LiftOff™

Administrator's Guide PDF

Ashley Mascari, braXos Security

Revision History

Revision	**05/14/2024**
Version 2.25.0	

LiftOff™ : Administrator's Guide PDF

by Ashley Mascari

Abstract

This guide provides detailed steps on how to manage LiftOff from an Administrator's view.

Table of Contents

List of Figures

List of Examples

Chapter 1. Overview

LiftOff is a suite of products that include:

Licensed Products

LiftOff Mobile™	Touchless elevator dispatching powered by the LiftOff mobile app. Options include Lightning VMS™ and Access Control Sync™
Ascent™	Elevator kiosk management and destination authorization through portal-managed credentials
Concert™	Elevator kiosk management and destination authorization through access control system-managed credentials
Access VMS™	Visitor Management for elevator access via access control credential provisioning

This guide documents the user-interface components of LiftOff that property administrators use to:

- Enroll users, both actively and passively
- Grant access to secured floors
- Grant special elevator calling privileges (such as VIP)
- Manage roles
- Adjust building-wide settings
- Run Reports

For those properties licensed for Access VMS™ or Lightning VMS™, the Commander portal allows visitor hosts and security to:

- Invite visitors
- Check-in visitors
- Re-send visitor credentials

These operations are performed in LiftOff's Commander portal, accessible via any modern browser at:

https://liftoff.braxos.com

Before logging into LiftOff Commander, the property manager, security, or visitor host must install the LiftOff mobile app and define a PIN code, which is used to authenticate to the portal. Before that can happen, the property manager must have been granted either the Administrator or Approver role by a fellow Administrator or by braXos Support (support@braxos.com).

Chapter 2. Commander Login

Installation of LiftOff Mobile

Introduction

LiftOff Mobile™ is delivered to consumers as a mobile application that utilizes BLE (Bluetooth Low Energy) technology to validate physical presence inside a LiftOff Mobile™-enabled building. In addition to LiftOff Mobile™ consumers, elevator installers, building administrators, and visitor hosts use the LiftOff application to manage access to LiftOff Commander at buildings licensed for LiftOff Mobile™, Ascent™, Concert™, and Access VMS™. This chapter documents the process of enrollment and configuration from the property manager or visitor host perspective.

OS Requirements

LiftOff mobile requires an iOS or Android device. Currently, iOS 13.0+ is required.

Installation

To install LiftOff, visit the Apple App Store (iOS) or Google Play Store (Android) with the mobile device on which the application ought to be installed. Once installed, the LiftOff icon will appear on the home screen:

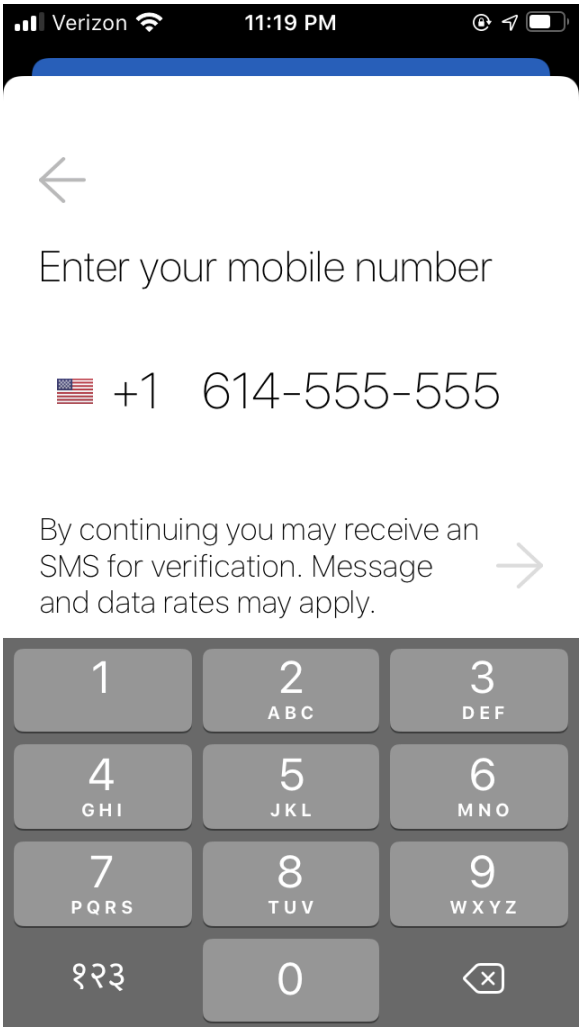
Figure 2.1. LiftOff Home Icon

Tap the LiftOff icon to begin the enrollment process.

Registration

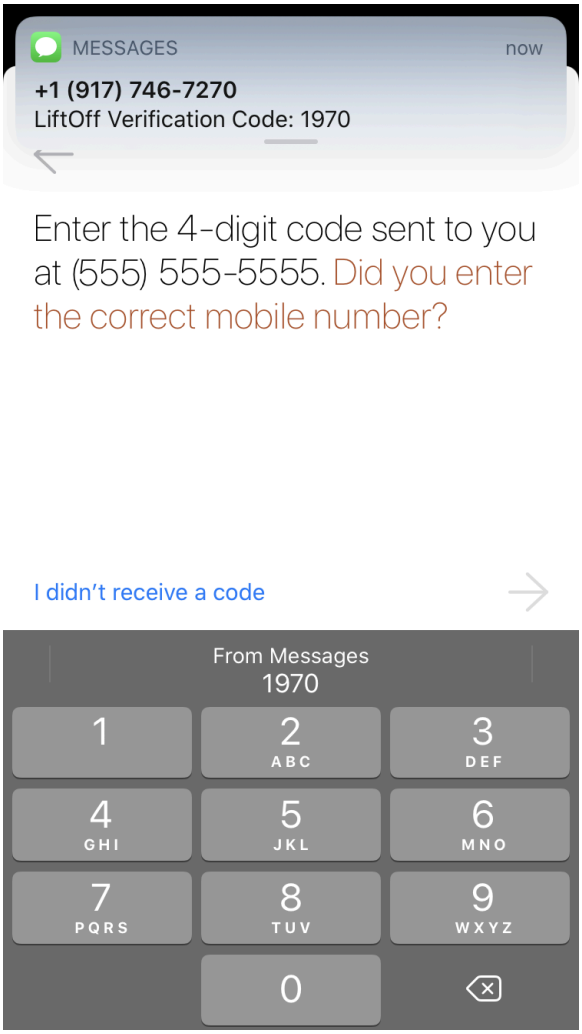
When LiftOff is first launched, the property manager or visitor host will be prompted for the phone number of the device on which LiftOff will be used:

Figure 2.2. Registration



LiftOff attempts to automatically determine the appropriate country and phone number format, but the default determination can be changed. Once the phone number is entered, an SMS verification code will be transmitted to the device:

Figure 2.3. Verification



On iOS, tapping "From Messages" will automatically insert the SMS verification code. Once verified, LiftOff will ask for the First Name (Given Name), Last Name (Surname), and email address. LiftOff will then attempt to locate nearby LiftOff buildings and will display them.

Note

The verification code sent via SMS is valid for five minutes. Once five minutes has been exceeded, re-entry of the phone number is required.

iOS and Android will ask for application privileges:

- Location Services
- Bluetooth
- Notifications

For those buildings licensed for LiftOff Mobile™, choose "While Using the App" for location services, or, if AutoLift and QuickLift support is desired, choose "Always".

Request for Commander Access

Before a PIN code can be assigned in the LiftOff app for use in accessing LiftOff Commander, the property manager or visitor host must have been granted the role of Administrator, Approver, Security, or VisitorHost. There are three approaches to acquiring the role once the LiftOff mobile app has been installed:

- An existing building Administrator uses the Users panel to enroll the property manager or visitor host, either with the Add User function, or via a CSV upload, and then assigns the appropriate role
- The person desiring Commander access uses LiftOff mobile's "Request Access" feature to request access, and an existing Administrator or Approver grants it, including the role membership
- If this is the first property manager for a building, either the Elevator Mechanic, during the turnover process, or braXos support enrolls the initial Administrator

In the last case (first property manager), an email to braXos support (support@braxos.com) with name, phone number, and email will cause the initial property administrator to be enrolled in the building.

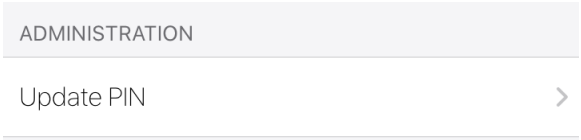
PIN Creation

Once either braXos Support or a fellow Administrator/Approver has granted Administrator, Approver, Security or VisitorHost roles, the property manager or visitor host can use the LiftOff app to assign himself or herself a PIN code used to authenticate to LiftOff Commander. To do so, launch LiftOff mobile, tap the Settings gear:

Figure 2.4. Settings Gear

A section title, ADMINISTRATION, should be displayed. This is only displayed if the LiftOff account has been granted Administrator, Approver, Security or VisitorHost privileges by either braXos Support or a fellow Administrator or Approver. Tap Update PIN to set the 4-digit PIN Code:

Figure 2.5. Update PIN



LiftOff will require some form of biometric verification (e.g.: TouchID, facial recognition) to update the PIN to ensure the PIN code has been set by the phone's owner. Note the PIN code assigned, as it is used with two-factor authentication in LiftOff Commander.

Note

Avoid PIN codes that are easily guessed. Examples include: 1111 and 1234.

LiftOff Commander

Once a property manager or visitor host has assigned himself or herself a PIN code in LiftOff mobile, the property manager or visitor host can log into LiftOff Commander:

https://liftoff.braxos.com

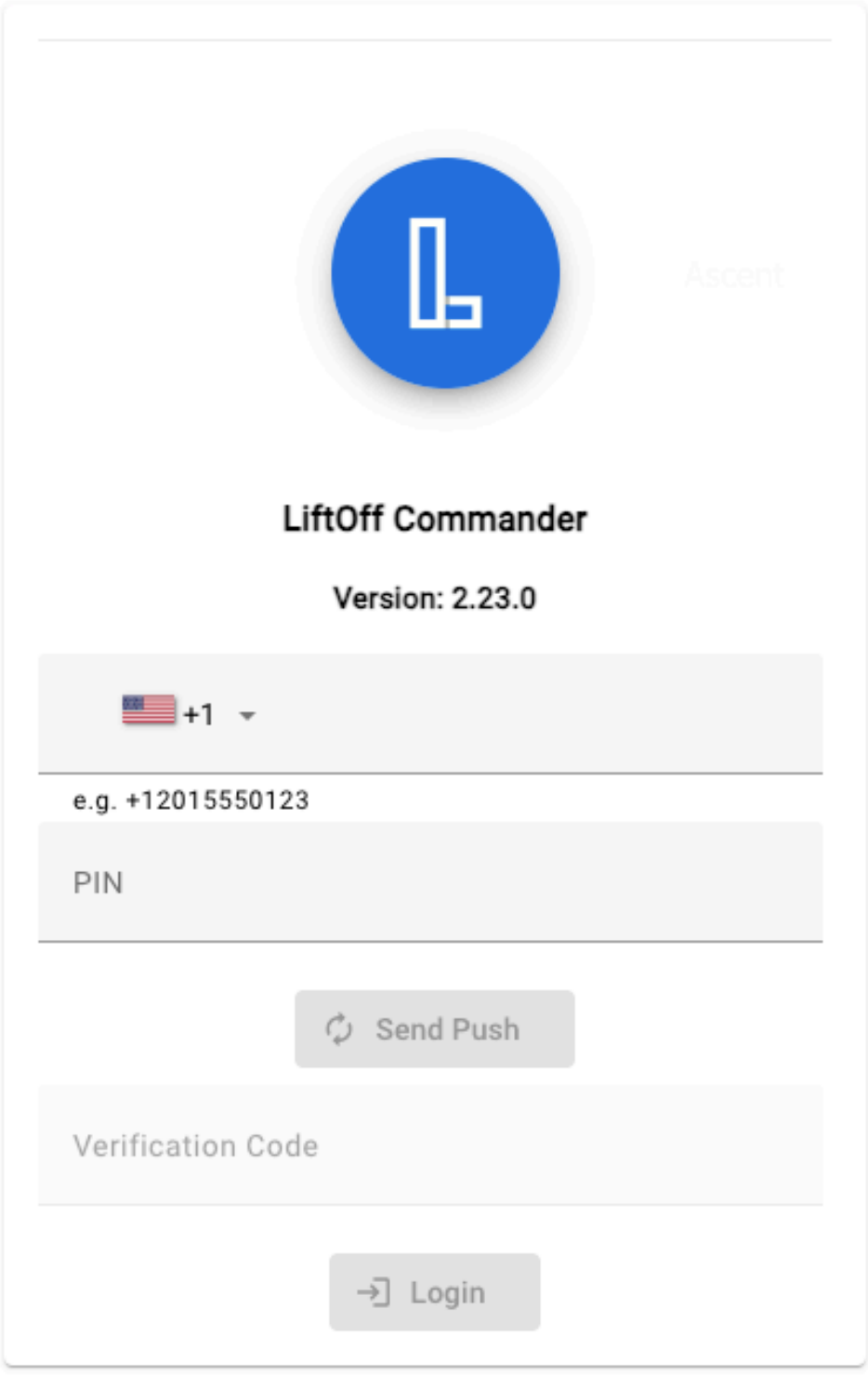
Requirements

Any modern browser may be used, but Google Chrome™, FireFox™ or Microsoft Edge™ is recommended.

Login

To login into LiftOff Commander, enter the aforementioned URL. The property manager will be presented with a two-factor login screen:

Figure 2.6. Login



The phone number and PIN code should be the values supplied to LiftOff mobile. Once supplied, clicking “Send Push” will result in a push notification sent to the mobile device. The verification code can then be used to authenticate to LiftOff Commander.

Chapter 3. Commander Portal

Building Selection

Once authenticated, the property manager or visitor host can choose the active building by selecting the building from the site drop-list in the navigation bar at the top of the page. If the site desired is not in the list, please contact support@braxos.com:

Figure 3.1. Building Selection

Security Toggle

For buildings licensed for Concert™ or Ascent™, a Security Toggle control is available next to the building selection:

Figure 3.2. Security Toggle

If the toggle is enabled, security is enforced at the elevator kiosks. Users will have to present a valid security credential to call a destination that they are authorized to access. If the toggle is disabled, security is not enforced and all destinations will be accessible by riders, per the default configuration of the elevator manufacturer. Only Administrators in buildings licensed for Concert™ or Ascent™ may toggle security on or off.

Appliance Connection Status

Adjacent to the user profile avatar is the Appliance Connection Status icon. This indicates whether or not a gateway appliance is successfully communicating with the cloud. If the appliance is communicating successfully, a connected cloud is rendered:

Figure 3.3. Appliance Connected

Hovering over the icon will display the date and time the connectivity was established. If the appliance is not communicating with the cloud, a broken cloud icon is displayed:

Figure 3.4. Appliance Disconnected

Appliance Icons

A building may be licensed for more than one product, such as LiftOff Mobile™ and Concert™. If so, multiple appliance icons will be displayed. The color of the icon indicates which appliance status is being reflected:

Appliance Colors

ESA: Gold — Ascent™ appliance (Elevator Security Appliance). Used to communicate with the cloud and the elevator controller as the primary security system.

LGA: White — LiftOff Mobile™ appliance (LiftOff Gateway Appliance). Used to communicate with the cloud and the elevator controller using the direct call interface.

ACG: Blue — Access VMS™ appliance (Access Control Gateway). Used to communicate with the cloud and the access control system for the provisioning of visitor credentials.

HGA: Coral — Concert™ appliance (Hybrid Gateway Appliance). Used to communicate with the cloud and both the access control system and the elevator system.

