Smartalock Administration Guide (Full)
Version 2.0
August 2019

1.0 Introduction

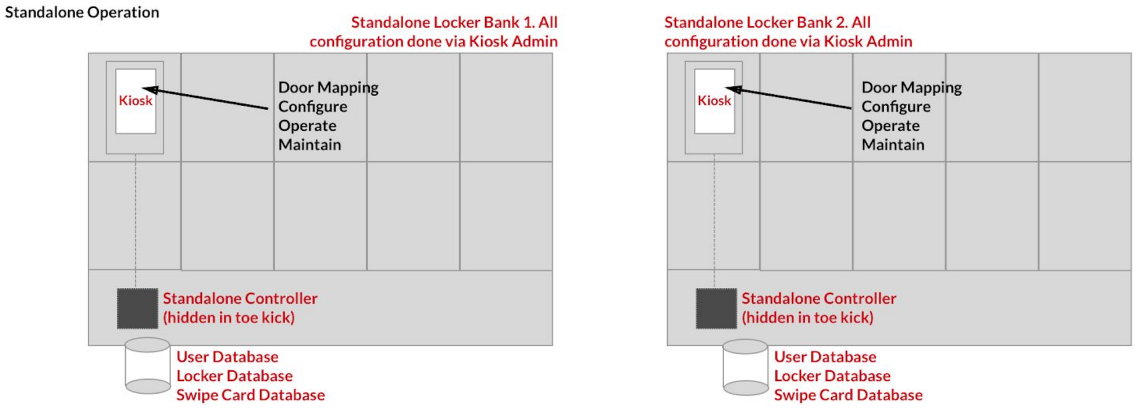
Smartalock is an advanced smart locker system designed for use in agile office workplaces, universities and gyms. This document describes the different operating mode for the Smartalock system and then provides a guide for operating the system in the configured mode.

This guide does not cover the initial installation of the Smartalock system. System installation including wiring locks and kiosks to controllers, and optionally controllers to an IP network along with the initial configuration and mapping of doors is performed by a Smartalock trained installers and resellers.

1.1 Operation Modes

Where more than 1 locker bank is being deployed for a customer, they can be deployed in 2 modes: Standalone or Master/Slave. Where there is only 1 locker bank it must operate in Standalone mode. The differences between these modes is shown and described below:

1.2 Standalone Operation:


Standalone Operation
Standalone Locker Bank 1. All configuration done via Kiosk Admin
Kiosk
Door Mapping
Configure
Operate
Maintain
Standalone Controller (hidden in toe kick)
User Database
Locker Database
Swipe Card Database
Standalone Locker Bank 2. All configuration done via Kiosk Admin
Kiosk
Door Mapping
Configure
Operate
Maintain
Standalone Controller (hidden in toe kick)
User Database
Locker Database
Swipe Card Database

In Standalone Mode, each Smartalock locker bank is a completely independent system. It is initially configured via the touchscreen kiosk, and all ongoing administration is also performed via the same touchscreen kiosk. The database of users, swipe cards and their locker allocations, along with the general system settings are all stored on the controller unit generally hidden in the locker toe kick.

The system administrator can enter the kiosk “Admin” mode via a secure PIN code that is entered directly on the touch screen Kiosk. The guide for administering the standalone system starts at section 2.0 below.

