Cloud Video Platform' in a smaller, white font. Below this is a login form. It has two input fields: 'Email' and 'Password'. The 'Email' field contains the text 'galaxyvideotest@openeye.net'. The 'Password' field contains a series of dots, and there is an eye icon to its right. Below the input fields are two buttons: a grey 'BACK' button and an orange 'LOG IN' button. Below the buttons is a link that says 'Forgot password?' in orange text.

Login Page appearance will vary based on brand or setup.

5. Click **LOG IN button** (or click NEXT button) - as needed.
6. When the *VMS Page* opens, the video will display for the selected reader.
7. The VMS Camera will display *live video* (or recorded), based on your selection.



(Fig. 1 "Live" video feed)



(Fig. 2 "Search" recorded video playback)

NOTE: Controls and options may vary based on brand of VMS, configuration, setup, user permissions.

8. Use the control buttons to ...

- select the desired camera independently
- **play, pause, forward, reverse, stop** and **speed** control recorded video playback.
- **pan/tilt/zoom, iris** control camera during live video, depending on the camera type installed.

NOTE: the VMS *brand*, *camera type*, or *setup of system options* may, or may not, support these listed or unlisted features. User's VMS login account permissions may apply and requirements may vary between VMS brands. Contact your system administrator for assistance with operating camera controls and playback controls, as well as viewing cameras and video.

9. When you close the Video Viewer, the page session is ended. User must provide login credentials at each View request.

* The user must have login rights that grant permission to view video on the VMS server.

See Related Topics

[Video of Live Events](#)[Video of Alarms](#)[Video - Elevator page](#)[Video - Reader Activity](#)

Reports

Reader Activity History

This topic covers viewing, printing, or exporting the Reader Activity History Report.

ALSO SEE: You can also pull the activity history for an individual reader from the [Hardware Reader page](#).

FEATURED TOPICS

[Overview and Prerequisites](#)[Pull the Reader Activity History](#)[View Video from the Activity History](#)

Overview and Prerequisites

The *Reader Activity History Report* is configurable. User can choose a custom Date Range, as well as selectively choose which readers to include and which events to see. The *unchecked* readers or events will not appear on the report. Likewise events that are outside the date-range will also be omitted.

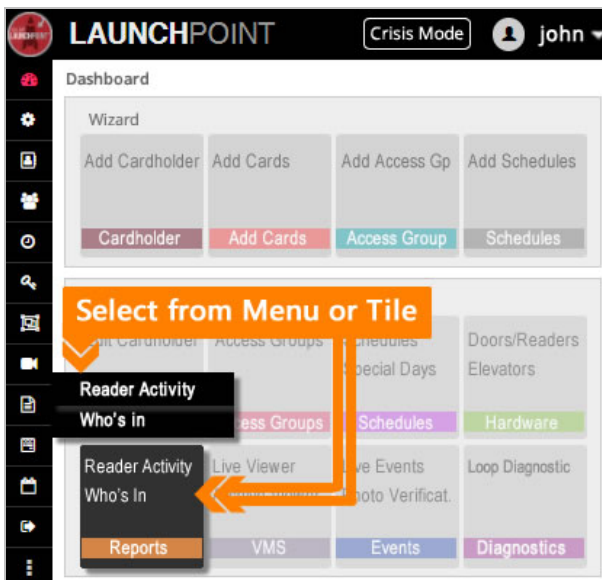
PREREQUISITES AND NOTES

- The user login account must have the correct permissions needed to view and print the report.
- User must have account permissions to the VMS system if Viewing Video is needed.
- The selected reader(s) must have activity and must have the type of events selected.

Under the Configure section of the Dashboard, you will click the Reports tile.



← Reports Icon (from sidebar menu)

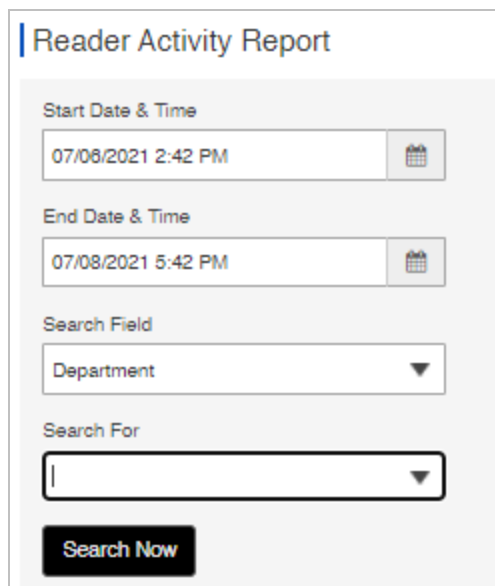


Pull the Reader Activity History

The fields in the page are dynamic depending on what is selected in the Search field.

1. In the **Start Date field**, click the **Calendar Function** button to choose a date and time.
2. In the **End Date field**, click the **Calendar Function** button to choose a date and time.

3. In the **Search Field** droplist, click the desired criteria (i.e. Department, Customer, First or Last Name, ...)
4. You can narrow your search criteria by adding a selection in the **Search For** droplist, depending on what you selected in the Search Field.
5. Click the **Search Now** button to open up more data fields.