Behavior while Disconnected

For LiftOff Mobile™-licensed buildings, if the appliance is in the disconnected state, mobile application calls will fail and users will receive a notification that their request to dispatch an elevator has given up after twenty seconds. Please reach out to your elevator manufacturer's elevator mechanic to resolve the issue.

Note

Users may still receive timeouts waiting for a car assignment even though there is no issue with appliance connectivity to the cloud. If this occurs, please reach out to your elevator manufacturer for support.

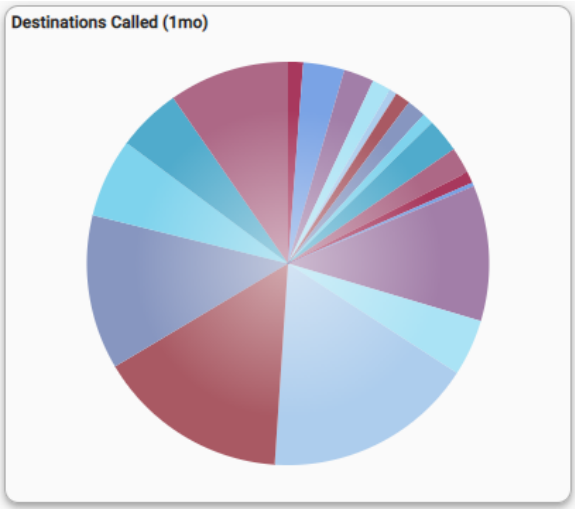
For Concert™ or Ascent™-licensed buildings, if the appliance is in the disconnected state, changes to the building configuration: schedules, floor access groups, card formats, etc., will not be reflected at the elevator kiosks.

For Access VMS™-licensed buildings, if the appliance is in the disconnected state, visitor credentials will not be able to be synchronized to the building's access control system.

Dashboard

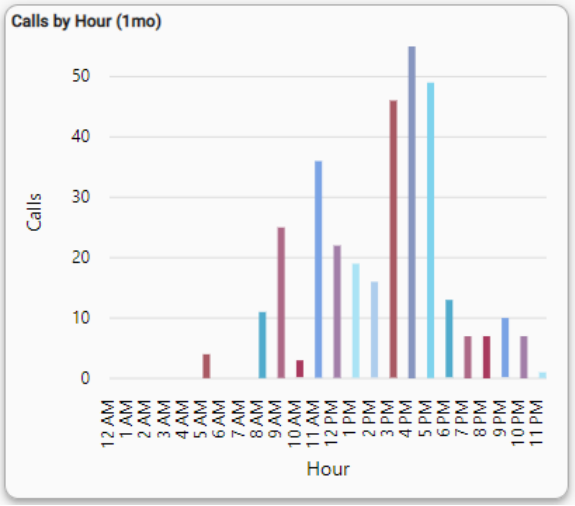
After logging in, the property manager will be presented with a dashboard of four widgets reflecting the last 30 days worth of elevator car calling statistics:

Figure 3.5. Destinations Called



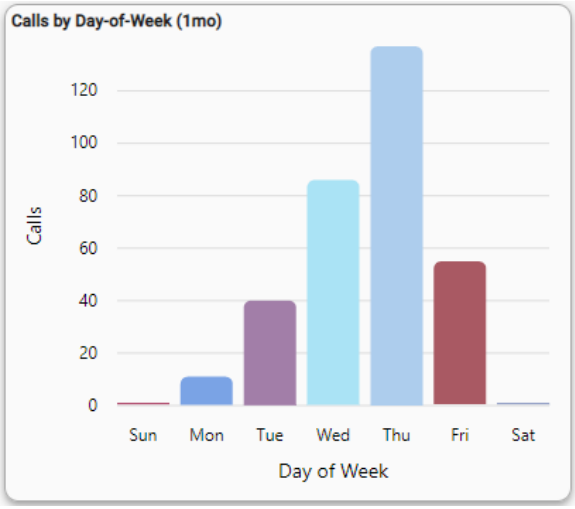
The Destinations Called widget shows graphically the percentages each accessible destination is called.

Figure 3.6. Calls by Hour



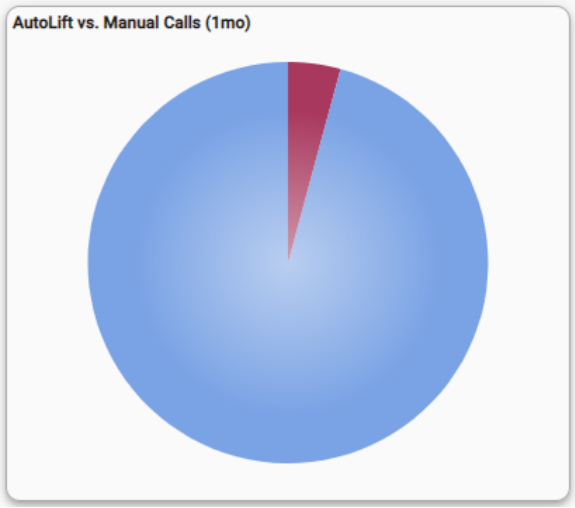
The Calls by Hour widget displays as a vertical bar chart the total times during the day when the elevator has been called.

Figure 3.7. Calls by Day-of-Week



The Calls by Day-of-Week widget shows a vertical bar representation of the total number of calls based upon the weekday.

Figure 3.8. AutoLift vs. Manual Calls

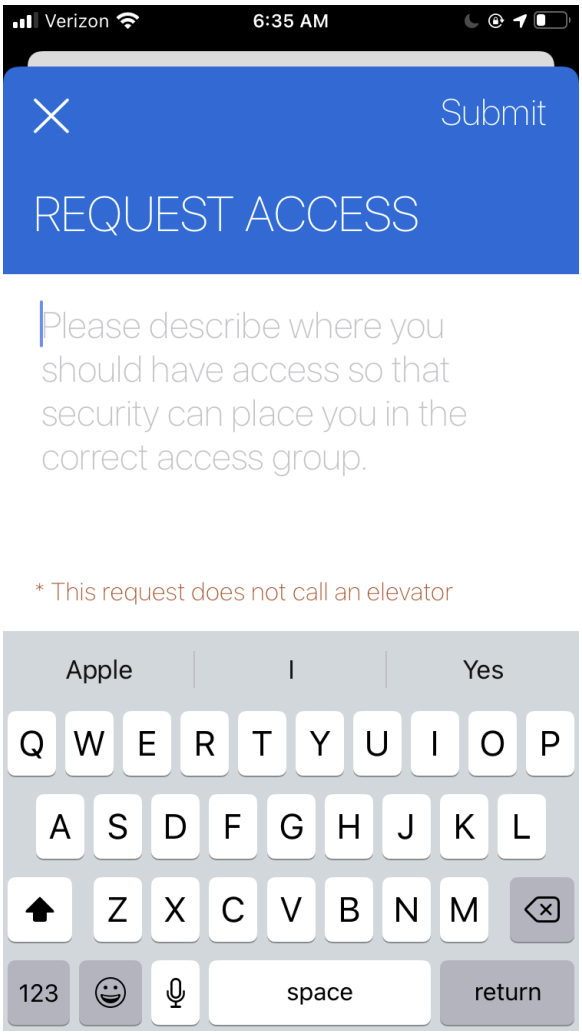


For buildings licensed for LiftOff Mobile™, the AutoLift vs. Manual Calls (1mo) pie chart shows the percentage of calls placed automatically via LiftOff mobile's Auto Lift feature vs. those calls placed by a user explicitly selecting a destination floor.

Pending Requests for Access

Requests for access can be made for multiple reasons: A rider may not see a destination that they feel they ought to be able to access; a new administrator or visitor host may be requesting on-boarding. Using the LiftOff mobile application, they can submit a request for access:

Figure 3.9. Request for Access



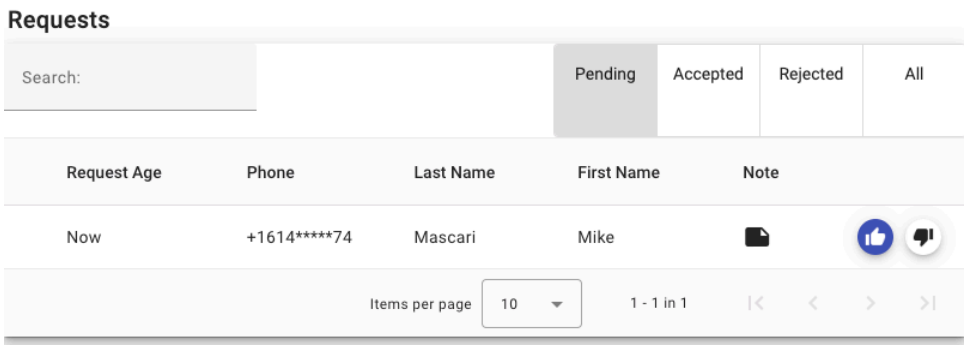
Once the access is submitted, two things occur:

- A push notification will be sent to all property managers who have the Approver role
- A pending notification status will be set in Commander's top navigation:

Figure 3.10. Request for Access

Clicking on the Pending Notification icon in Commander's top navigation displays the Request for Access approvals panel:

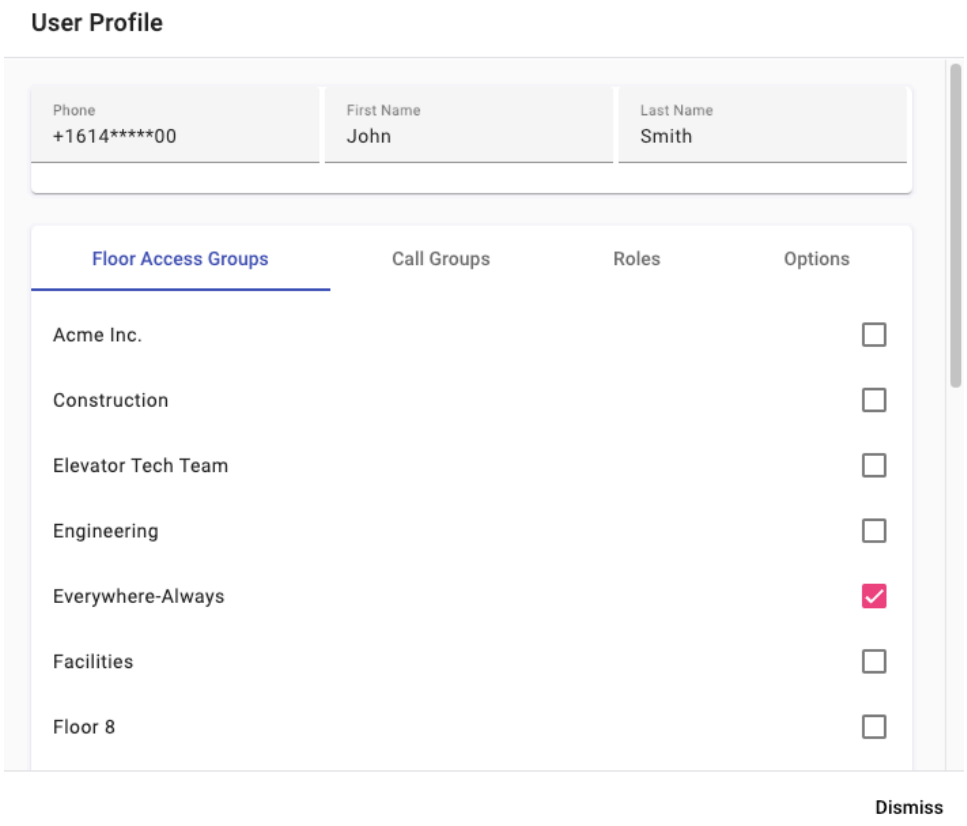
Figure 3.11. Pending Requests



Hovering over the Note reveals the content of the request. The property manager may then either accept or reject the request by clicking the "thumb's up" or "thumb's down" command button. In either case, a push notification is sent to the requestor as to the status of the request.

If a "thumb's up" is given, the LiftOff user is automatically enrolled in the building and the Approver is presented with the user's LiftOff profile:

Figure 3.12. User Profile



Clicking the Accepted tab displays all previously approved requests. Conversely, clicking the Rejected tabs shows those requests that have been rejected. A previously rejected request can be approved later by clicking the "thumb's up" command button. Clicking All shows all requests.

Note

In addition to receiving a push notification at the time a request has been submitted, property managers with the Approver role will receive a push notification once per hour until all pending requests have been resolved.

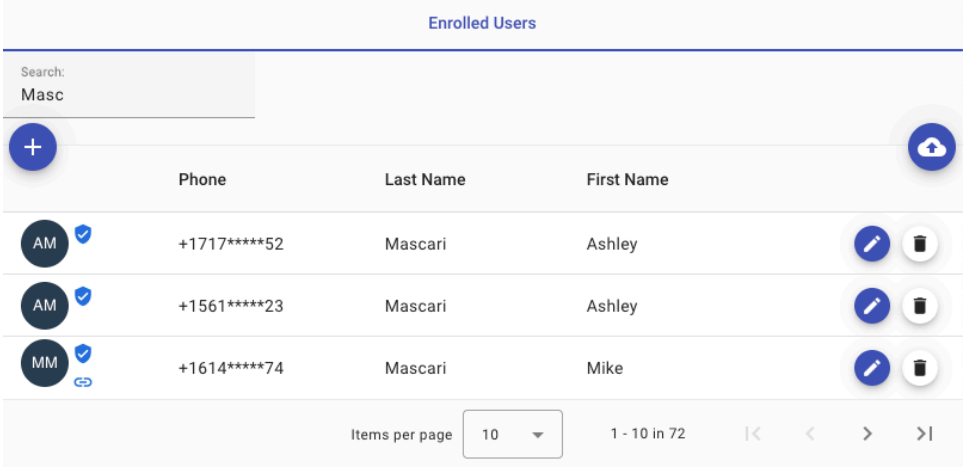
Chapter 4. Users

The Users panel allows property managers to:

- Manually enroll LiftOff users into the building
- Enroll LiftOff users into the building via batch CSV
- Edit User privileges in the building
- If licensed, manage an access control system sync

User Search

Figure 4.1. User Search



The Search control allows for searching for users by Last Name, First Name, or that part of the phone number that remains unobfuscated following enrollment.