The advantages of Standalone mode include

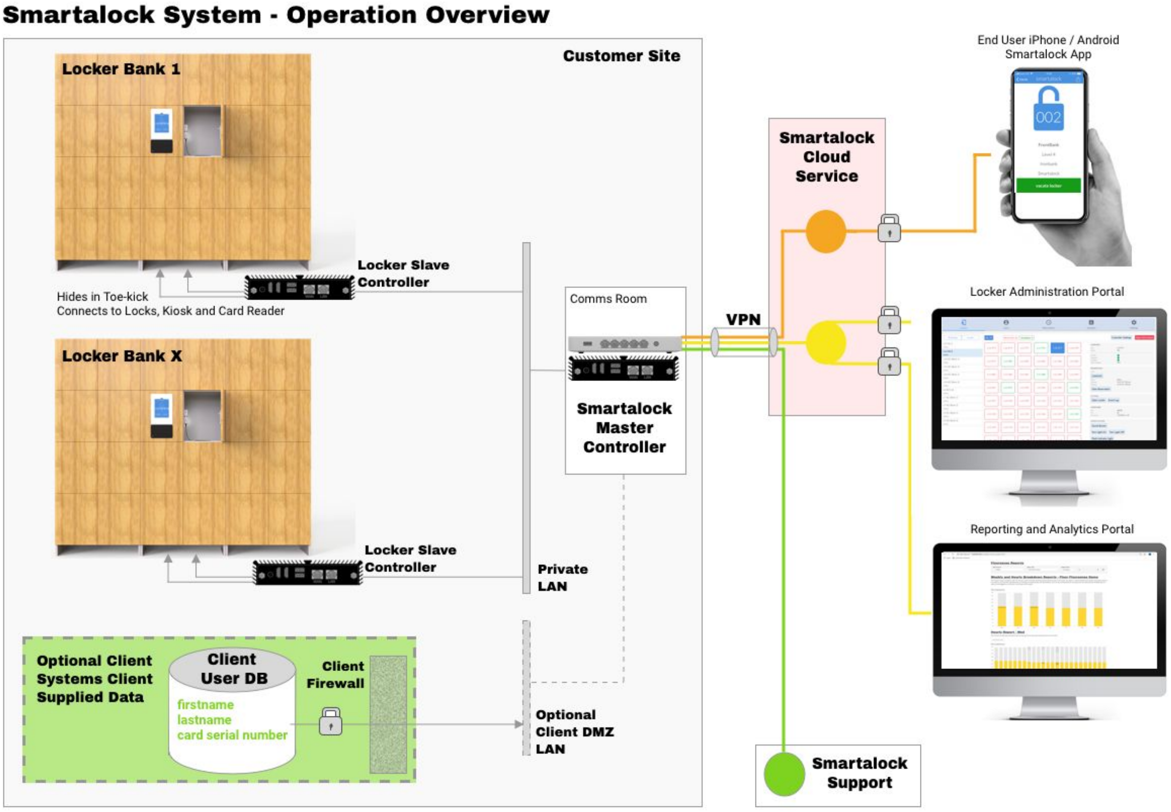
- Simple configuration interface available directly from each locker bank
- No LAN and/or Internet connection required to operate
- Generally no IT involvement in system deployment

The disadvantages of Standalone mode include

- Duplication of user database between different standalone locker banks
- Single point of failure for the Controller
- Simple configuration interface via touchscreen less efficient for performing bulk tasks such as creating a lot of users.
- Must be managed at the locker bank itself - no remote access.
- System Analytics will not be easily available

Standalone mode is only preferable when there is only a single locker bank, and where such locker bank will only operate in “Adhoc” mode - meaning they give out lockers dynamically to anyone with a valid swipe card - and therefore there is minimal requirement to create, store and track system users.

1.3 Master Slave Operation:



In Master/Slave Mode, each Smartalock locker bank forms part of a single larger system. The locker bank has its initial door mapping (assigning a locker number to each door) via the touchscreen kiosk, but after that all system administration is performed via a web browser connection to the Master server.

The Master server is a single small appliance provided by Smartalock that is generally installed in a customers comms/computer room.

The touchscreen kiosk on each locker bank is generally used only for self service by the locker bank end users. End users use the kiosk to interact with the locker bank (ie swipe cards on reader to open their lockers, bind the smartphone app, change their PIN number and other user functions)

The system administrator can still enter the kiosk “Admin” mode via a secure PIN code and perform some Admin functions via the touchscreen kiosk for just that single locker bank, however the primary Administrator interface for Master/Slave systems is via the web user interface which runs on the Smartalock Master server. The guide for operating the Smartalock via the web interface begins at section 3.0 below.

The advantages of Master/Slave mode include

- Single simple web interface to manage hundreds of locker banks and thousands of users. The Locker banks can even be distributed between different buildings in different cities.
- Centralized, synchronized user, locker and swipe card database shared between master and all slave controllers
- Realtime system analytics
- Automated backups of all slave and master databases to Smartalock cloud secure storage (optional - IT security documentation available on request)
- Each locker bank can still operate in “Offline” mode if Master server fails or not available via the network.
- Integration with other Smartalock products such as the floorsense desk reservation / occupancy sensing system will require the Master/Slave mode.