Reader Activity Report

Start Date & Time
07/08/2021 2:42 PM

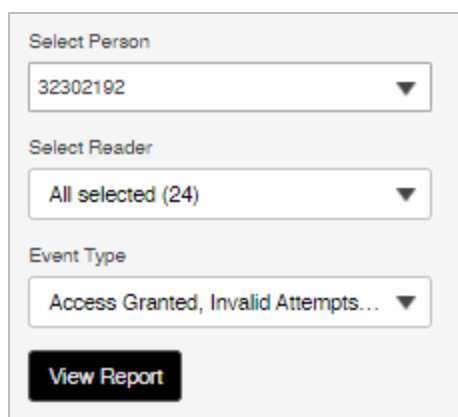
End Date & Time
07/08/2021 5:42 PM

Search Field
Department

Search For
|

Search Now

6. In the **Select Person** droplist, click the desired person (or "everybody") that you want to see events for ().
7. In the **Select Readers** droplist, click the desired reader you want to see events for (all readers or an individual reader).
8. In the **Event Types** droplist, select any events you want to see by checking the checkboxes. You can check any or all boxes as needed (i.e. select_all, or select individual event types).
9. Click **View Report** button to pull the Event Report.



Select Person
32302192

Select Reader
All selected (24)

Event Type
Access Granted, Invalid Attempts...

View Report

10. The Event Report screen will display in a grid list at the bottom of the same screen.
11. You can export the report to **Excel** or **PDF** as needed.

[Excel](#) [Pdf](#)

Event Date-Time	Reader/DoorName	Event Message	Person	Card Data	Show Video
07/08/2021 5:41 PM	Cluster: 055, Cont: 002, Brd: 1, Sect: 1-0	Valid Access	LeTestAdd, LeTestAdd (Card 1)	Facility Code: 146, ID Code: 23728	View Video
07/08/2021 5:41 PM	Cluster: 055, Cont: 002, Brd: 1, Sect: 1-0	Valid Access	LeTestAdd, LeTestAdd (Card 1)	Facility Code: 146, ID Code: 23728	View Video

Showing 1 to 2 of 2 entries

22 ▾ Items Per Page

Previous **1** Next

Viewing Video from the Reader Activity History

In the Reader Activity History, the user can click the **View Video link** to see video from the camera that is linked to the reader.

1. Follow the steps (above) to pull the Activity History.
2. Click on the [View Video](#) link in the Show Video column for the desired event.

[Excel](#) [Pdf](#)

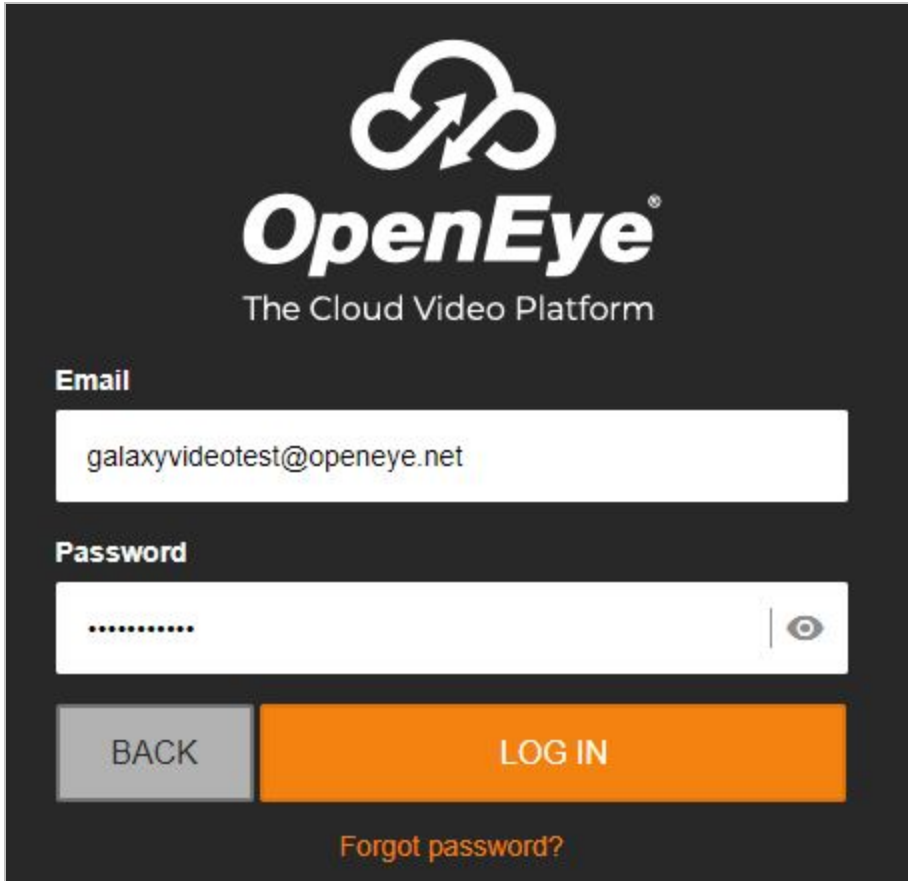
Event Date-Time	Reader/DoorName	Event Message	Person	Card Data	Show Video
07/08/2021 5:41 PM	Cluster: 055, Cont: 002, Brd: 1, Sect: 1-0	Valid Access	LeTestAdd, LeTestAdd (Card 1)	Facility Code: 146, ID Code: 23728	View Video
07/08/2021 5:41 PM	Cluster: 055, Cont: 002, Brd: 1, Sect: 1-0	Valid Access	LeTestAdd, LeTestAdd (Card 1)	Facility Code: 146, ID Code: 23728	View Video