If a blue check-mark is next to a user, then the user has installed LiftOff mobile and enrolled a device:

Figure 4.2. Confirmed Avatar

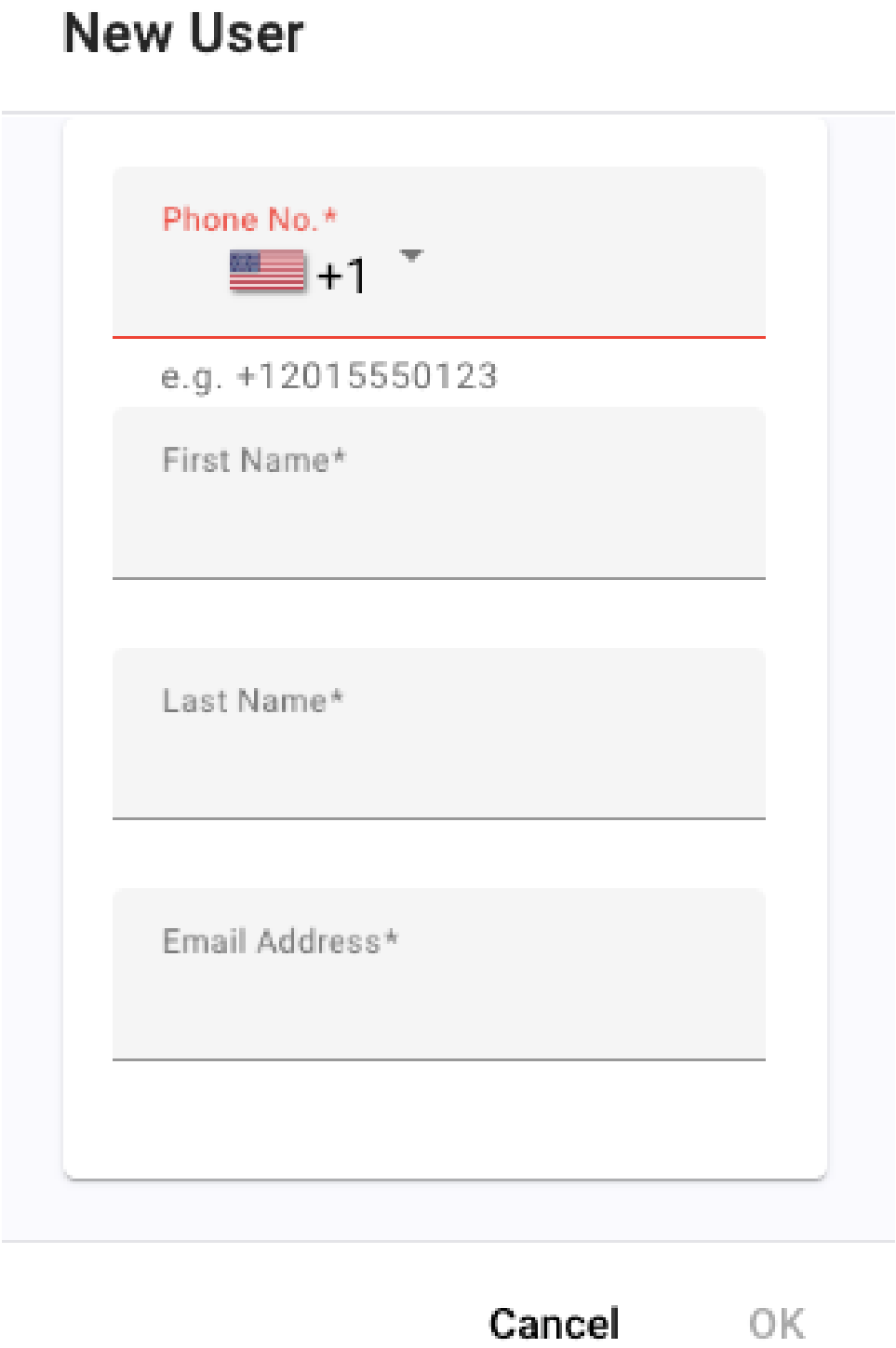
For LiftOff Mobile™ buildings licensed with an Access Control Sync™, if a chain link is next to a user, then the user's floor access and active status is being synchronized from an access control system.

Figure 4.3. Linked Avatar

Adding a New User

To add a new user, click the “+” action button to bring forward the New User dialog:

Figure 4.4. New User



As with installing the LiftOff mobile app, adding a New User requires the phone number, first name, last name, and email address. Users come in two flavors: they

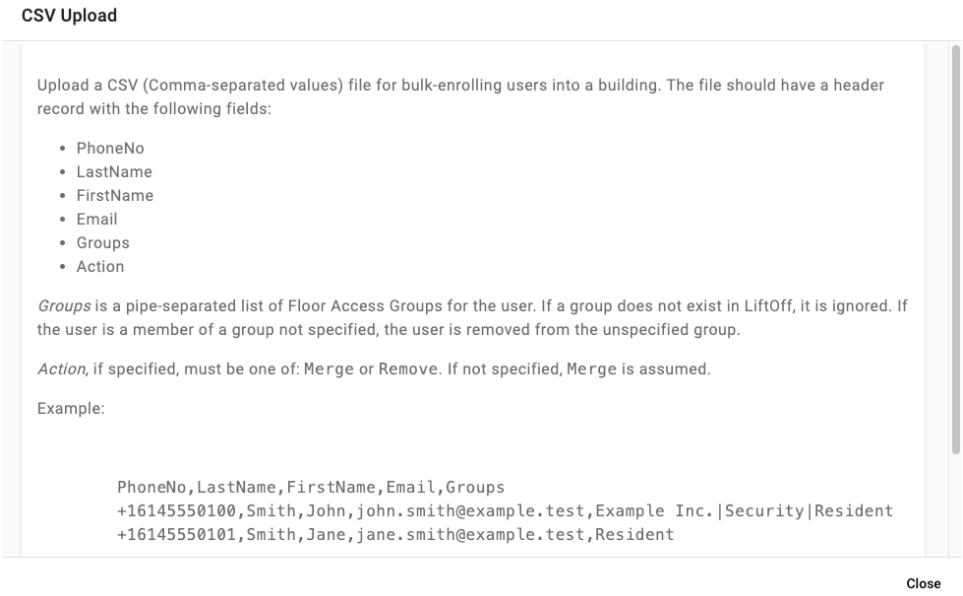
are either exclusively Commander portal users in the case of Concert™ and Access VMS™ or they are both end-users and potentially Commander portal users in the case of LiftOff Mobile™ or Ascent™. Adding new users can be performed prior to the user installing the application, so long as the user uses the same phone number and last name at the time of mobile application installation. This allows the property manager to place the user into the appropriate Floor Access Groups and Roles prior to the application being installed on the user's device.

As previously stated, if the user has already installed the LiftOff mobile application using the same phone number and last name, a blue check-mark will appear next to the user's avatar.

CSV Upload

On the Users panel, click the cloud CSV Upload command button to perform a bulk upload of users from a CSV file:

Figure 4.5. CSV Upload



The CSV Upload dialog allows for a CSV file to be submitted for batch processing. Like the New User dialog, the phone number, last name, first name, and email values are required.

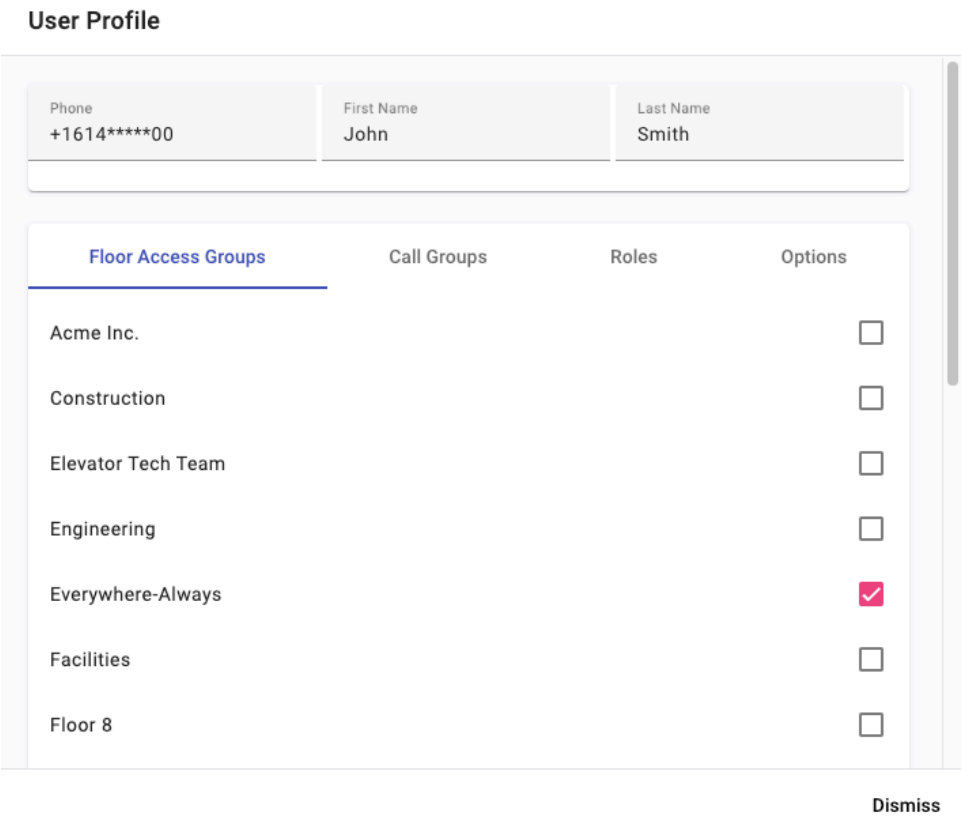
Optionally, a Groups field can be supplied which will indicate which Floor Access Groups the users ought to be placed into. If the Groups field is present in the CSV file, and a user is currently a member of a group not specified in the CSV data, the user is removed from the group.

Similarly, an Action field can be supplied to either upsert (Merge) or unenroll (Remove) users from the property. If the action is Merge, the data will be used to either enroll a new user or update the group membership of an existing user. If the action is Remove, the user will be unenrolled from the building entirely. This has the same effect as clicking the "trashcan" command button next to the user's profile in the User panel.

User Edit

By clicking the “pencil” command button on the associated User record, a user’s floor group membership, call group membership, and roles may be edited by the property manager. When clicked, the User Profile dialog is presented:

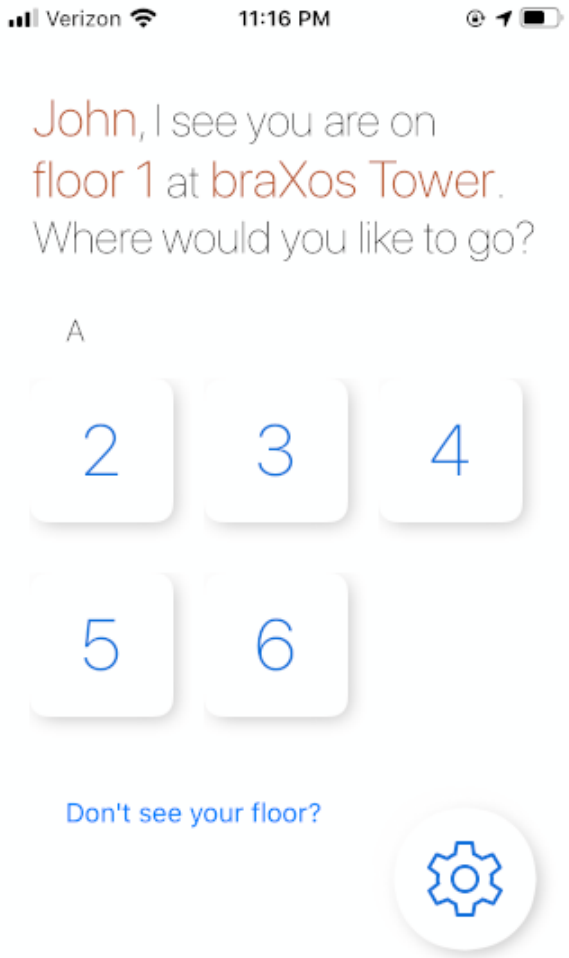
Figure 4.6. User Edit



Floor Access Groups

The User Profile dialog allows the property manager to assign or unassign membership in one or more of the building’s Floor Access Groups. For LiftOff Mobile™ and Ascent™, Floor Access Groups define which destination floors are callable from which source floors and when for a group's members. By ticking or unticking the relevant Floor Access Group’s checkbox, the user is immediately added to or removed from the Floor Access group. This impacts what the LiftOff Mobile™ user sees when in proximity of an elevator bank:

Figure 4.7. Destinations



For Ascent™ users, the authorized destinations at the kiosks will immediately reflect the change in group membership.

Note

The floors displayed to a user, either on the mobile app for LiftOff Mobile™ users or at the elevator kiosk for Ascent™ users, are the *union* of all the available destination floors from all the Floor Access Groups the user is a member of, contingent upon the time of day and the floor they are on.

For Access VMS™ and Lightning VMS™ users, membership in a Floor Access Group gives that user, if also granted the VisitorHost role, the ability to invite visitors to any destination configured as accessible in the Floor Access Group.

For Concert™ users the tab is not displayed, as membership in a Floor Access Group in Commander has no impact. Cardholders' effective group membership is dictated by the access groups indicated in the access control system.

Call Groups

The Call Groups tab similarly allows the property manager to edit the membership of a user with respect to call groups defined in the building. Call Groups define special elevator calling privileges, such as VIP, which are then used when the rider places a call via LiftOff mobile. Like Floor Groups, ticking or unticking the membership has an immediate impact and is relevant to buildings licensed for LiftOff Mobile™ or Ascent™. The Call Groups tab is not displayed if the building is only licensed for Concert™ or Access VMS™.

Roles

Roles determine which roles the user has been granted. Currently, the roles defined in Commander are:

- Approver – has access to approve requests for access, receives push notifications of requests, has authority to add and remove users from Floor Access Groups and Call Groups. Can grant Approver to other users, but no other role. An Approver can also change the schedule on which a Floor Access Group or Call Group operates as well define new Floor Access Groups and Call Groups.

- Administrator – has the same privileges as Approver, but does not receive request for access push notifications unless he or she is also granted the Approver role. Also has access to Schedules, Settings, and Reports. An Administrator can grant Administrator or Approver role to building users.

- Deployer – has specific privileges for programming beacons for LiftOff Mobile™ buildings and defining elevator banks for LiftOff Mobile™, Ascent™, and Concert™ buildings. This includes defining which special privileges are available in the building based upon elevator controller software capabilities. A Deployer can only grant Deployer role to building users.

- Support – has all privileges and is a braXos employee. Users with the support role can grant any role to any building user.

Note

Once a role has been granted, the user may then log into LiftOff Commander. All roles require two-factor authentication in order to authenticate.

Options

If the building is utilizing an external source of data, 3rd party API, or has a turnstile integration with braXos Steward, the details of the synchronization are displayed in the Options tab. Specifically:

- External ID

  This displays the external identifier that is linked to the user's profile from the external system. When synchroniation of floor access groups or call groups is performed, this identifier is used as the key to correlate the data from the source system.

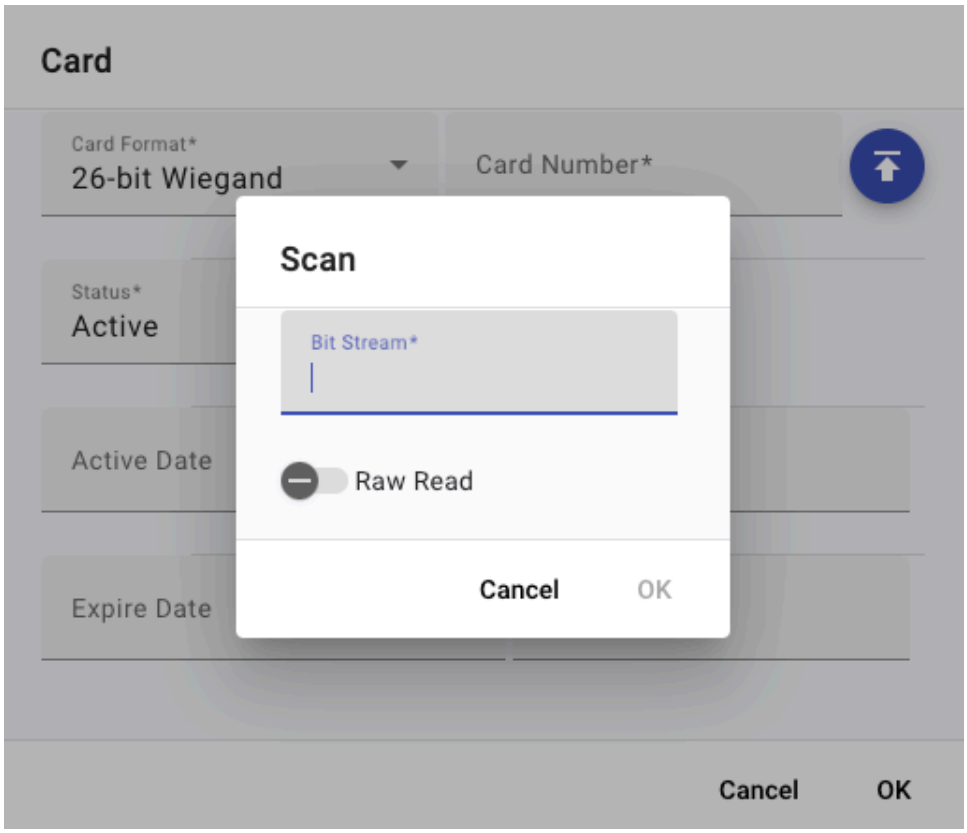
- Home Floor

This displays the home floor of the user. Currently, this may only be set by a 3rd Party's use of the API. Once set, this is used by the braXos Steward turnstile integration to determine which floor to place a call for when a user proceeds through a turnstile.