The disadvantages of Master/Slave mode include

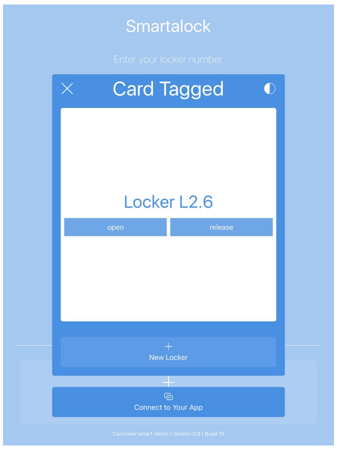
- Requires each locker bank to have an Ethernet connection into a common LAN where the Master Server can also reside
- Requires customer to provide Internet access to the outside WAN port of the master controller for certain functions. Internet is **not** a requirement for end user locker operation with a swipe card or PIN, but is required for smartphone operation.
- May require involvement by customers IT department during deployment.

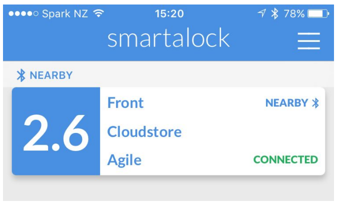
.

Once a system is configured as Master/Slave it cannot revert to standalone mode without being completely reset to factory defaults. All users, locker allocations and swipe card information would be lost.

1.4 Smartalock Terminology

There is some terminology used within the Smartalock system which is explained below

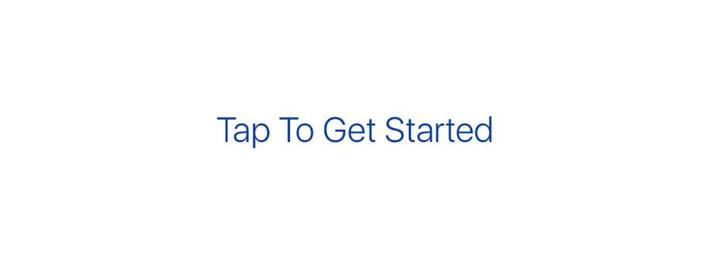
Term	Description
Adhoc Reservation  Smartalock Enter your locker number Card Tagged Locker L2.6 open release New Locker Connect to Your App Controller:smart-demo | Version:0.9 | Build:15	Where a locker bank is setup by the administrator to support Adhoc Reservations (for all, or just a subset of lockers) it will allow any Swipe card user to obtain a locker on demand, on a first come, first served basis until all the lockers available for adhoc use are consumed. A locker can be requested simply by swiping a card which the internal kiosk card reader can read (usually tuned to customers particular brand of building access card). On this happening, an Adhoc Reservation is created, the locker door is opened, and the locker is removed from the pool of available lockers for other users. The user can **release** the locker reservation at any time during use when accessing their locker. If the reservations expires prior to the user releasing it, the locker door can be opened by the card a final time, or depending on the Administrator settings it may automatically open, or require the

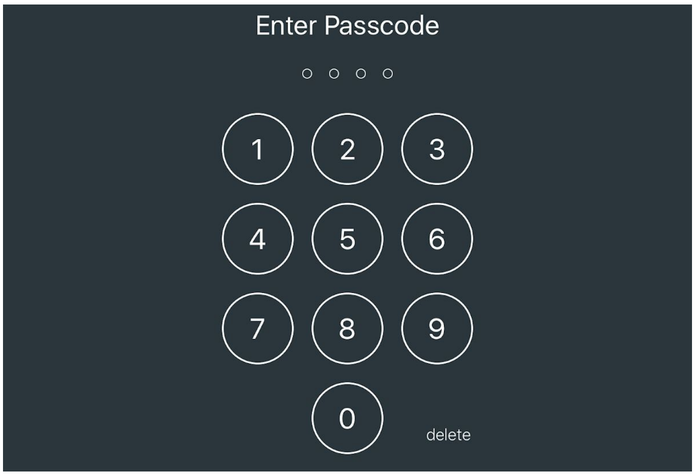
	Administrator to open it for the user. The kiosk will warn that the reservation has expired so closing the door will release the locker back into the available pool. The card will then no longer be able to open the locker, however swiping the card again will create a new reservation, and the default algorithm will most likely assign the same locker. Adhoc Reservations are generally for a short time period - for example, 1 hour in a classroom, 2 hours for gym, 1 day for an Office workplace. The time period is set by the Administrator. The default behaviour if a reservation expires is to keep the door closed, **but only allow 1 more open by the owner** (to clear the locker). The Administrator however can change the default behaviour to open the locker automatically at the end of the reservation. If the card user is finished with the locker before the reservation expires the user can Vacate the locker by tapping the **release** button on the kiosk screen after swiping their card.
Fixed Reservation  ●●●●○ Spark NZ 15:20 78% smartalock NEARBY 2.6 Front Cloudstore Agile NEARBY CONNECTED	A Fixed Reservation is where a locker is pre-allocated to a user for longer term use - for example a school term, a year, or permanently for an office employee. Fixed Reservations are created and removed by the Administrator through the Administrator via the Admin interface on the Kiosk or via the Web Admin application. They are not able to be *created* by the user by swiping their card, however the Smartalock card can have an existing Fixed reservation added to it, so it can be accessed via a card To add a fixed reservation to the Smartalock App see section 3.0 below