Showing 1 to 2 of 2 entries

22 ▾ Items Per Page

Previous **1** Next

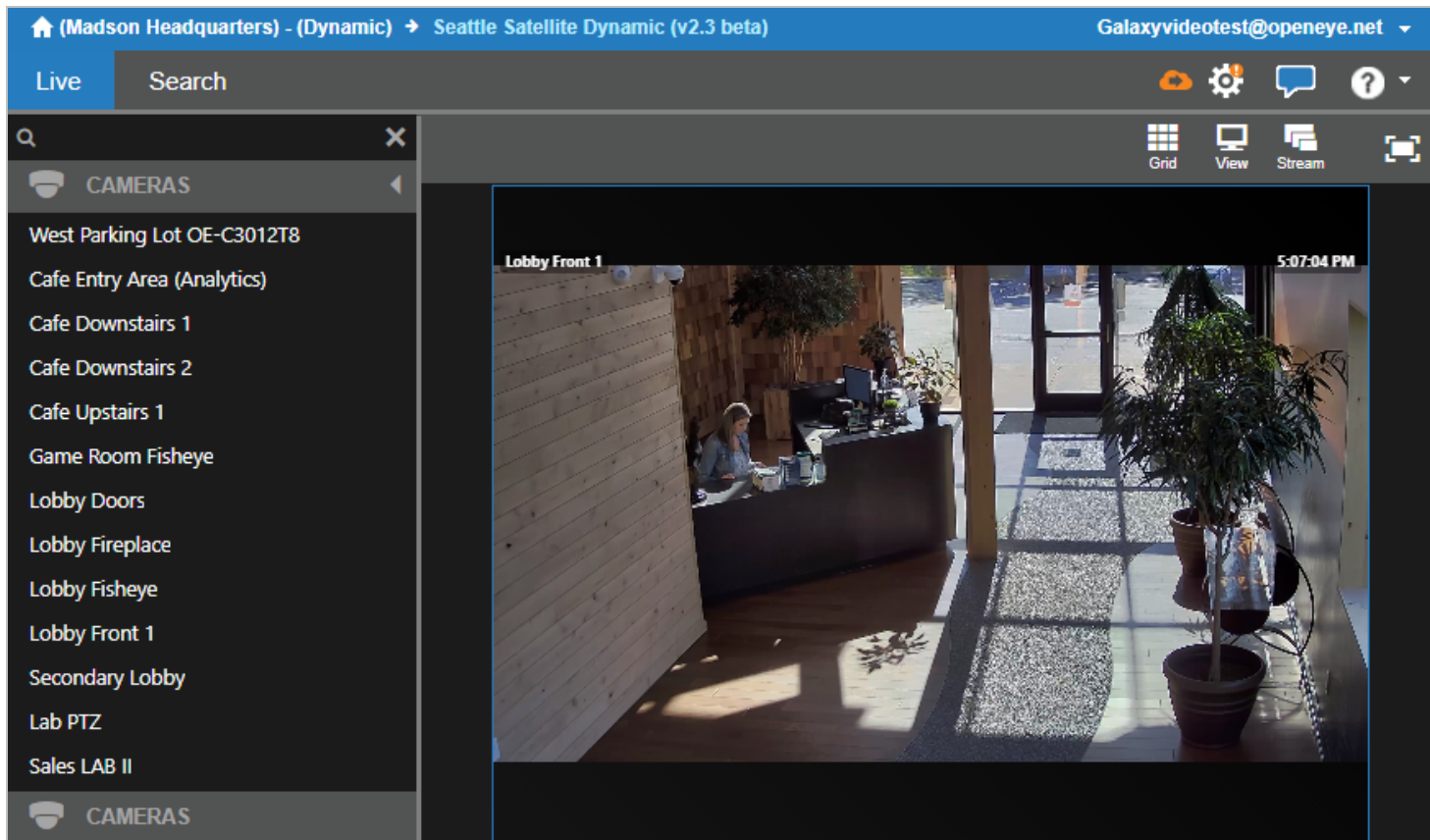
3. User must provide the valid login credentials: name/email and password.



The image shows a login page for OpenEye, a cloud video platform. The page has a dark background. At the top, there is a logo consisting of a stylized cloud with an arrow pointing upwards, followed by the text "OpenEye" in a large, bold, white font, and "The Cloud Video Platform" in a smaller, white font below it. Below the logo, there are two input fields. The first is labeled "Email" in white text, and it contains the text "galaxyvideotest@openeye.net". The second is labeled "Password" in white text, and it contains a series of dots. To the right of the password field is a small eye icon. Below the input fields, there are two buttons: a grey "BACK" button and an orange "LOG IN" button. Below the "LOG IN" button, there is a link that says "Forgot password?" in orange text.

Note: Login Page may vary slightly based on brand or setup.

4. The video from the associated camera will play.



(video feed)

Who's In Report

This topic covers functionality related to viewing the Who's In Report.

FEATURED TOPICS

[Overview and Prerequisites](#)

[Who's In - by Area \(Muster\)](#)

[Who's In - by Cardholder](#)

Overview and Prerequisites

The **Who's In Report** is a *real-time snapshot* of the List of Cardholders that are "in" a designated area (or that meet a specific criteria set by the user) when the report is queried.

PREREQUISITES AND NOTES

- The user login account must have the correct permissions needed to view and print the report.
- If there is no data to match the selected report criteria, the report will show "no data found".

TERMS

"**Real-time snapshot**" means the data is real-time at the *moment in time* the report is queried. **NOTE:** the place the *Who's In Page* remains static until the user refreshes (F5) the data. Then LaunchPoint retrieves another real-time snapshot of the data.