Cards

If the building is licensed for Ascent™, the Administrator or Approver can issue a physical credential to the user that can be used with traditional card readers to unlock authorized areas. The Cards tab provides the means by which a user's credentials are managed:

Figure 4.8. Cards



A user may have one or more credential. Cards can be assigned to users by clicking the + button to pop open the Card dialog. The Administrator or Approver can then issue a credential with the following attributes:

- Card Format
- Card Number
- Status
- Active Date and Time (optional)
- Expire Date and Time (optional)

The Card Format setting indicates which digital structure the card media is using. This is defined per the process documented in the Access Control Settings section of the Settings chapter. The Card Number indicates the displayed value of the credential. This value can often be read into the system using a USB-cabled card reader.

Note

When reading the card number using a reader, there are two modes of operations:

- Normal Mode
- Raw Mode

If the reader is configured to report the raw bits of the credential, which include the card number, facility code, and parity bits, toggle on the Raw Read option. The number read in the Bit Stream field will be different than the number extracted by the system as the Card Number. The extracted value is determined by the card formation definition. If the reader is configured to report just the card number, leave the Raw Read option disabled.

Alternatively, the Card Number can simply be input based upon what is printed on the card.

The Status of the credential indicates whether or not the current credential should be honored at controlled spaces. It is independent of the Active Date and Time and Expiration Date and Time. For a credential to be honored, the Status must be active *and* either the active and expiration dates are not supplied or the current date is greater than the Active Date and Time and less than the Expire Date and Time.

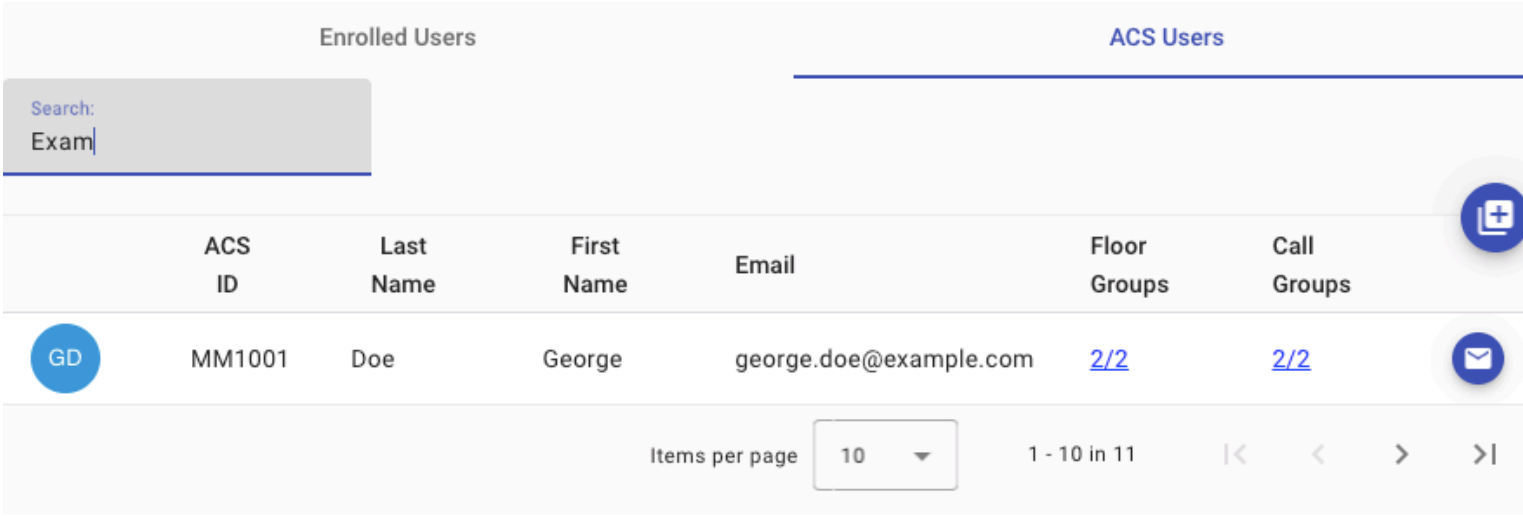
Removing Users

Clicking the “trashcan” command button, upon confirmation, will unenroll a user from the building. Any membership in Floor Access Groups, Call Groups, or Roles will be removed.

Users will still be in LiftOff, can be re-enrolled, can call public floors at LiftOff Mobile™-licensed buildings, and can use LiftOff mobile at other LiftOff Mobile™-licensed properties.

ACS Synchronization

Figure 4.9. ACS Sync



An option for LiftOff Mobile™-licensed buildings is to have user floor group membership and enrollment status synchronized from an access control system. Thus, if the building is also licensed for Access Control Sync™, an ACS Users tab will be displayed. This tab provides visbility into the accesss control system data that has been synchronized from the building's *ACS* to Commander. The interface allows those with Administrator and/or Approver roles to:

- View who from the ACS has been synchronized
- Verify the correctness of the email address
- Visualize which Floor and Call group memberships are managed by the synchronization
- Determine when the last synchronization occured
- Note when the user was last emailed an *Email Code*
- Confirm whether or not the user has entered a valid *Email Code* into the mobile application
- Manually (re)send a linking Email Code

ACS Sync Process

When an ACS sync executes, the synchronization queries the access control system for the following data elements:

- ACS Unique ID
- First Name
- Last Name

- Email Address
- Access Groups

This data is then used by LiftOff to enroll users in a LiftOff Mobile™-licensed building, unenroll inactive users from the building, and enroll the users in the appropriate floor access and call groups.

There are two synchronizes that are configured when an ACS Synchronization is enabled at a building:

- Fast Sync
- Full Sync

The *Fast Sync* occurs within a matter of a minute or two (or faster) when a change is made to a profile in the access control system. The speed with which the synchronization occurs is dependent upon the access control system technology used. Generally, modifying a person's access control system record should result in the Last Sync attriubute being updated in the ACS Users panel within a matter of a minute or two.

The *Full Sync* occurs on a scheduled execution basis, usually once per night. The full synchronization will query all relevant (see below) access control records and ensure the cloud is up-to-date with the latest variants. This provides an automatic recovery mechanism should a service disruption cause a *Fast Sync* to fail.

In either sync scenario, access control records *must* have a valid email address for the record to participate in the synchronization. Upon the first synchronization, LiftOff will email the user a six character alpha-numeric (all upper case letters) *Email Code*, directing the user to enter the code into the mobile application. Once performed, the user's LiftOff account is "linked" to the access control record for the building. The user's LiftOff profile is automatically enrolled and the user is automatically placed into the appropriate floor access and call groups based upon the access groups indicated by the *ACS*. Subsequent synchronizations will similarly automatically enroll/unenroll the user and manage group membership. A "link" icon will appear both in the Enrolled Users panel as well as the ACS Users panel. Hovering over the "link" icon on the ACS Users panel will show the date and time the user entered the *Email Code* into the application.

If the user ignores the *Email Code* message, or if the email address is incorrect in the access control system, the access control record remains unlinked, and the user will not be able to access destinations they would otherwise be able to access unless manually granted access by an Administrator or Approver at the building. After a configurable wait time Email Frequency (default is one day), LiftOff will send a follow-up email asking the user to enter the code. LiftOff will continue to do so until Max Attempts (see Settings) has been exhausted. The default number of attempts is 5.

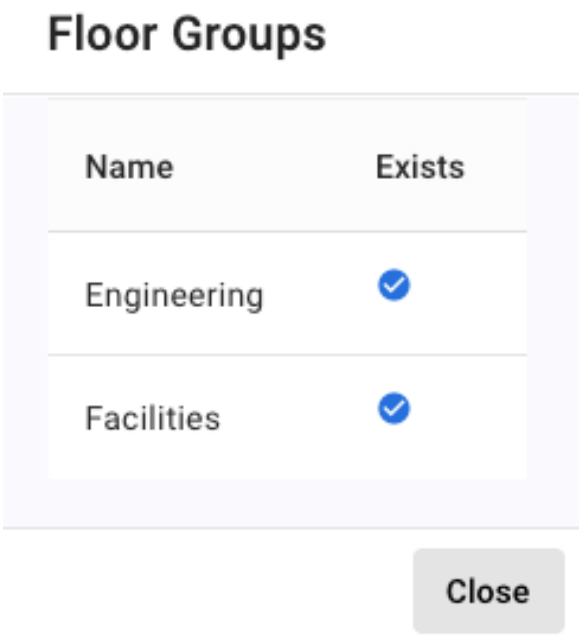
The Administrator or Approver in a building can send an *Email Code* invitation to an access control system user manully by tapping on the Email icon associated with their ACS record. The email defaults to the email address as indiciated by the access control system, but a dfferent email address can be specified. When using the Email button to manually send an email, the system ignores the Settings values that restrict the frequency and maximum number of attempts and will *always* send an email.

Manually sending an email also increments the number of attempts. Exampe: if three had been sent automatically by the system, and a one is sent manually by an administrator, and the maximum number of attempts is 5, then only one more automatic email will be sent.

Floor Access and Call Group Management

Once an access control system record is linked by the user entering the *Email Code*, either at the time they install the application, or by tapping on Settings and the Do you have an email code? link, membership in *matching* floor access and call groups is automatically managed by the synchronization. Users will be *removed* from any group not indicated by the synchronization. The ACS Users panel, for each record synchronized from the access control system, will display a link, which, when tapped, will display the groups sourced from the ACS and whether or not a matching *Floor Access Group* or *Call Group* exists in LiftOff:

Figure 4.10. ACS Groups

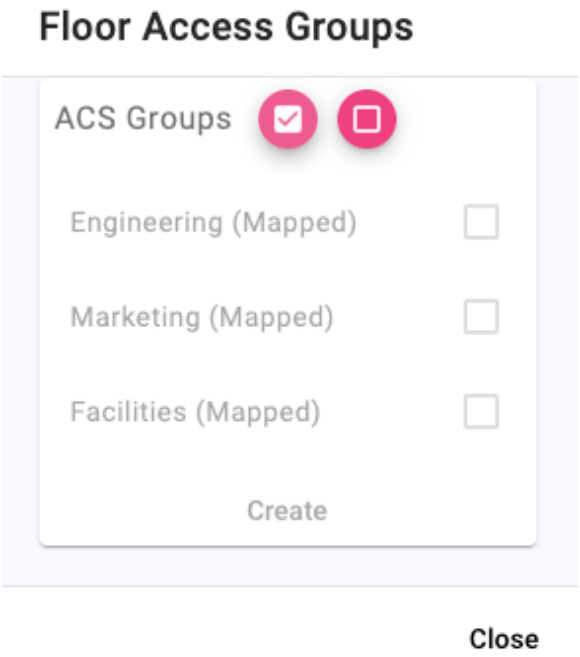


Note

The synchronization does *not* automatically create the corresponding floor access group and/or call groups in LiftOff Commander for a variety of reasons, including the technical limitations imposed by most access control systems. Therefore, the matching group must be created by the Administrator and/or Approver. Once created, access control-linked users will instantaneously be placed into the group(s).

Floor Access Groups may also be created in-bulk by tapping on the Bulk Add button at the upper-right of the external users table. The following dialog is then presented:

Figure 4.11. ACS Sync



The listing shows those access groups that have been surfaced from the access control system and whether or not a corresponding access group has been created. If a corresponding group has not yet been created, ticking the checkbox next to the group or tapping the Select All control followed by clicking the Create command button will result in the automatic creation of the group. Linked users will instantaneously be put into the group. After the groups are created, authorized destinations must still be indicated by the Administrator by editing the Floor Access Group accordingly.

Off-boarding

A linked user is automatically unenrolled from a building and removed from all floor access and call groups if the access control system indicates that the profile is no longer active. If a new identity is issued in the access control system, or if the old profile is re-activated, the user will have to re-enter a new *Email Code* into the mobile application, which will automatically be sent upon the next synchronization.

For additional details on the configurable settings which govern the behavior of the synchronization, see ACS Sync Settings section of the Settings chapter.

Privacy Considerations

Administrators and Approvers in LiftOff Commander have the ability to view a user's first and last name, as well as an obfuscated representation of the user's phone number. In addition, at LiftOff Mobile™, Concert™ and Ascent™-licensed buildings, Administrators may view the elevator transaction history. The transaction history of LiftOff Mobile™ non-enrolled users to public destinations will be anonymized. The transaction history of Commander-enrolled LiftOff Mobile™ and Ascent™ users, as well as access control-hosted Concert™ users, is anonymized subject to regional laws and regulations.

Chapter 5. Floor Access Groups

Overview

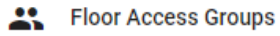
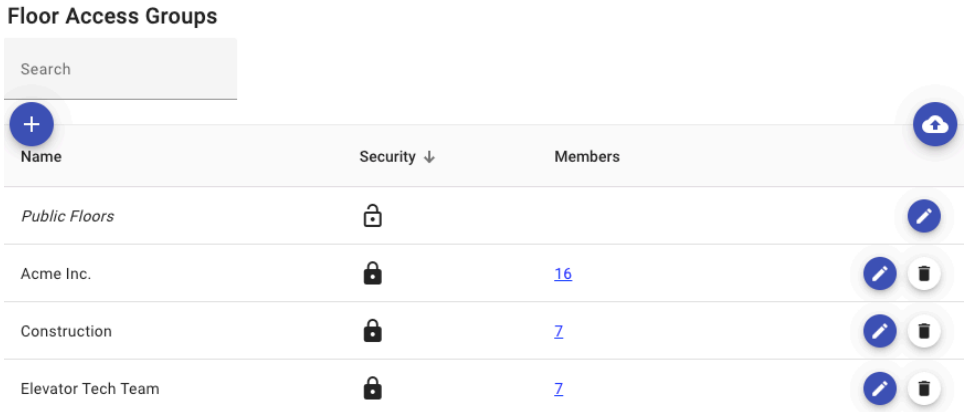


Figure 5.1. Floor Access Groups



Floor Access Groups are used to define which destination floors are accessible, from which source floors, and when. Depending upon the licensed product(s), the function of a Floor Access Group differs:

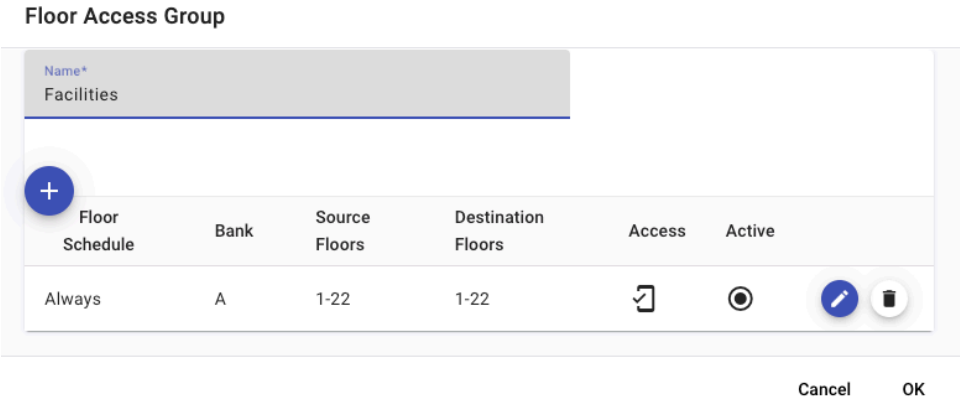
Function

LiftOff Mobile™ and Ascent™	Membership in the group gives the user access to the authorized destinations. For LiftOff Mobile™ users, the authorized destinations are reflected in the LiftOff mobile app. For Ascent™ users, the authorized destinations are reflected at the elevator kiosk.
Access VMS™	Membership in the group gives the user who has also been granted the VisitorHost role the ability to invite visitors to the destinations implied by the Floor Access Group.
Concert™	Concert™ "links" the Floor Access Group to access groups in the access control system of record. Those users who have been granted the corresponding access group in the *ACS* will be authorized to access the destinations indicated by the Floor Access Group.