2.0 Standalone / Kiosk System Administration

This section describes the sections of the Kiosk Admin interface, along with how to perform common workflows such as creating a user, binding their existing swipe card and allocating them a locker. Other common tasks such as transferring a locker from an existing user to a new user, and sharing a single locker between users are also covered.

2.1 Access to the Kiosk Administration Interface

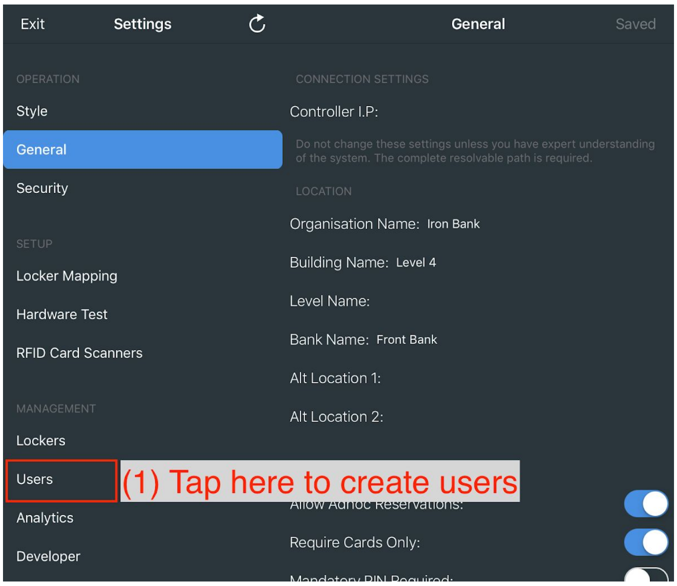
Tap To Get Started	To enter Administrator mode, first wait unit the Kiosk Lock Screen appears. The screen will be all blue or white and say “Tap to Get Started” at the top. When this screen is visible firmly tap

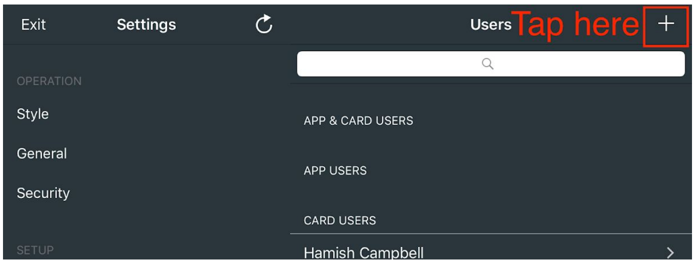
	twice quickly on the **center** of the screen
 Enter Passcode 1 2 3 4 5 6 7 8 9 0 delete	If double tap was successful the screen will turn black and a PIN pad will appear. Enter the Administrators PIN code. By default this is **5555** **If the double tap resulted in the normal end user blue screen “Enter Locker Number” then wait until the “Tap to Get Started” appears and try the double-center-tap again.**

2.2 Creating New Users and Binding Swipe Cards

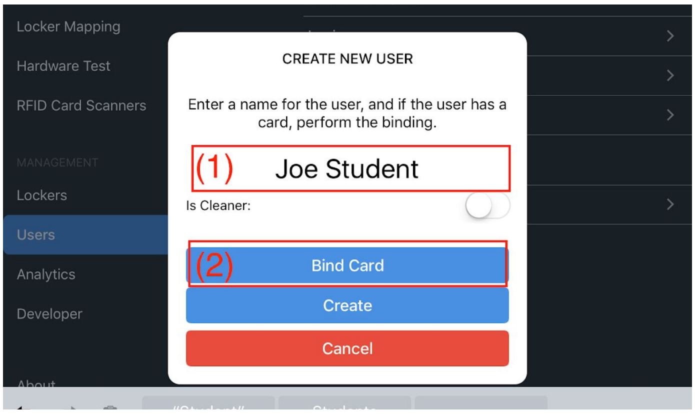
Where lockers will be fixed allocated to users, it is necessary to create a user in the kiosk Admin interface before they can be allocated a locker. If the Locker bank will allow dynamic (adhoc) allocation of lockers to users - ie on a first come first served anonymous basis, then it is not necessary to pre-create any users for adhoc use.