"**View Status**" is the selector that specifies whether the data is 'by area' or 'by cardholder'.

"**Area**" is a group of doors and readers that are configured to create a *designated secure area* in the system that can be tracked or monitored for activity. **MORE:** Areas are assigned "in" and "out" readers so that the system can track when and if any cardholders enter or leave the designated area.

RULES OF OPERATION

- The user chooses which *Status* to view (i.e., by area or by cardholder) and sets any other criteria as appropriate.
- LaunchPoint grabs a *real-time snapshot* of the Cardholders that meet the View Status and criteria.
- The Who's In Report opens and displays the List of Cardholders in a new browser tab.
- The Who's In Report (List of Cardholders) is static and does not receive updates unless the user refreshes (F5) the page.
- The *Who's In Page* cannot be printed or exported - the List of Cardholders is only viewed online.

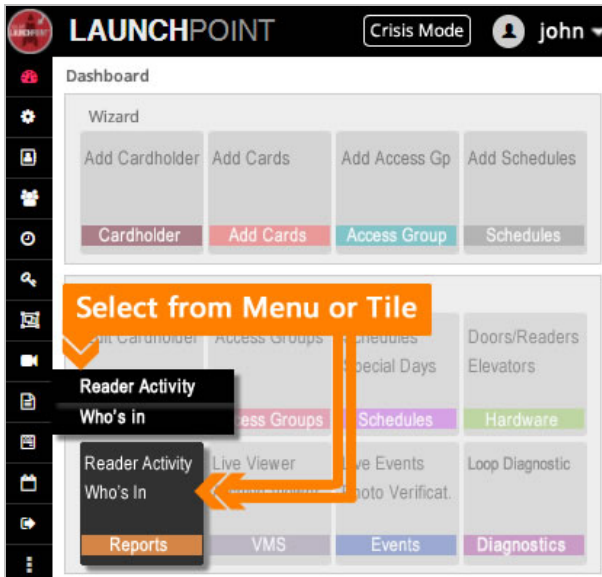
OPEN THE WHO'S IN REPORT

There are two ways to open the *Who's In Report Page* ...

- **Side Menu:** select "Reports" menu icon and select the Who's In option.
- **Dashboard:** select 'Reports' tile and select the Who's In option



← Reports Icon (from sidebar menu)



Pulling Who's In Report by Area

The fields in the page change dynamically depending on what is selected in the User Status field.

There are 2 ways to pull the Who's In Report

User can choose to pull the report ...

- by Area
- by Cardholder

The available fields will change based on whether you choose "by Area" or "by Cardholder".

Who's in

View User Status

☒ By Area
 ☐ By Cardholder(s)

Select a Loop and Area

Choose a loop

[55] Live Events 2 ▼

Choose an area

** IN ** ▼

☒ Only Show User Since Date & Time

07/13/2021 6:28 AM

Search

STEPS

1. Select the **By Area** radio button.
2. Choose a **Loop/Cluster**. (You must select a loop, you cant select more than one loop name)
3. Choose an **Area** (i.e. IN, OUT, NO AREA, or NO CHANGE, ...)
4. (optional) You can narrow your search criteria by "checking" the **Only Show Since Date/Time** checkbox and choosing a date.
5. Click the **Search** button to query the report - *which opens the Who's In Report in a new tab.*

Who's in

User Name	Current Area	Last Access Point	Last Access Time	Loop Name	Department
Parnel Roberts	** IN **	In Reader	07/08/2020 5:02 PM	Main Lab	
Victor Yung	** IN **	In Reader	07/10/2020 10:27 AM	Main Lab	
Alison Arngrim	** IN **	In Reader	07/10/2020 1:22 PM	Main Lab	
Karen Grassle	** IN **	In Reader	07/10/2020 10:26 AM	Main Lab	
Eugene Orowitz	** IN **	In Reader	07/10/2020 10:27 AM	Main Lab	

6. To refresh/update the Who's In Report, user must press F5 keyboard key.

Pulling Who's In Report by Cardholder

The fields in the page change dynamically depending on what is selected in the User Status field and other criteria.

Who's in

View User Status

☐ By Area ☒ By Cardholder(s)

☒ Advanced

Last Name

▼

Roberts

☐ Traced Cards Only

☒ Only Show User Since Date & Time

07/13/2021 6:26 AM

Search

STEPS

1. Select the **By Cardholder** radio button.
2. (optional) you can check the **Advanced** checkbox to narrow your search results.
3. Choose an **Data Field** (i.e. Firs Name, Last Name, ...)
4. (optional) You can filter results by checking the Trace Cards checkbox. When checked, the data set will only include cards with trace enabled on the card/cardholder.
5. (optional) You can narrow your search criteria by "checking" the **Only Show Since Date/Time** checkbox and choosing a date.
6. Click the **Search** button to query the report - *which opens in a new tab*.

Who's in

User Name	Current Area	Last Access Point	Last Access Time	Loop Name	Department
WilliamArnot		Cluster: 006, Cont: 001, Brd: 1, Sect: 2-0	07/12/2021 11:56 AM	[06] Todd	
joenesbitt		Safe Door	07/12/2021 5:10 PM	[04] Joe	

Page 1

▼

100 Per Page

▼

Go

Custom Report Scheduler

The *Report Scheduler* lets the user create **custom reports** for a variety of reasons. Custom reports can be saved and reused 'on-demand' or run at scheduled times.