Floor Access Group Management

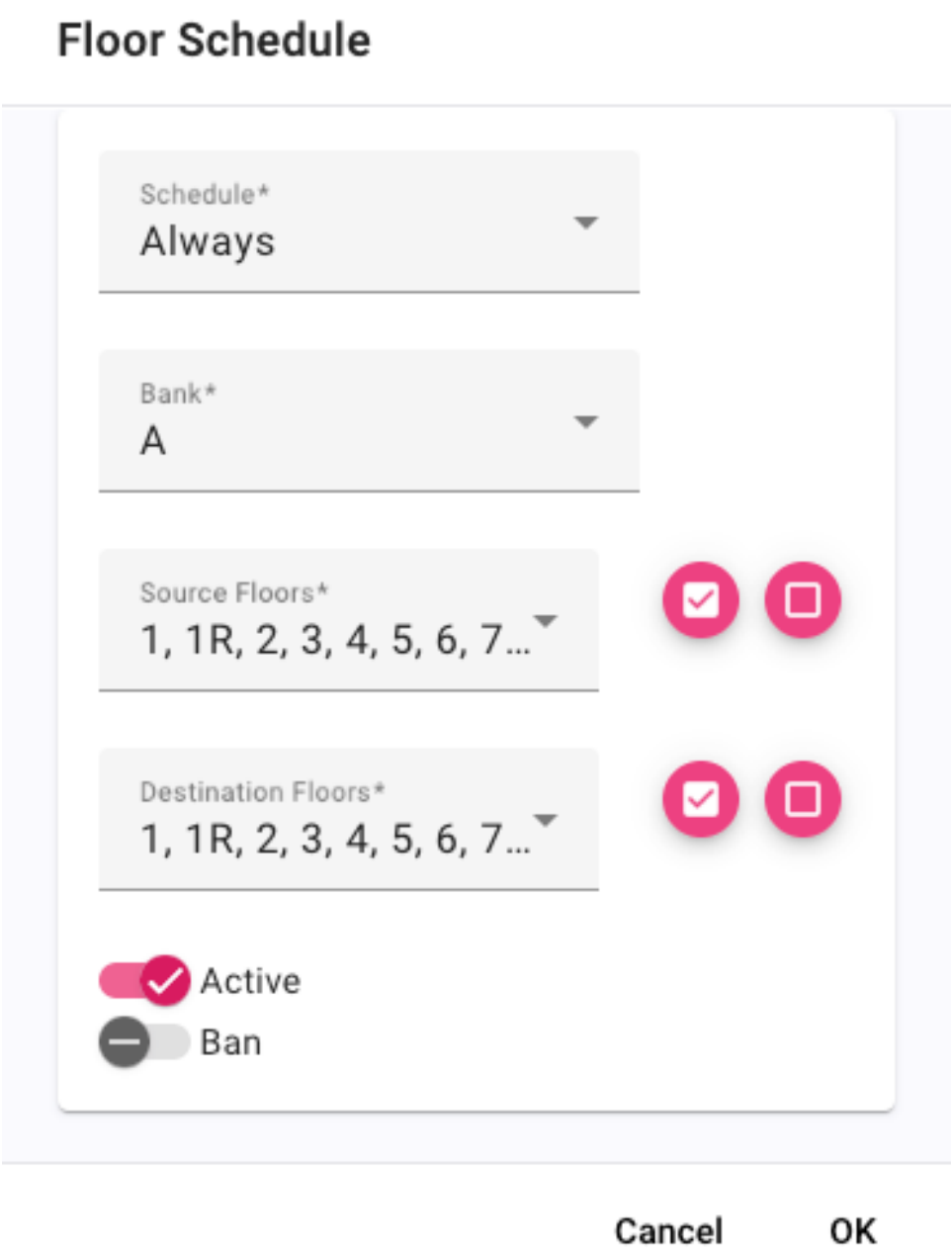
For those buildings licensed for LiftOff Mobile™, Ascent™, or Access VMS™, new floor access groups may be added by property managers by clicking the "+" command button, launching the Floor Access Group dialog. For Concert™ buildings, the property manager can click the "pencil" button next to the access control-synchronized group name to create the Floor Access Group definition:

Figure 5.2. New Floor Access Groups



Once the Floor Access Group is given a name, accessible floors can be added by clicking the "+" command button:

Figure 5.3. Floor Schedule



The Schedule defines when the Floor Schedule is in effect. When a rider is in the elevator lobby outside the schedule, the source and destination floors do not apply.

The Bank, Source Floors, and Destination floors determine which floors will participate in allowing car calling by LiftOff.

The Active toggle is used to determine if the Floor Schedule is in effect. This allows the property to define specific rules that may only be applicable under certain scenarios and enable or disable those floor schedules at will.

The Ban toggle reverses the behavior in LiftOff. If enabled, any Destination floors specified are excluded from being accessible from the Source floors specified during the scheduled window, regardless of what other Floor Schedule rules may say. This can be used, for instance, when construction is taking place and access to a specific destination should be prohibited.

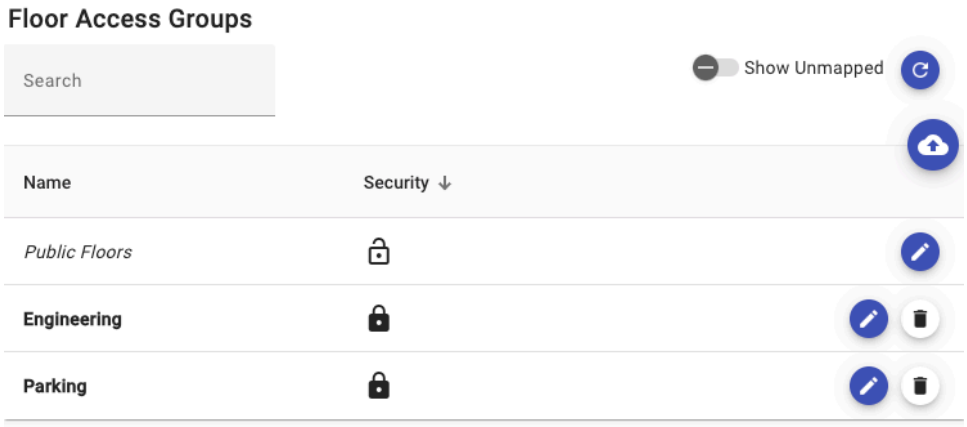
A special Floor Access Group, Public Floors, exists which impacts the user experience accordingly based upon product licensing:

- LiftOff Mobile™: LiftOff app users who are not in any group, or even enrolled in the building, may place a call for the destinations authorized, contingent upon the schedule
- Ascent™ and Concert™: The destinations indicated are reflected as accessible at the elevator kiosks without having to supply a credential
- Access VMS™: Visitor hosts can invite visitors to any of the destinations implied by the Public Floors floor access group definition

A Floor Access Group can be edited by clicking the "pencil" command button. A Floor Access Group can be deleted by clicking the "trashcan" command button. The impact of editing or deleting a Floor Access Group is contingent on the products licensed.

If the building is a Concert™-licensed building, editing an access-control synchronized floor access group establishes the "link" between the rules of destination control defined in Commander and the access group assigned to users in the *ACS*. The Floor Access Group will then be displayed in a *bold* font, indicating that the "link" has been established. Deleting the Floor Access Group breaks the "link". Unlinked access groups synchronized from the access control system are displayed in light grey and can filtered out by toggling off the Show Unmapped switch:

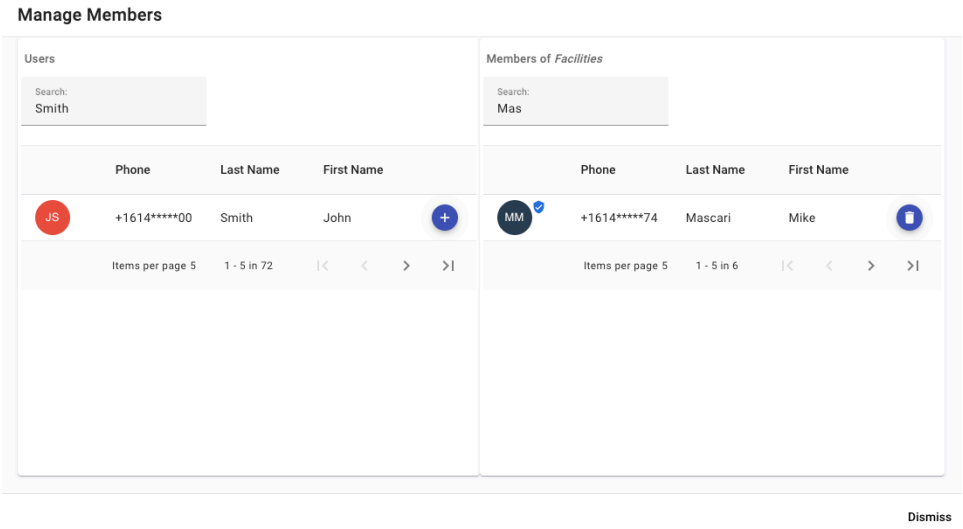
Figure 5.4. Concert™ Floor Access Groups



When the Refresh button is tapped, Concert™ will execute a refresh to (re)synchronize the access groups from the access control system to Commander.

For LiftOff Mobile™, Ascent™, and Access VMS™-licensed buildings, membership in a Floor Access Group can be managed either by directly accessing the user's profile, or by clicking the Members link. Clicking the Members link launches the Floor Access Group Membership dialog:

Figure 5.5. Manage Members

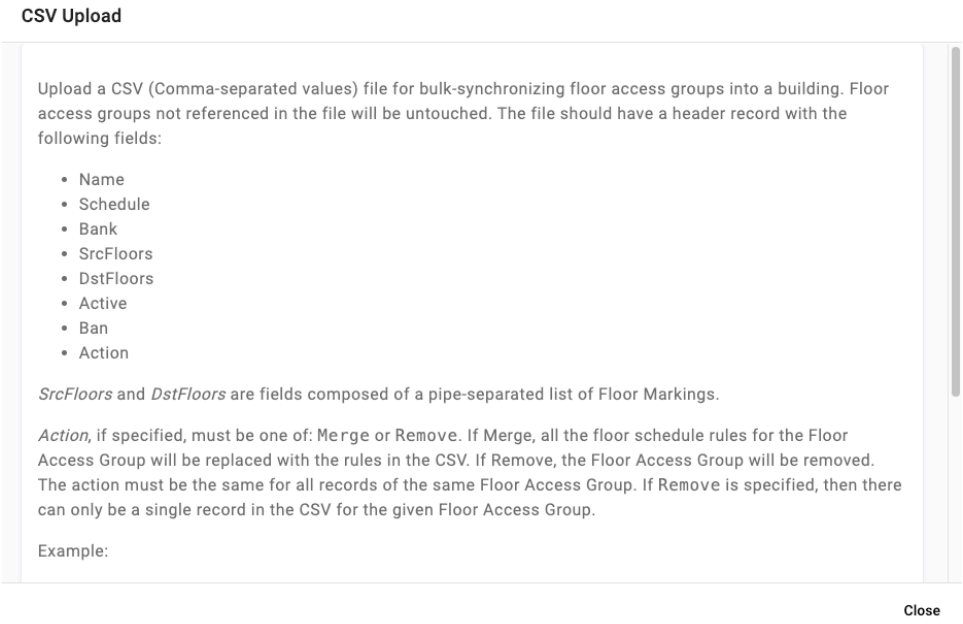


Membership can be added by clicking the "+" command button in the Users pane. Membership can be removed by clicking the "trashcan" command button in the Members pane. Changes in membership take effect immediately.

Floor Access Group CSV Upload

Commander supports loading floor access group definitions en masse via the upload of a *CSV* file. After clicking the CSV Upload command button, Commander will display the upload dialog:

Figure 5.6. Floor Access Groups Upload



Like the upload of users via *CSV*, the upload of floor access groups must confirm to the file format as indicated in the dialog. The easiest approach towards creating an an intial *CSV* file is to copy-paste the example in the dialog and modify according to one's needs. The fields in the CSV are:

- **Name.** Indicates the floor access group to add, modify, or remove, contingent upon the Action value. See below for details.
- **Schedule.** Indicates the schedule for the floor access group rule. The schedule must already exist for the record in the upload to be successfully processed.
- **Bank.** Indicates the elevator bank for the floor access group rule. The elevator bank must already exist for the record in the upload to be successfully processed.
- **SrcFloors.** Indicates the source floors from which the user may place a call. The floor values must match the Floor Marking values as specified by the deployer in the Floors component of the car group. Unrecognized floors will emit an error and will be ignored by the upload, whilst valid floors will still be proceesed. Note that two records in the *CSV* with the same schedule, bank, and source floors is not currently supported.
- **DstFloors.** Indicates the destination floors from which the user may place a call. The floor values must match the Floor Marking values as specified by the deployer in the Floors component of the car group. Unrecognized floors will emit an error and will be ignored by the upload, whilst valid floors will still be proceesed.

- **Active.** Indicates whether the floor access rule is in effect. The value must be either `true` or `false`. If `false`, the rule will be created for the associated floor access group, but will not be in effect until toggled on by the administrator.

- **Active.** Indicates whether the floor access rule is in effect. The value must be either `true` or `false`. If `false`, the rule will be created for the associated floor access group, but will not be in effect until toggled on by the administrator.

- **Ban.** Indicates whether the floor access rule is a *Ban* rule. The value must be either `true` or `false`.

- **Action.** Defines what the system should do with the record. Valid values are `Merge` or `Remove`. The Action value must be consistent across all records for the same floor access group (i.e.: you cannot indicate to remove a floor access group while also indicating records to merge). If the Action value is `Merge`, the existing definition of the floor access group is replaced with the set of rules in the *CSV* file. Existing membership in the group is preserved. If the floor access group does not already exist, a new one is created, and any relevant ACS users (i.e.: those who have been synchronized and verified) are automatically placed within the floor access group. If the Action is `Remove`, the floor access group is removed from the building.

All changes to floor access group definitions made by the *CSV* upload go into effect immediately.