To create a user and bind an existing swipe card to them follow the below workflow.

 Exit Settings General Saved OPERATION Style General Security SETUP Locker Mapping Hardware Test RFID Card Scanners MANAGEMENT Lockers Users Analytics Developer CONNECTION SETTINGS Controller I.P: Do not change these settings unless you have expert understanding of the system. The complete resolvable path is required. LOCATION Organisation Name: Iron Bank Building Name: Level 4 Level Name: Bank Name: Front Bank Alt Location 1: Alt Location 2: Allow Adhoc Reservations: ● Require Cards Only: ● Mandatory PIN Required: ○ (1) Tap here to create users	Tap the Users button on Left and then create a user by performing these steps:



Tap the + button in top right, then:



CREATE NEW USER

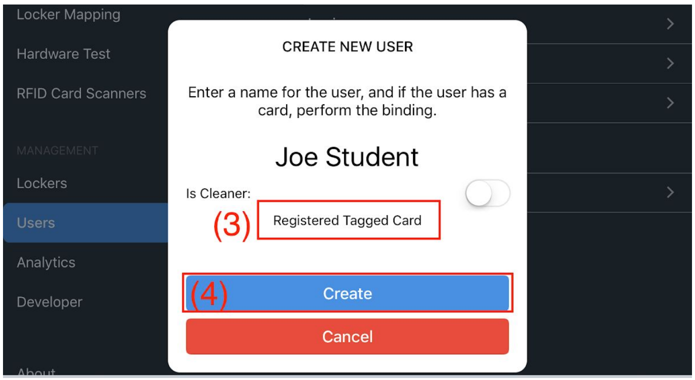
Enter a name for the user, and if the user has a card, perform the binding.

Joe Student

Is Cleaner:

1) Enter Name for User

2) Tap **Bind card** and then swipe a new Smartalock card on Kiosk card reader. This card is associated with a user not a locker.



CREATE NEW USER

Enter a name for the user, and if the user has a card, perform the binding.

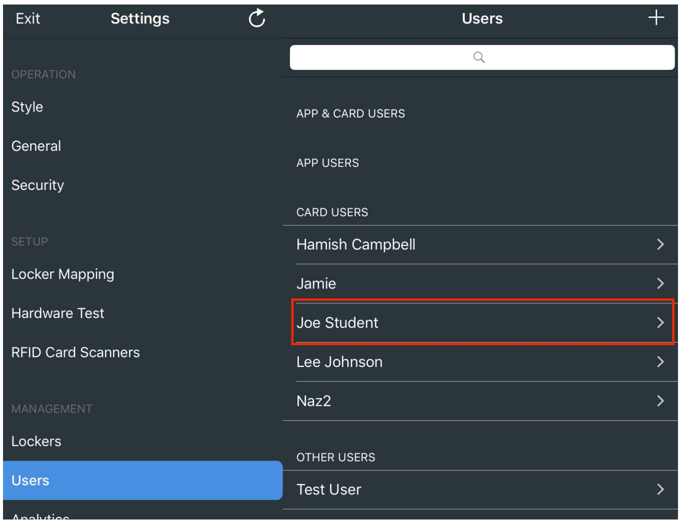
Joe Student

Is Cleaner:

Registered Tagged Card

3) Wait for confirmation (listen for beep)