FEATURED TOPICS

[Rules and Requirements](#)

[How to Create New Reports](#)

[List of Scheduled Reports](#)

Rules and Requirements

The Reports Scheduler includes a wide variety of reports covering *hardware activity, system event activity, card activity, cardholder population*, and more.

1. The user's login account must have the correct permissions to view and configure the report.
2. To avoid excluding data, the user must set the correct report time-span (a.k.a. the "past # hours") which is counted from the report's scheduled run-time.

For Example: If you want the report to run at 6pm to collect all the events from 8am, then you must chose to capture the **past 10 hours**. You can test your report with the run ASAP feature verify you are getting all the data from the time-frame.

3. The **red asterisk (*)** indicates a field that user must fill-out to send the report.
 - a. You must include at least 1 email recipient (red asterisk)
 - b. You must include a subject line.
 - c. You can optionally include up to 4 email recipients and one BCC (blind or back copy), as well as text in the email body that describes why you are sending the report or what it is about.

4. Whatever you put in the **Comments field** will be used as the Report Name in the 'Select Report' droplist. Be sure to use a *naming convention* that is brief and will sort and identify the report the way you want.
5. The system will generate the scheduled report even if there is no data matching your selected criteria. If you know it is incorrect to have an empty report, then verify that you have selected the correct criteria and report duration (past # hours).
6. You must have a *compatible software application* to view the reports. The report will be attached to email in 2 formats - CSV and PDF.
 - CSV file opens in MS Excel or other compatible application.
 - PDF file opens in the free *Acrobat Reader* or other compatible reader.

How to Create a New Scheduled Report

This section describes the steps to build a scheduled report and includes information about how report features work.

QUICK STEPS: Build a Scheduled Report in 7 Easy Steps ...

1. Select the **Report Type** from the cascading menu.
2. Choose "**NEW**" report.
3. Select the **Report Criteria** (filters/grouping - such as loop, department, etc.).
4. Add **Email Criteria** (i.e., recipients*, a subject*, body text, and comment, ...)
5. Choose the **Report Duration** or time-span to query (i.e., past # of hours).
6. Configure the **Report Schedule** (i.e., runtime - as in daily, monthly vs. on-demand).
7. **Save the Report** (saves the schedule & runs the report).

STEP 1 • HOW TO OPEN A SCHEDULED REPORT

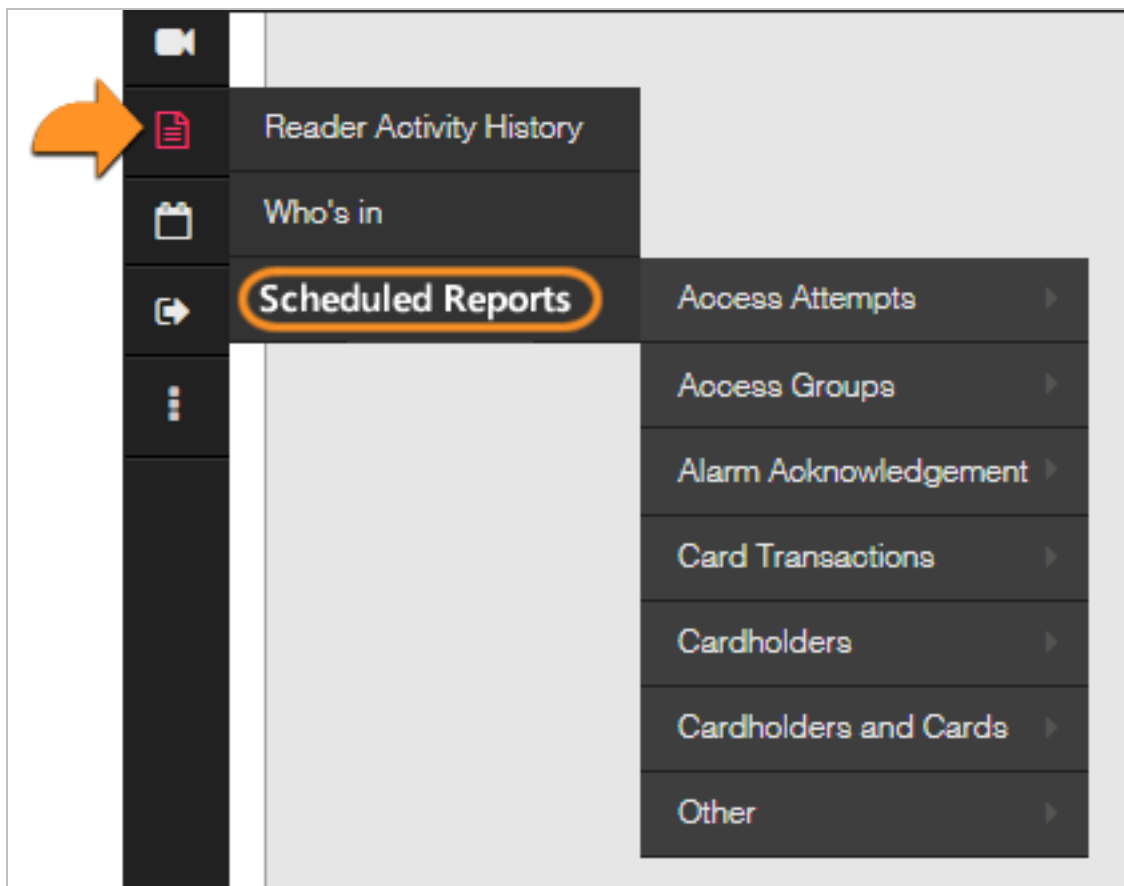
You can open the list of Scheduled Reports from the Report icon on the left side menu.