Note

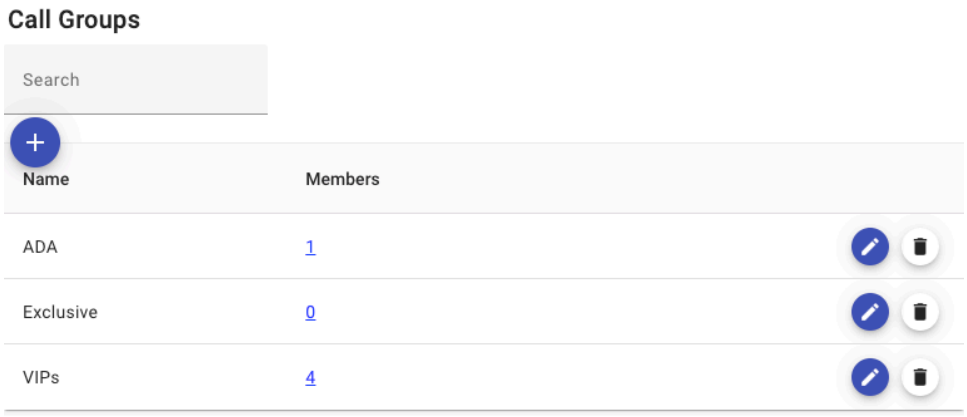
For Concert™-licensed buildings, Floor Access Group definitions in the CSV that do not match the access groups synchronized from the access control system will be ignored.

Chapter 6. Call Groups

Call Groups

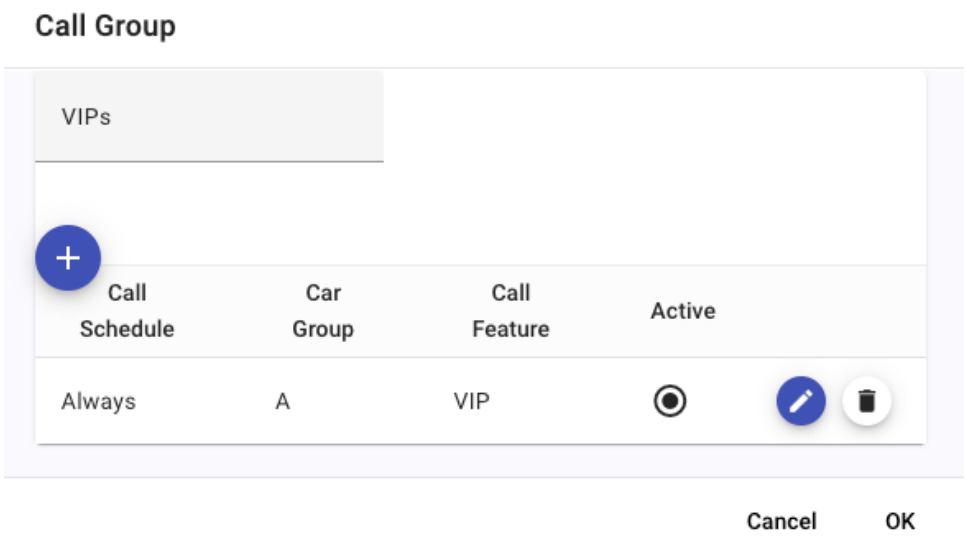
Like Floor Access Groups, Call Groups are used to organize enrolled LiftOff Mobile™, and Ascent™ users into groups that have certain privileges. For Call Groups, these privileges are special features that are enabled when the rider calls an elevator, either using the LiftOff mobile app or at the presentation of an Ascent™ credential. Membership is managed in a similar way as with Floor Access Groups, and management of the definition of Call Groups occurs in the Call Groups panel:

Figure 6.1. Call Groups



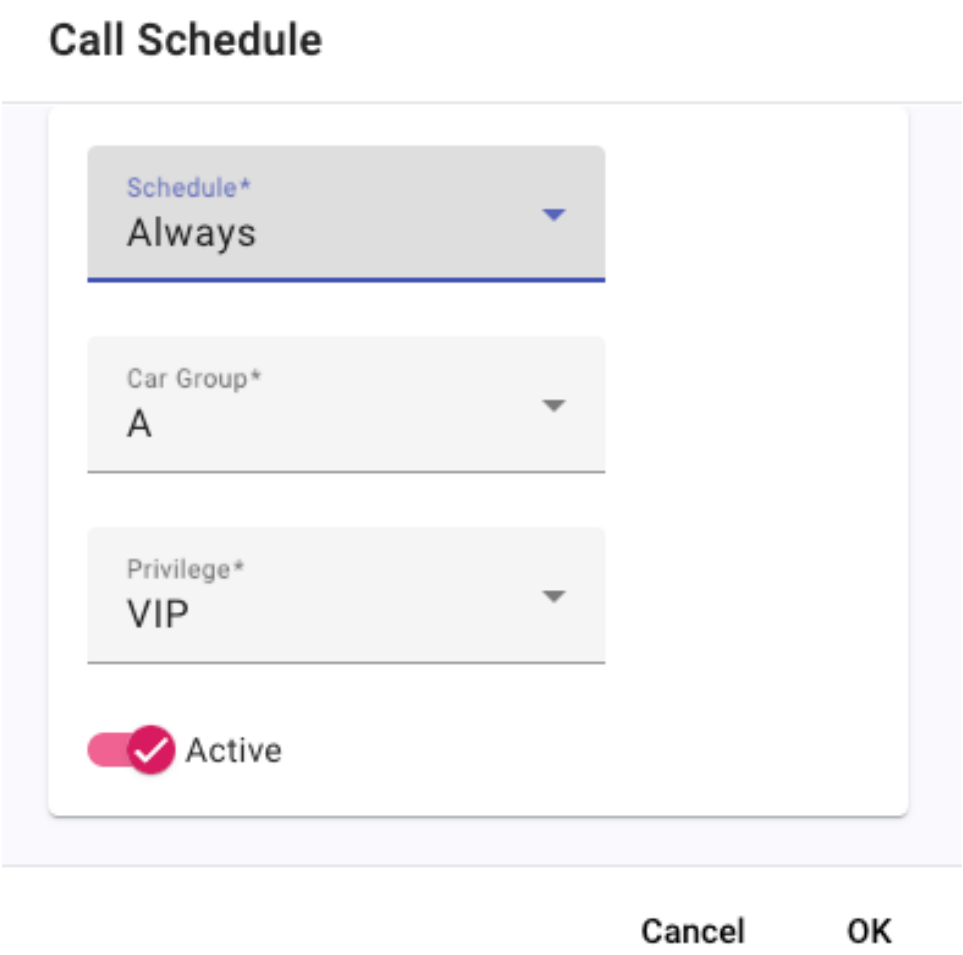
Clicking the "+" command button to create a new Call Group launches the Call Group Dialog:

Figure 6.2. New Call Group



The Name field of the Call Group is required. Once supplied, Call Schedules can be added that determine when the call feature is in effect for members of the group:

Figure 6.3. Call Group Schedule



The Schedule attribute determines when the Call Schedule applies, the Car Group determines the applicable Car Group, and the Privilege attribute determines what special feature will be enabled when group members place a call for an elevator. Examples of Privilege values include VIP, ADA, Housekeeping, etc. The set of possible Privilege options are determined by who the elevator manufacturer is and what has been enabled by the elevator mechanic in the elevator controller.

In addition to the above options, the Active toggle determines whether the Call Schedule is in effect.

Once defined, Call Schedules can be edited and removed from Call Groups using the "pencil" command buttons and "trashcan" command buttons respectively.

Chapter 7. Roles

Roles determine the privileges of users within the LiftOff Commander portal. Most LiftOff Mobile™ and Ascent™ users will never be granted a role in any building. The entire Concert™ user population should be composed of Administrators, Approvers, Deployers, or Support. Like Concert™, the Access VMS™ user population is limited to those individuals that need access to the portal (e.g.: Visitor hosts, Security). The defined roles are:

Approver – has access to approve requests for access, receives push notifications of requests, has authority to add and remove users from Floor Access Groups and Call Groups. Can grant Approver to other users, but no other role. An Approver can also change the schedule on which a Floor Access Group or Call Group operates as well define new Floor Access Groups and Call Groups.

Administrator – has the same privileges as Approver, but does not receive request for access push notifications unless he or she is also granted the Approver role. Also has access to Schedules, Settings, and Reports. An Administrator can grant Administrator or Approver role to building users.

Deployer – has specific privileges for programming beacons and defining elevator banks including defining which special privileges are available in the building based upon elevator controller software capabilities. A Deployer can only grant Deployer role to building users.

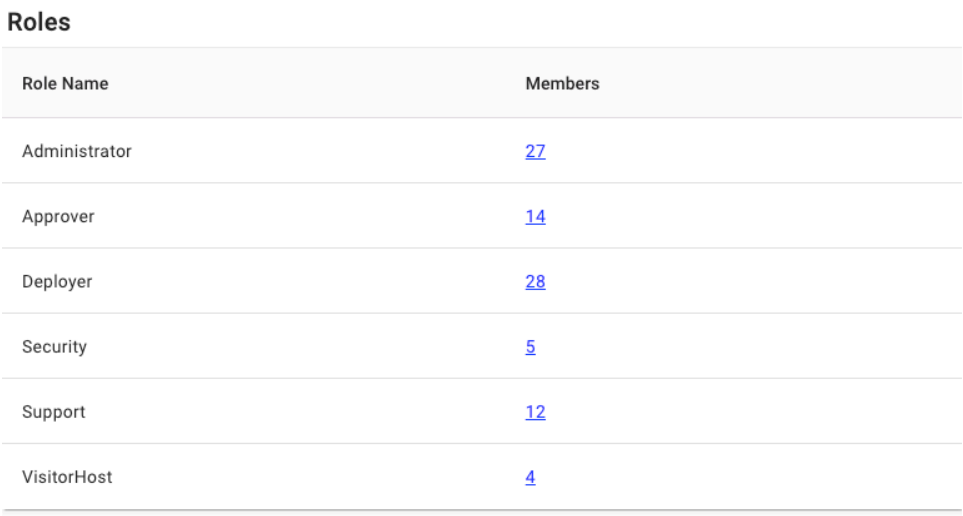
Support – has all privileges and is a braXos employee. Users with the support role can grant any role to any building user.

VisitorHost – for Access VMS™ and Lightning VMS™-licensed buildings only. This role grants the ability of the user to log into Commander and invite visitors to the building to floors associated with the user's Floor Access Group membership.

Security – for Access VMS™ and Lightning VMS™-licensed buildings only. This role grants the ability of the user to log into Commander and perform visitor check-in and manual (re)sending of temporary visitor credentials.

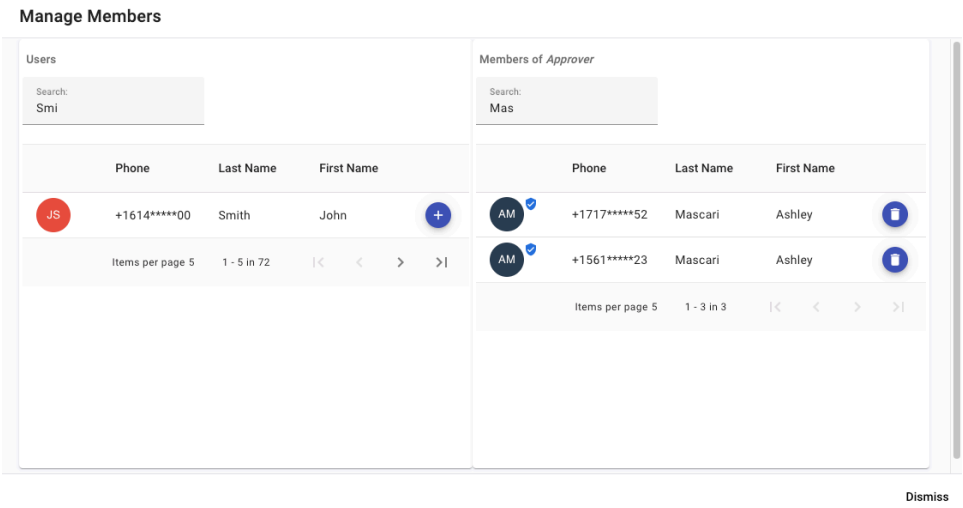
To manage role membership, display the Roles panel by clicking the Roles side navigation item:

Figure 7.1. Roles



Unlike Floor Access Groups and Call Groups, Roles are built-in. Membership, however, is managed in a similar way. To change Role membership, a user's profile may be displayed from the User's panel, or, by clicking the Members link in the Roles panel:

Figure 7.2. Manage Role Members



Like membership elsewhere, a user can be granted the associated Role by clicking the "+" command button in the Users pane, while having a role revoked by clicking the "trashcan" in the Members pane of the Role. Changes to Role membership apply immediately.

Note

The current roles assigned to the currently authenticated LiftOff Commander user is displayed by clicking on the profile Avatar in the upper-right of the LiftOff Commander interface.

Chapter 8. Schedules

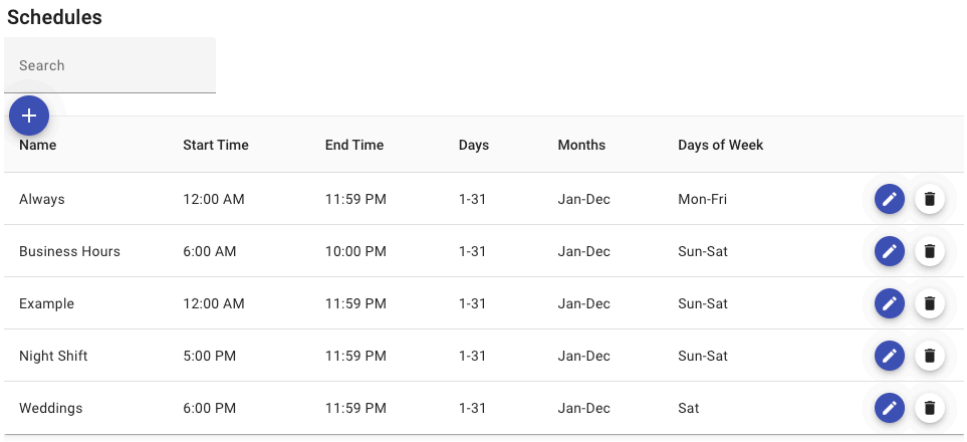
Schedules

Schedules are used to define a repeating segment of time that constrains the ability of a user or visitor from either calling a car through Floor Access Group membership or calling a car with special privileges (e.g.: VIP) through membership in a Call Group.

The Always schedule is a predefined schedule that, when used with a Floor Schedule or Call Schedule is always in effect.

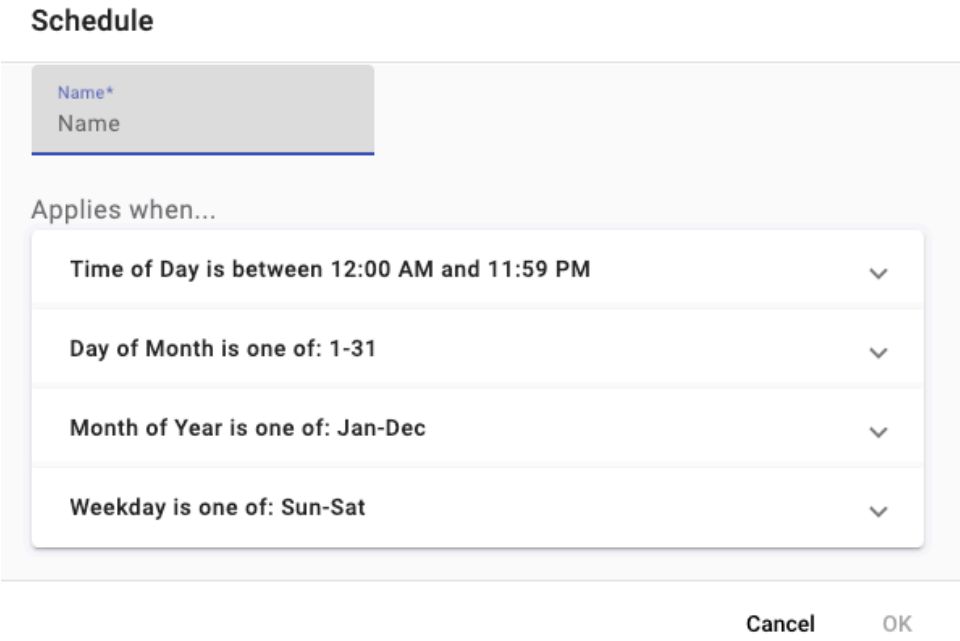
The Schedules panel is used to manage schedules:

Figure 8.1. Schedules



To define additional schedules, click the "+" command button, which will launch the Schedule Dialog:

Figure 8.2. New Schedule



The Name field of the Schedule is required. In addition to the Name, the Schedule has a series of criteria to determine whether or not it is in effect. The criteria are:

- Time of Day: A range of when the Schedule begins and when it ends. Note that the Time of Day cannot "wrap" around midnight – the start time must be earlier than the end time. If a window of time must wrap around midnight, two Schedules must be created.
- Day(s) of the Month
- Month(s) of the Year
- Day(s) of the Week

Once the criteria has been specified, clicking OK creates or updates the Schedule object.