4) Tap Create User

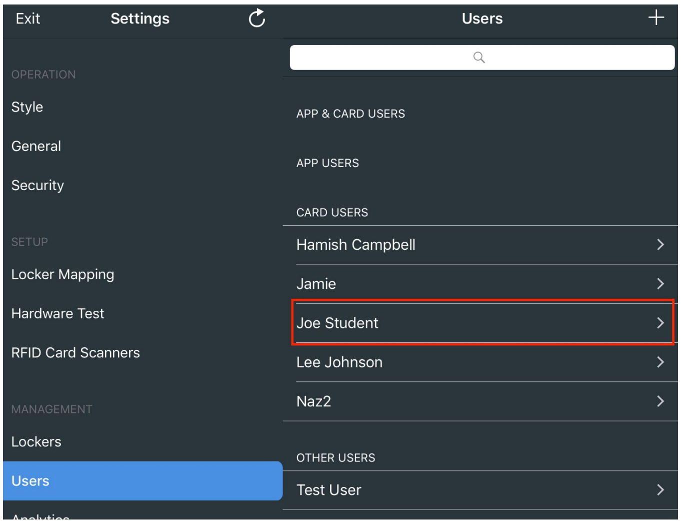


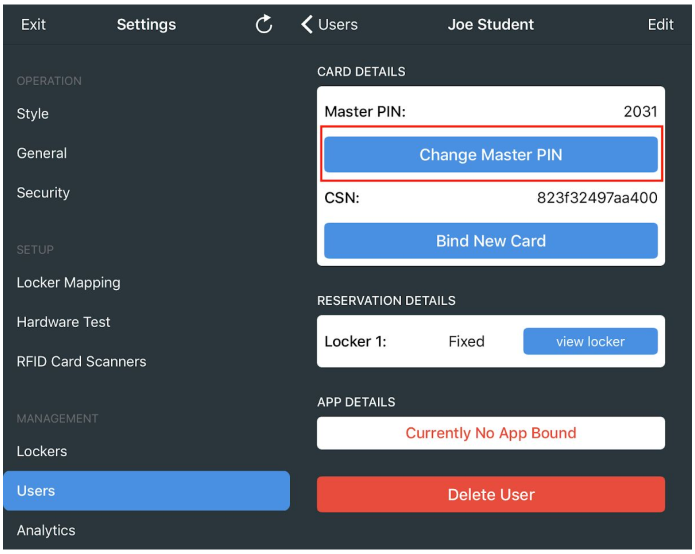
5) New User now appears in User List

Repeat the User Creation process for all the new users. When all the new users are created, they can be fixed allocated lockers from the locker tab.

2.2.1 Editing an Existing User

Sometimes it may be necessary to edit an existing user. The most common reason is to update a user's PIN if they have forgotten it, bind a different swipe card, or to rename a user that has left the company to a new starter at the company which is the fastest way to transfer a locker from a departing employee to a new employee.





Master PIN: 2031

CSN: 823f32497aa400

Locker 1: Fixed

To enter Administrator mode, first wait unit the Kiosk Lock Screen appears and then firmly tap **twice** on the **center** of the screen

Enter **5555** to go to the Admin Screen

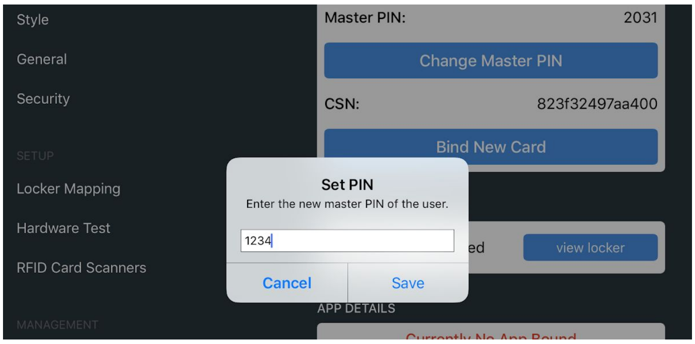
Tap on Users (left hand side)

Select the User

Tap “Change Master PIN”

Enter new value - ONLY ENTER 4 NUMBERS. DO NOT ENTER LETTERS. Then tap Save.

To Rename a user tap on the user's name and from the User details page tap the **Edit** button (top right). This allows the users name to be changed and saved.