1. Click the **Report icon** on the side menu.



▪ < Reports Icon (only on the side menu)

2. When the *menu* opens, choose the **Schedule Report option** (beneath the Who's In Report).



3. When the *cascading menu* expands, choose the report you want.
See the [List of Available Reports](#) at the end of this topic.

STEP 2 • CHOOSE “NEW” REPORT

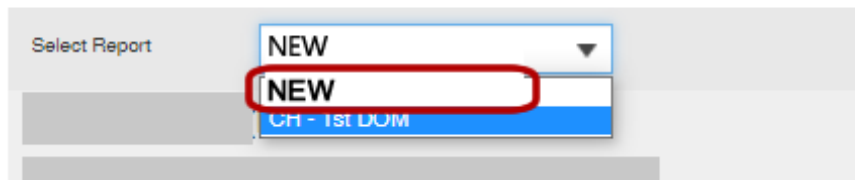
This step focuses on creating a “new” report.

About Existing Reports: You can also choose an *existing report* that has been saved. Be aware that you are not making a new copy of an existing report, but you are just changing the existing report. The report screens and data fields will work the same whether you are creating a new report or editing a report that has already been built.

1. Choose “NEW” in the **Select Report droplist** at the top of the screen.

You can also select an existing report from the saved reports that were previously built.

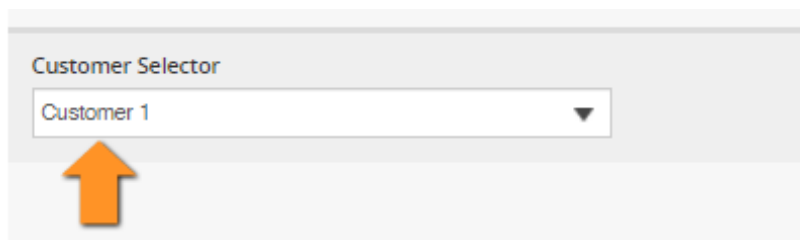
2. When you choose ‘NEW’, you begin building a new report. The report fields will be set to default options.

| LaunchPoint Report**STEP 3 • SELECT REPORT FILTER/GROUP CRITERIA**

This step selects the Report Criteria that will filter the queried report data.

About Report Criteria: Each *report type* has different criteria, such as Loop(s), Customer, Department, etc. The available criteria fields are dynamic and change according to which report you have selected. For example, if the report looks at reader activity, you will need to select which loop to filter by. If the report queries cardholder activity, you will need to select which customer or other applicable filter.

1. Select the appropriate Report Filter **Select Report droplist** at the top of the screen.
 - This field is dynamic and changes to loop or other appropriate filter, based on which report you are building.



STEP 4 • ADD EMAIL CRITERIA FOR THE REPORT

You must choose at least one **email recipient** and enter a **subject line** that identifies the report - such as 'Daily Invalid Access Attempts'.

1. Enter the **email address** of the first recipient (required).
Add up to 4 email recipients as needed.
2. Enter the **Subject text** for the email (required). The **subject text** should be always true and identify the report to the email recipient(s). You would not want specific information that is only true once if the report is going to run on a repeated cycle.

You may want to include the following in the subject line ...

- **Report Name** (such as Invalid Access, Who's In, Cardholder Activity, ...)
- **Report Cycle** (monthly, weekly, daily, or day - *such as Monday, Friday ...*)
- **Report Filter/Group** (customer, department, loop(s), or other filters ...)
- **Report Duration** (the time-span covered - morning ,

For example, if the Invalid Access Report is sent daily, then you may want to name the report "Daily Invalid Access for Department" in the subject line.

Email Recipient 1:	creynolds@yourcompany.com
Email Recipient 2:	
Email Recipient 3:	
Email Recipient 4:	
Email Recipient Bcc:	
Email Subject:	Daily Invalid Access by Customer
Email Body:	To whom it may concern ...
Comments:	CH - 1st DOM

- 3. Enter email **Body text** as desired (optional). Use *consistent description* that explains the scope/criteria, and detailed definition of the report data. This text you enter here should be always true regardless of how many times the report cycle will run.
- 4. Whatever you enter in the **Comments field** will become the report name in the 'Select Report' droplist.
- 5. Add a **BCC Recipient** as desired (optional).

STEP 5 • CHOOSE THE REPORT DURATION (Past # Hours)

This field is dynamic and does not always display depending on which report you are pulling. The report duration sets how many *past number of hours* the report data is queried - counting from the runtime.

For example: If you need to see all *reader activity* since 8am, and you run the report at 6pm, then you will want the duration (past # hours) to be at least the **past 10 hours**. Make sure to test your report.

- 1. Enter a numeric value that is large enough to capture all the data you need to see.

...

STEP 6 • CHOOSE THE REPORT CYCLE (Scheduled vs On-Demand)

The report cycle is the scheduled time that you want the report to run or process - i.e., the run-time.

1. Choose "Run Daily" or "Run Advanced" if you want the report to run on a scheduled basis.

- a. Running Daily is shown below ...

Select (check) one or more days and choose the run time (hh:mm).

Choose AT LEAST one Schedule from the following

☐ Disabled ☐ Run ASAP ☒ Run Daily ☐ Advanced

Choose AT LEAST one item from the following

☒ Monday

☒ Tuesday

☒ Wednesday

☒ Thursday

☒ Friday

☐ Saturday

☐ Sunday

Runs at the following HOUR.