Schedules can be added by clicking the "pencil" command button. Once the edit has completed, the Schedule is immediately put into effect.

Schedules can also be deleted by clicking the "trashcan" command button, and confirming the Schedule deletion.

Note

Any Floor Schedule or Call Schedule that references the Schedule in question will also be deleted.

Chapter 9. ACS Systems

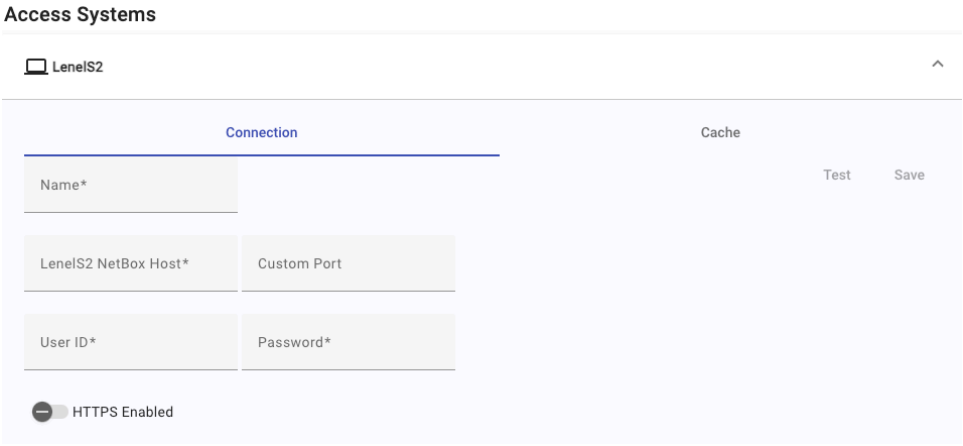

ACS Systems

For Concert™-licensed buildings an ACS Systems panel is available that allows the building Administrator or Deployer to configure and test connectivity to the access control system that is being integrated with the elevators. The expectation is that the *HGA* (Hybrid Gateway Appliance) has been networked to both the access control system and the elevator system. Irrespective of the access control system in use, the Administrator or Deployer may:

- Configure access control connectivity
- Test access control connectivity by the HGA
- View the status of the HGA cardholder cache
- Force a fast cache refresh
- Force a full cache refresh

LenelS2 Connectivity

Figure 9.1. LenelS2 Connectivity Settings



For buildings utilizing LenelS2™ technology, Commander displays a connectivity configuration panel that requests the following data elements for establishing connectivity to LenelS2™:

Name

The Name field is used to uniquely identify this access control system from potentially other access systems used at the property. The name can be any value meaningful to the property.

Hostname

The Host field is used to indicate the DNS-resolvable hostname or IP address of the LenelS2™ NetBox controller. If a hostname is specified, it must be resolvable by the *HGA*, typically by having the *HGA* acquire its IP address and local DNS resolver information via DHCP and ensuring that the NetBox's hostname is registered with the building's DNS. If an IP address is specified, no DNS resolution is required. In either case, the *HGA* needs to be able to reach the NetBox over the IP network.

Custom Port

If the NetBox Web API is running behind a reverse proxy, the port may not be on the standard port of either 80 (for http) or 443 (for https). If so, a custom port number may be indicated.

User ID and Password

For the *HGA* to interact with the LenelS2™ NetBox using its Web API, an account needs to be created on the NetBox that has *System Setup* privileges. In addition, the NetBox needs to have the following set on the Data Integration tab of the Network Controller panel in the Configuration Site Settings area of the LenelS2™ NetBox:

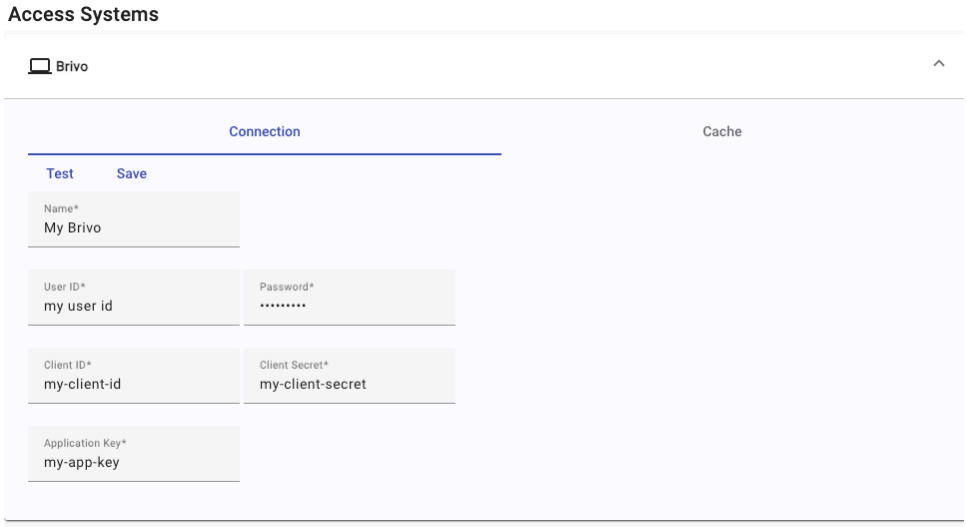
- Enabled
- Use Authentication
- Use login username/password for authentication

HTTPS Enabled

If an *SSL* certificate has been deployed to the LenelS2™ NetBox, communications to the NetBox Web API can be performed over https. Toggling this control on enables *SSL* functionality.

Brivo Connectivity

Figure 9.2. Brivo Connectivity Settings



For buildings utilizing Brivo™ technology, Commander displays a connectivity configuration panel that requests the following data elements for establishing connectivity to Brivo™:

Name

The Name field is used to uniquely identify this access control system from potentially other access systems used at the property. The name can be any value meaningful to the property.

User ID and Password

The User ID and Password fields are used to indicate the credentials that the *HGA* will use to authenticate to the Brivo™ cloud API. These credentials should be created in Brivo™ by the access control system administator or integrator. The user identity created should have at least *`Senior Level Administrator`* privileges.

Client ID and Client Secret

To enable the *HGA*'s ability to communicate to the Brivo™ cloud API, the Brivo™ administrator or integrator needs to create an "Application" in Brivo™:

1. Login to OnAir
2. Navigate to Setup/AccountAccount Settings
3. Click on the Application Management tab
4. Select *`Password`* authentication
5. Save and click Application Details to acquire the `Client ID` and `Client Secret`

Application ID

The *`Application ID`* can be acquired from braXos engineering after Brivo Inc. has added the site's Brivo™ instance to the braXos set of application keys. To acquire

the ID, please reach out to <support@braxos.com> or your braXos Customer Care representative.

Connectivity Test

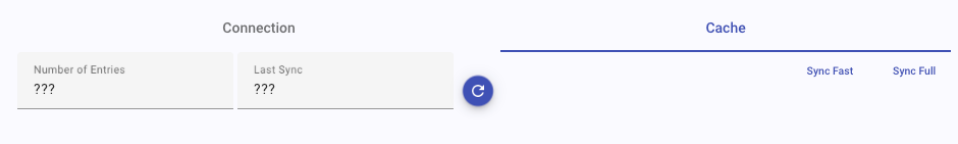
Once the access control specific information has been entered, connectivity by the *HGA* to the access control system can be tested by clicking the Test button on the connectivity panel. This will automatically save the current state of the connectivity confirmation and then perform a connectivity test to the access control system. If successful, Commander will indicate as such, else the details of the connectivity error will be displayed.

Typical errors:

- *Networking* - Can the *HGA* reach the API of the access system over an IP network? Are the APIs enabled on the access control system?
- *Authentication* - Are the credentials correct?
- *Authorization* - Is the account used to authenticate authorized to invoke the APIs?

Cache Management

Figure 9.3. Cache Management



The on-premise *HGA* acts as a security panel by caching credential information from the access control system. This allows the device to interact with the elevator system even when communications fails between the *HGA* and the access control system. In addition, it ensures fast, low-latency interactions between itself and the elevator controller(s).

Credentials from the access control system are automatically refreshed in both "fast" and "full" modes. In "fast" mode, the *HGA* uses the capabilties of the access control system API to acquire recently changed user and credential information. This is usually either instantenous, or within a minute or two contingent upon the ACS's API capabilities. In "full" mode, the *HGA* performs a full synchronization of all cardholder information from the access control system. Since this is a time and compute-intenstive process, this is typically scheduled for execution once per night.

Administrators and Deployers can view the state of the cache -- how many records have been synchronized by the access control system as well as when the last record(s) have been synchronized by tapping the Cache tab of the Access Systems panel. If no synchronization has yet occurred, ??? is displayed for both values. By tapping the Sync Fast button, the *HGA* will execute a "fast" synchronization and update the cache information accordingly.

Note

If no records have been recently modified in the access control system, the Last Sync attribute will not be updated.

By clicking the Sync Full button, the *HGA* will execute a "full" synchronization, ensuring that the *HGA*'s internal cache matches the full population of cardholders in the access system.

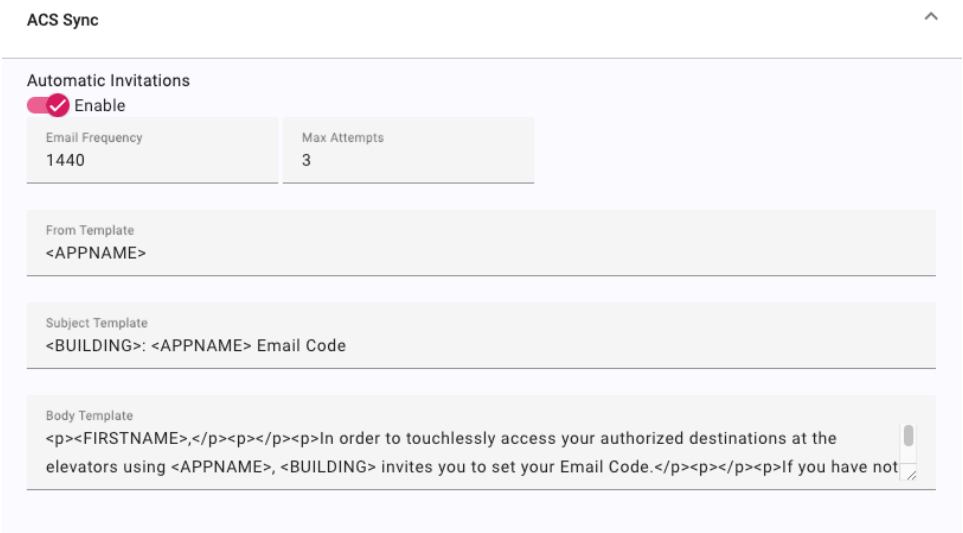
Chapter 10. Settings

Settings are used to control the functionality of LiftOff. Depending upon the licensed products, various settings will be available:

- ACS Sync: Access Control Sync™
- Call Limits: LiftOff Mobile™
- AutoLift Settings: LiftOff Mobile™
- QuickLift Push: LiftOff Mobile™
- Visitor Management: Access VMS™ or Lightning VMS™
- Access Control: Ascent™ or Concert™

ACS Sync Settings

Figure 10.1. ACS Sync Settings



The ACS Sync settings section allows the property Administrator to tune settings which govern how access control system data is managed by LiftOff. These parameters are:

- Automatic Invitations

  When this setting is enabled, an *Email Code* will be sent to the user on the basis of the email address in the access control system upon synchronization. If disabled, no email is sent, unless the Administrator or Approver taps the Email icon on the ACS Users panel.

- Email Frequency

  This value, measured in *minutes*, determines how long LiftOff should give the user to enter the *Email Code* into the mobile application before sending a follow-up email. The default is one day.

- Max Attempts

  This value determines the number of times LiftOff will automatically send an *Email Code* to an access control system user's email address before giving up. The default is 5.

- From, Subject, and Body

  These three input fields indicate the content that is emailed to the user when the *Email Code* is sent. The From and Subject fields send the content as plaintext, whereas the Body field sends the content as *HTML*.

Before sending, LiftOff substitutes the following variables with their corresponding values. These variables can be entered anywhere within the content of the From, Subject, or Body fields, enclosed by angle brackets:

- `<APPNAME>`. Used to indicate the mobile application name (e.g.: LiftOff).

- `<BUILDING>`. Used to indicate the name of the building.
- `<FIRSTNAME>`. Used to indicate the first name of the user.
- `<CODE>`. Used to indicate the *Email Code* the user should enter.

LiftOff Mobile™ Settings

Call Limits allows the property to place a maximum daily LiftOff Mobile™ car call quota on users. When enabled, the Administrator is prompted for the number of calls per calendar day. If a LiftOff Mobile™ user attempts to exceed the number of calls, an error message is displayed notifying the user that he or she has exceeded the daily call limit.

AutoLift Settings allows the Administrator to define from which floors an AutoLift may execute. Some properties utilize turnstiles in the lobby, performing automatic home floor calls on behalf of the user. In such cases, the AutoLift Setting may be utilized to prohibit its use by users from the turnstile floor.

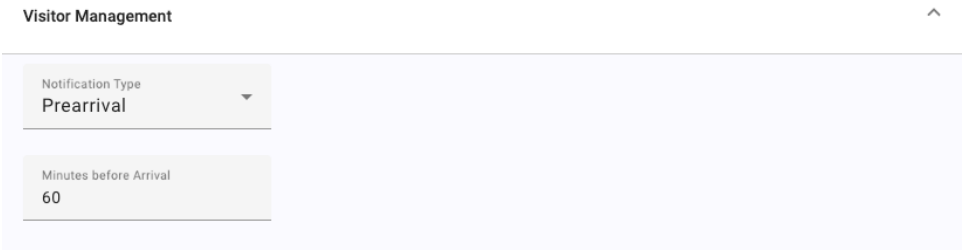
QuickLift Push allows the Administrator to determine whether or not users will receive a push notification when they approach an elevator bank. When this toggle is enabled, as users approach the elevators, they will receive a notification that allows them to quickly select a destination. At maximum, six destinations are displayed, including:

- The Lobby floor, if the user is currently not on the lobby
- The user's favorite floor
- The user's most recently called destinations
- The building's most popular destinations

When the QuickLift Push option is toggled off, users do not receive the notification.