Master PIN: 2031

CSN: 823f32497aa400

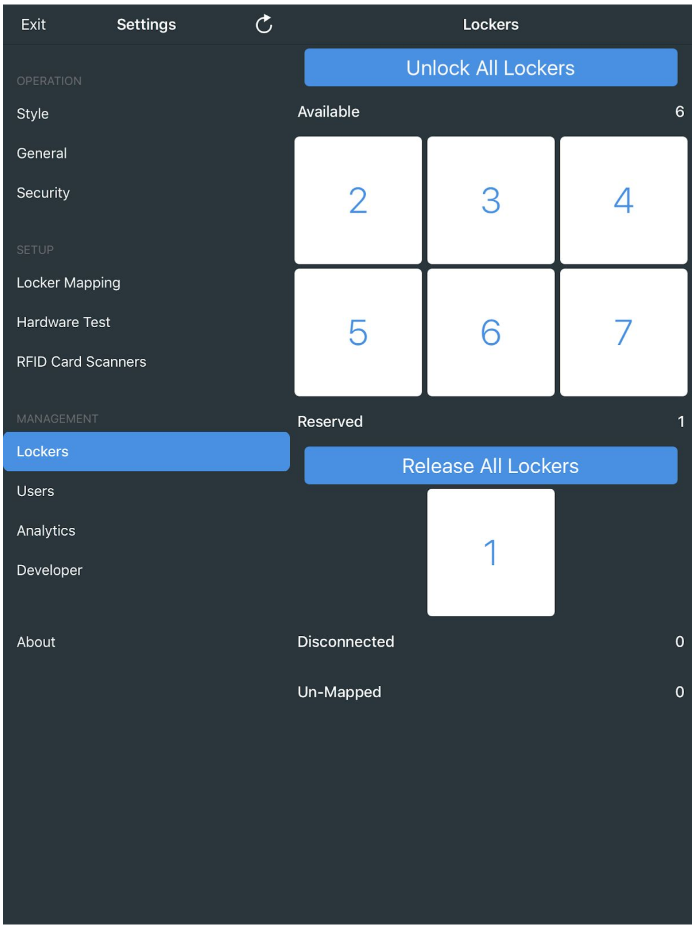
Set PIN

Enter the new master PIN of the user.

1234

2.3 Allocating and Releasing Lockers - Fixed Allocations

Once users are created, Lockers can be allocated to them via the Locker tab. Follow the below workflow to allocate a free locker to a user. The locker will belong to the user forever until it is manually released by the Administrator back into the available pool.



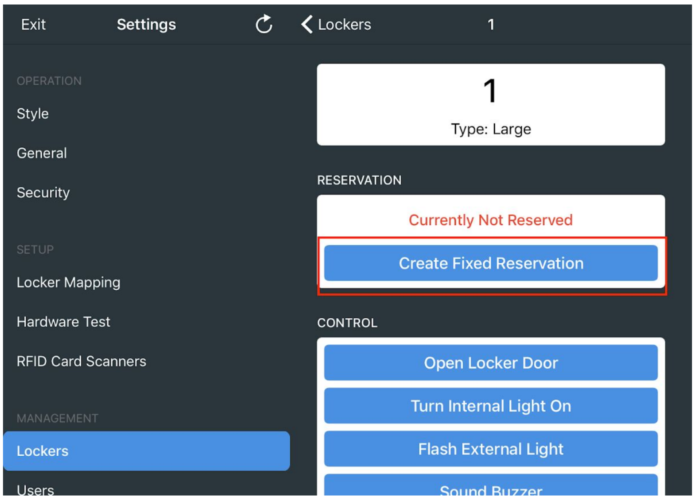
Available 6

Reserved 1

Disconnected 0

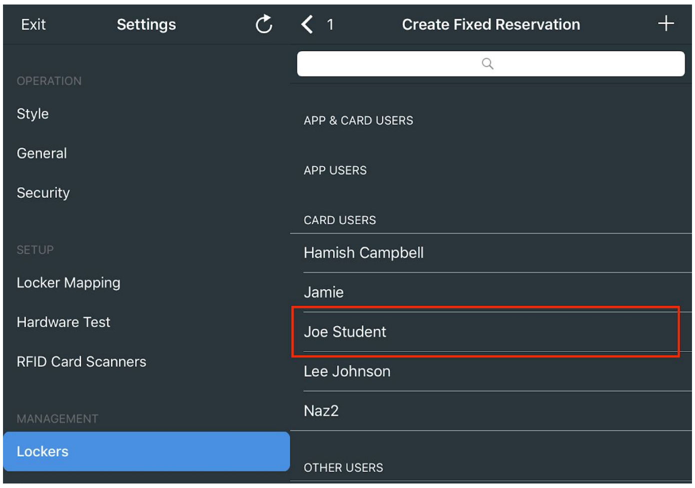
Un-Mapped 0

Tap on lockers (left hand side) to see a list of all the lockers available. Tap on a locker from the **Available** list