12 am ▼

...and the following MINUTE

00 ▼

Last Update

- b. Running Advanced (monthly or quarterly, etc. ...

Select (check) one or more days of the month or quarter; and choose the run time (hh:mm).

Choose AT LEAST one Schedule from the following

☐ Disabled ☐ Run ASAP ☐ Run Daily ☒ Advanced

Choose AT LEAST one item from the following

☒ First Day of the Month
☐ Fifteenth Day of the month
☐ First Day of the Quarter
☐ Last Day of the Quarter

Runs at the following HOUR.

12 am ▼

...and the following MINUTE

00 ▼

Last Update


2. (optional) Choosing "Run ASAP" will run the report on-demand.

Skip this step if you scheduled the report.

- a. Select the **Run ASAP** option.
- b. Click **Save** to run the selected report.

Choose AT LEAST one Schedule from the following

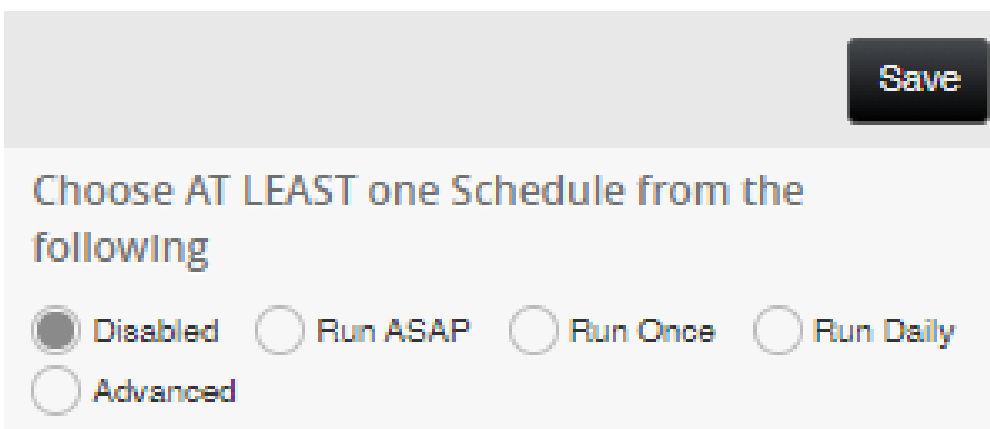
☐ Disabled ☒ Run ASAP ☐ Run Daily ☐ Advanced



3. (optional) Choosing "Disabled" will stop the report run cycle indefinitely.

Skip this step if you scheduled the report.

- a. Select the **Disabled** option.
- b. Click **Save** to disable the selected report.



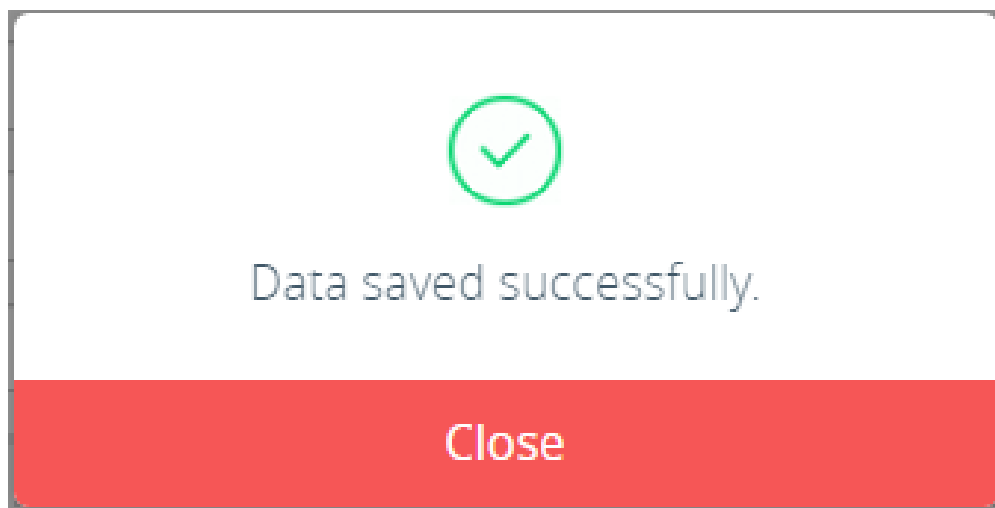
A screenshot of a user interface showing a 'Save' button in the top right corner. Below it, the text 'Choose AT LEAST one Schedule from the following' is displayed. Underneath, there are five radio button options: 'Disabled' (which is selected), 'Run ASAP', 'Run Once', 'Run Daily', and 'Advanced'.

STEP 7 • SAVE YOUR REPORT

Saving the report will add it to the Report Selection droplist at the top of the screen.