Visitor Management

Figure 10.2. Visitor Management Settings

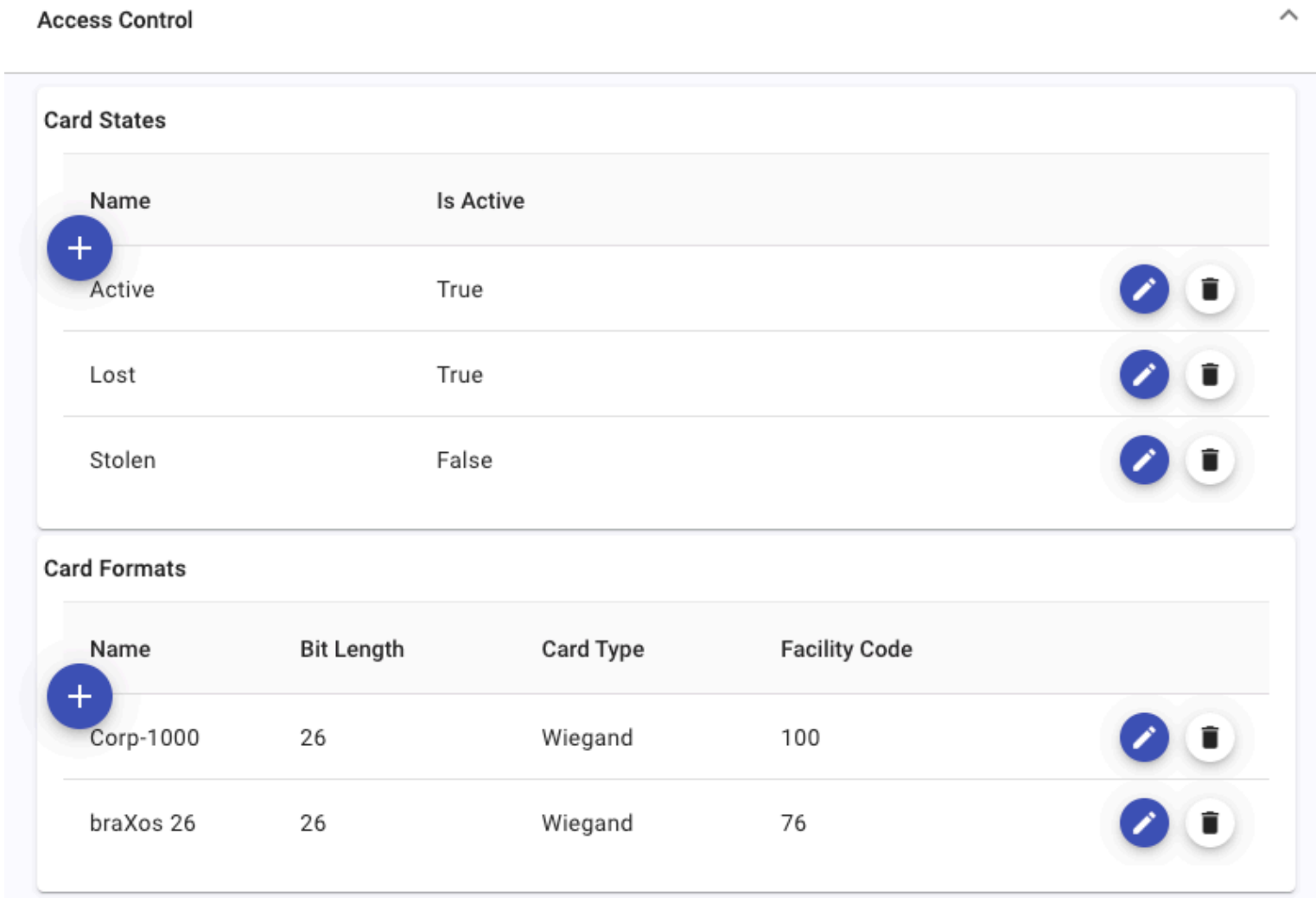


The Visitor Management settings panel allows buildings licensed with either Access VMS™ or Lightning VMS™ to indicate how and when invitations to visitors will be sent. When a visitor is invited to the building, the visitor host supplies the visitor's email or phone number. A credential is then sent to the visitor. For Access VMS™, the credential is a QR code of a credential that is provisioned into the building's access control system. For Lightning VMS™, the credential is a temporary code via a *URL*, that, when tapped in the elevator lobby, allows the visitor to place a LiftOff Mobile™ call to their authorized destination.

The Notification Type control indicates whether LiftOff ought to send the credential daily, before the expected arrival time, or not at all (i.e.: "Off"). If either Daily or Prearrival is specified, then the time at which the credential is sent is also configurable.

Access Control

Figure 10.3. Access Control Settings



The Access Control settings panel allows the Administrator for an Ascent™ or Concert™-licened building to manage credentialing options.

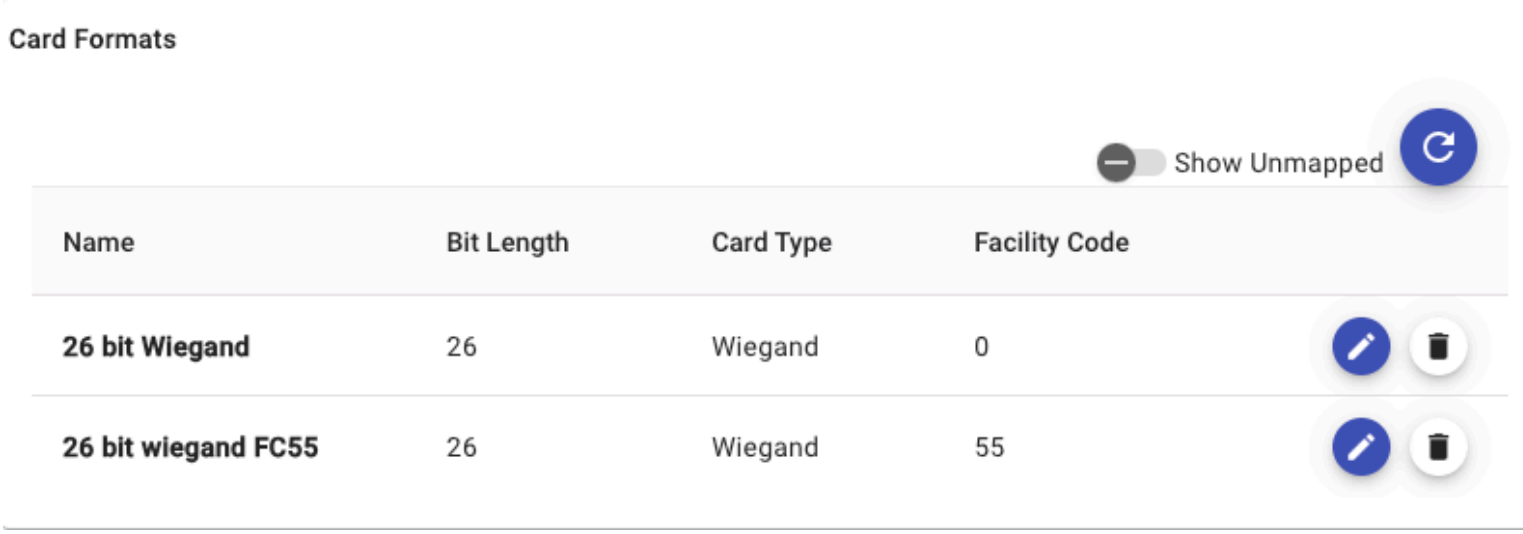
For Ascent™-licensed buildings, the Card States user interface allows the Administrator to define the set of card status values that a credential may be in. When defining the state, the Administrator will also indicate whether a credential in that state ought to be considered active or not. Example states include `Lost`, `Stolen`, `Temporary`.

For Ascent™ and Concert™-licensed buildings, the Card Formats user interface allows the Administrator to define the set of card format values that a credential can use. These definitions allow for the proper interpretation of the raw card data as it is presented by users at the elevator kiosks. The name is then referenced when a credential is issued. The characteristics of a card format are dependent upon the card type. Typical Wiegand credentials are composed of a facility code and a card

number. The facility code is a constant value across a set of card stock issued to card holders, while the card number changes with each credential. The card stock vendor or security integrator should be able to supply the Administrator with the appropriate values to input when defining the card format to the system.

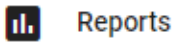
Like Floor Access Groups, in a Concert™-licensed building, Card Formats are "linked" to the card formats specified in the access control system by name. A "linked" card format will be displayed in *bold*, whereas an "unlinked" card format will be displayed in light grey. For a credential to be used successfully at the kiosk, the card format *must* be linked and its definition *must* match the definition in the access control system:

Figure 10.4. Concert™ Card Formats



When the Refresh button is tapped, Concert™ will (re)synchronize the card formats from the access control system to LiftOff Commander so that they may be linked.

Chapter 11. Reports

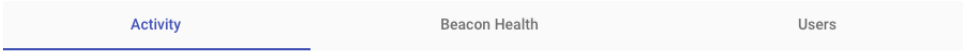


Property managers with the Administrator role may view reports. There are currently three reports available for viewing:

- Activity
- Beacon Health
- Users

By clicking the appropriate Report Tab, the associated Report panel is displayed:

Figure 11.1. Reports Bar



The report tabs available are contingent upon the licensed products:

- Activity: LiftOff Mobile™, Ascent™, Concert™
- Beacon Health: LiftOff Mobile™
- Users: LiftOff Mobile™, Ascent™ Concert™, Access VMS™

Activity Report

The Activity Report shows recent elevator car calling activity. For LiftOff Mobile™-licensed buildings, the activity is composed of elevator calls placed via the LiftOff mobile app, either by a LiftOff Mobile™ user or by a Lightning VMS™ visitor. For Ascent™ and Concert™-licensed buildings, the activity is authorized credentialed user activity at the elevator kiosks. The activity can be filtered on the basis of:

- Elevator Bank
- Start Date
- End Date
- User Search

The report shows the details of the elevator calling transaction, including:

- When the call was placed
- Who placed the call
- Elevator Bank
- Source Floor
- Destination Floor
- Car Allocated
- Whether or not the call was AutoLift
- User Type

Note

Deployers can view Activity reports, but the name of the rider is anonymized. Similarly, if a LiftOff Mobile™ rider is not enrolled in the building, but is accessing a public floor, the rider's personally identifiable information is anonymized. The level of anonymization is based upon a building's configuration which is determined by local laws and regulations.

The User Type describes the type of user that placed the call. This value can be one of the following, contingent upon what licenses the property has purchased:

- Mobile User (LiftOff Mobile™)
- Cardholder (Ascent™)
- Non-User Cardholder (Concert™)
- Visitor (Lightning VMS™)

The `Mobile User` is the mobile application user who uses their mobile device to place a call. The `Cardholder` is an enrolled user who authenticated to a kiosk using a Commander-managed credential. The `Non-User Cardholder` is an external user (i.e.: managed by an access control system) who authenticated to a kiosk using a credential. The `Visitor` is an invitee of a visitor host at a Lightning VMS™-licensed

building who placed a call for an elevator using Apple AppClip™ or Google Instant App™ technology.

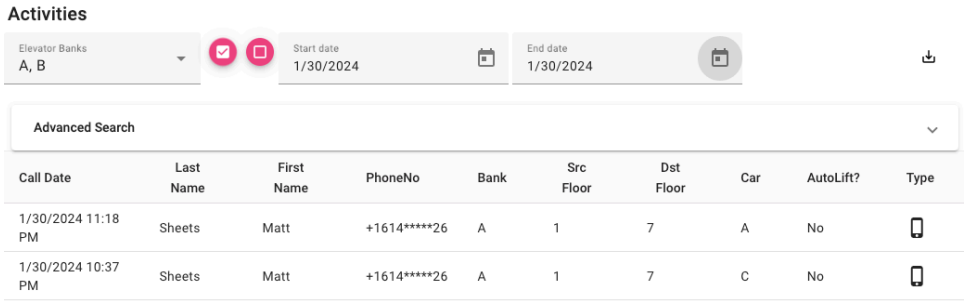
The report may be exported either as an XLS file or a CSV by clicking the download command menu and choosing the desired format:

Figure 11.2. Report Download

An example Activity Report follows:

Example 11.1. Activity Report

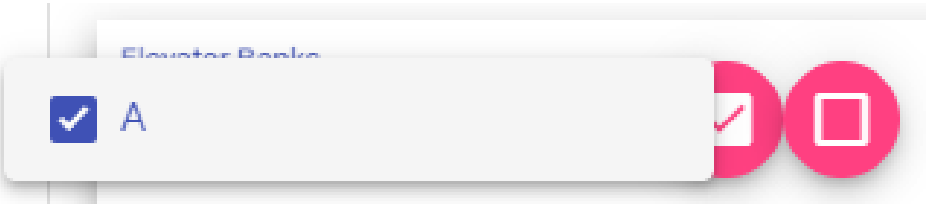
Figure 11.3. Activity Report



Beacon Health Report

For buildings licensed for LiftOff Mobile™, the Beacon Health Report details the current state of beacons deployed at the property. The report can be filtered by Elevator Bank:

Figure 11.4. Elevator Bank



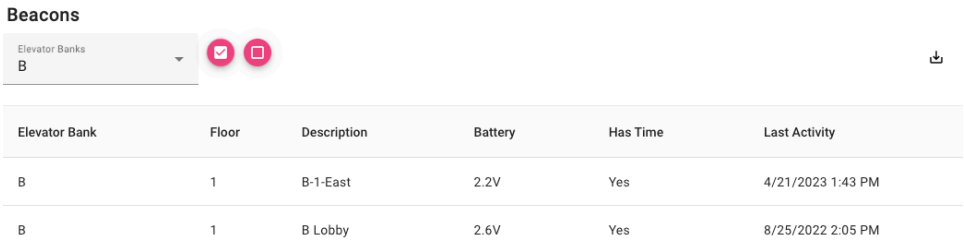
The report details each beacon's:

- Elevator Bank
- Floor
- Description
- Battery Life
- The last activity with the beacon

An example of a Beacon Health Report follows:

Example 11.2. Beacon Health Report

Figure 11.5. Beacon Health Report



Elevator Bank	Floor	Description	Battery	Has Time	Last Activity
B	1	B-1-East	2.2V	Yes	4/21/2023 1:43 PM
B	1	B Lobby	2.6V	Yes	8/25/2022 2:05 PM

Users Report

The Users Report provides a record-per-user perspective, suitable for export by means of the XLS and CSV export utility.

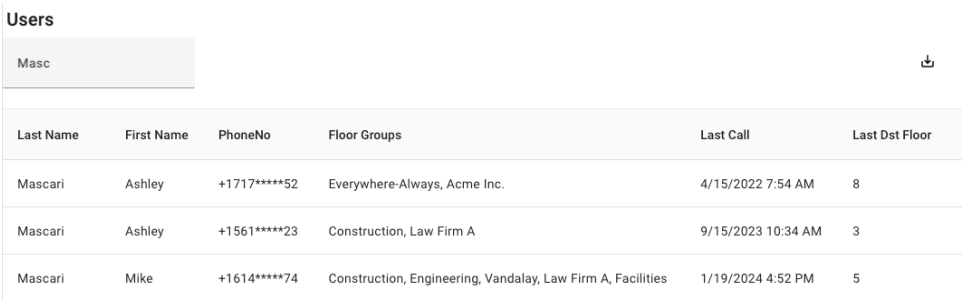
The report details:

- Last Name
- First Name
- Obfuscated Phone Number
- Floor Group Membership
- Last Call Made by the User
- Last Destination Floor Called

An example of a Users Report follows:

Example 11.3. Users Report

Figure 11.6. Users Report



Last Name	First Name	PhoneNo	Floor Groups	Last Call	Last Dst Floor
Mascari	Ashley	+1717*****52	Everywhere-Always, Acme Inc.	4/15/2022 7:54 AM	8
Mascari	Ashley	+1561*****23	Construction, Law Firm A	9/15/2023 10:34 AM	3
Mascari	Mike	+1614*****74	Construction, Engineering, Vandalay, Law Firm A, Facilities	1/19/2024 4:52 PM	5

Like the Activity Report and Beacon Health Report, data may be exported using the export tool.