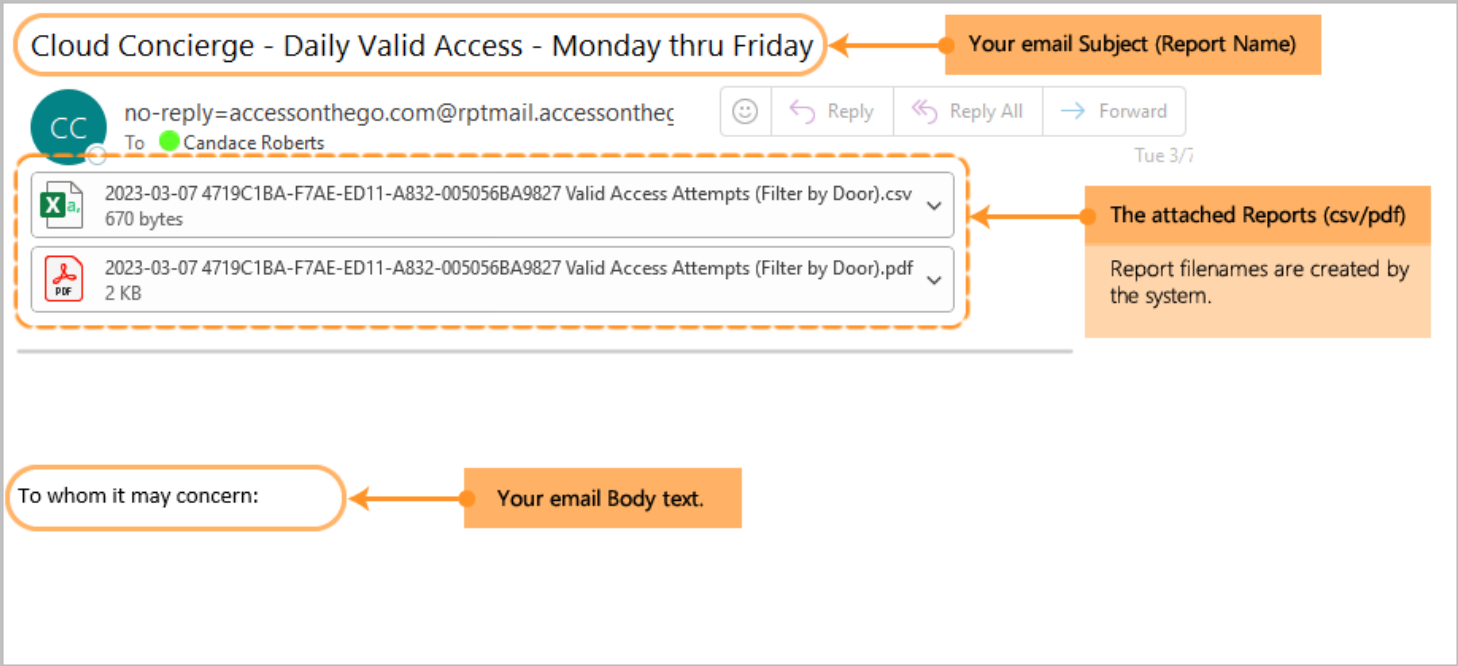
1. Click the **Save** button to save the report. Report will be added to the Report List at the top of the screen where you can select it again to edit whenever you need.

The system should display a user prompt to confirm your report has been successfully saved.



2. The scheduled report will be distributed as an **email attachment** to the chosen recipients.

The report is sent as an email attachment in two formats - i.e., CSV (Excel) and PDF.



Above image is an example of email attachments when scheduled reports run.

	A	B	C	D	E	F	G	H	I
1	CLIENT_NAME	PERSON	LAST_NAME	FIRST_NAME	CARD	FAC	CARD_ID	ACCESS_PROFILE	EXPIRATION
2	Dynacorp	Active	Jacobson	Jeff	Active	23	48793	Night Shift	Never
3	Dynacorp	Active	Brady	Marsha	Active	23	49025	Night Shift	Never
4	Customer 1 {Customer 1 Dept 1}	Active	Aaronson	Aaron	Active	23	47899	General Employees Profile	Never
5	Customer 1 {Customer 1 Dept 1}	Active	Abrams	Angela	Active	23	48621	General Employees Profile	Never
6	Customer 1 {Customer 1 Dept 1}	Active	Arnold	Charles	Active	23	48795	General Employees Profile	Never
7	Customer 1 {Customer 1 Dept 1}	Active	O'neal	Patrick	Active	23	48756	Customer 1 profile	Never
8	Customer 1 {Customer 1 Dept 1}	Active	Smith	Rupert	Active	23	49909	Customer 1 profile	Never
9	Customer 1 {Customer 1 Dept 1}	Active	Randalls	Paul	Active	23	47881	Customer 1 profile	Never
10									

Example of a CSV Report opened in MS Excel (above)

List of Available Scheduled Reports

Below is a list of the available Reports that you can create. The available filtering criteria will dynamically change to suit the Report you select - i.e., filter my loop, access group, department, etc.

NOTE: The system will produce the report even if there is no data matching your selected criteria. If you get an empty report, either there is no data matching your criteria, or you need to adjust your report duration or other criteria to get the data you expect.

1. **Access Attempts**
 - a. Valid Attempts
 - b. Invalid Attempts
2. **Access Groups**
 - a. Member by AG
 - b. Member by Loop
 - c. Summary
3. **Alarm Acknowledgments**
 - a. Doors n Readers
 - b. Guard Tour
 - c. Inputs
4. **Card Transactions**
 - a. By Cardholder
 - b. By Customer, order by cardholder (name)
 - c. By Door and Access Profile
 - d. By Door
 - e. By Input ID
 - f. By Loop
 - g. Related card transactions
5. **Cardholders**
 - a. By Access group
 - b. By Access Profile
 - c. By Customer
 - d. By Department
 - e. By Door
 - f. By Facility Code
 - g. Disabled Cardholders
6. **Cardholders and Cards**

- a. By Customer

7. **Other**

- a. Low Battery Wireless (readers)
- b. Who's In (personnel muster report)