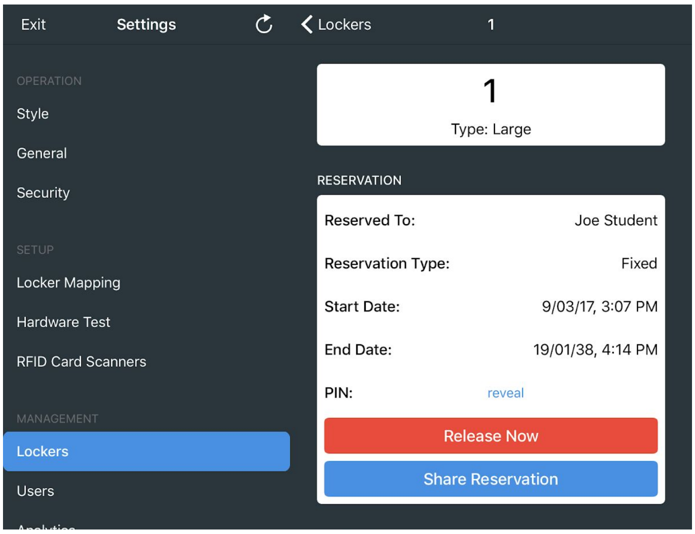


Once locker selected

tap Create Fixed Reservation, and



Then select the user. In systems with more than 100 users it will be necessary to search for the user in the search box first as generally only the first 100 users alphabetically are loaded from the Controller.



Reserved To: Joe Student

Reservation Type: Fixed

Start Date: 9/03/17, 3:07 PM

End Date: 19/01/38, 4:14 PM

PIN: reveal

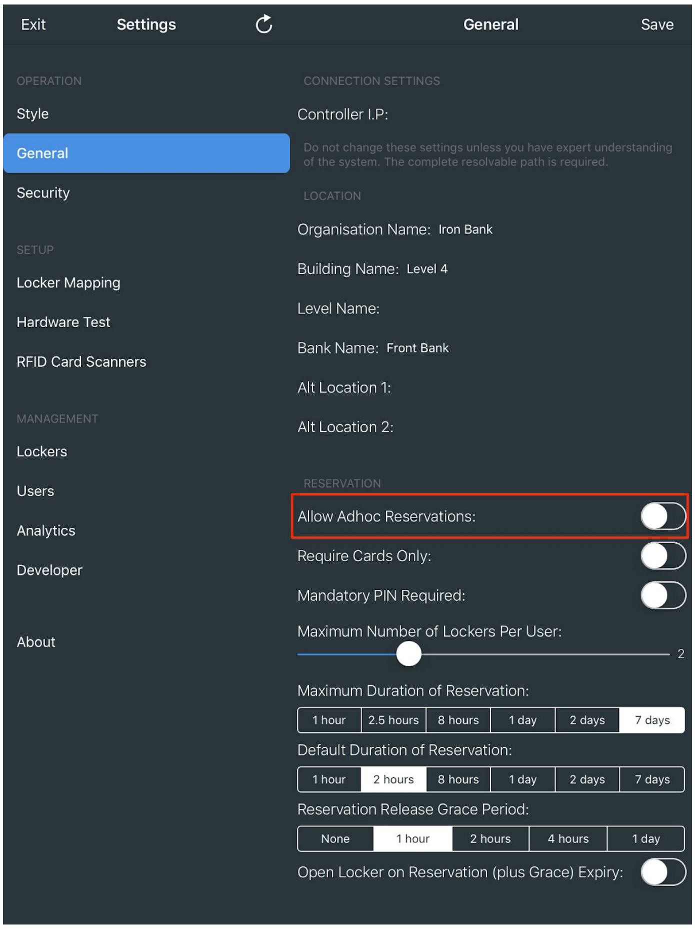
The screen will update once the reservation is created.

Tapping “Release Now” will remove the reservation from the user, freeing the locker up for allocating to a different user.

Tap Lockers to go back to the list of lockers to assign next locker to the next user.

2.4 General Administrative Settings

Smartalock in standalone mode has its general settings configured on the “General” tab. This interface allows for setting general features such as whether Adhoc allocation of lockers is allowed and how long adhoc reservations last for.



CONNECTION SETTINGS

Controller I.P:

Do not change these settings unless you have expert understanding of the system. The complete resolvable path is required.

LOCATION

Organisation Name: Iron Bank

Building Name: Level 4

Level Name:

Bank Name: Front Bank

Alt Location 1:

Alt Location 2:

RESERVATION

Allow Adhoc Reservations: ○

Require Cards Only: ○

Mandatory PIN Required: ○

Maximum Number of Lockers Per User: 2

Maximum Duration of Reservation: 1 hour | 2.5 hours | 8 hours | 1 day | 2 days | [✓ 7 days]

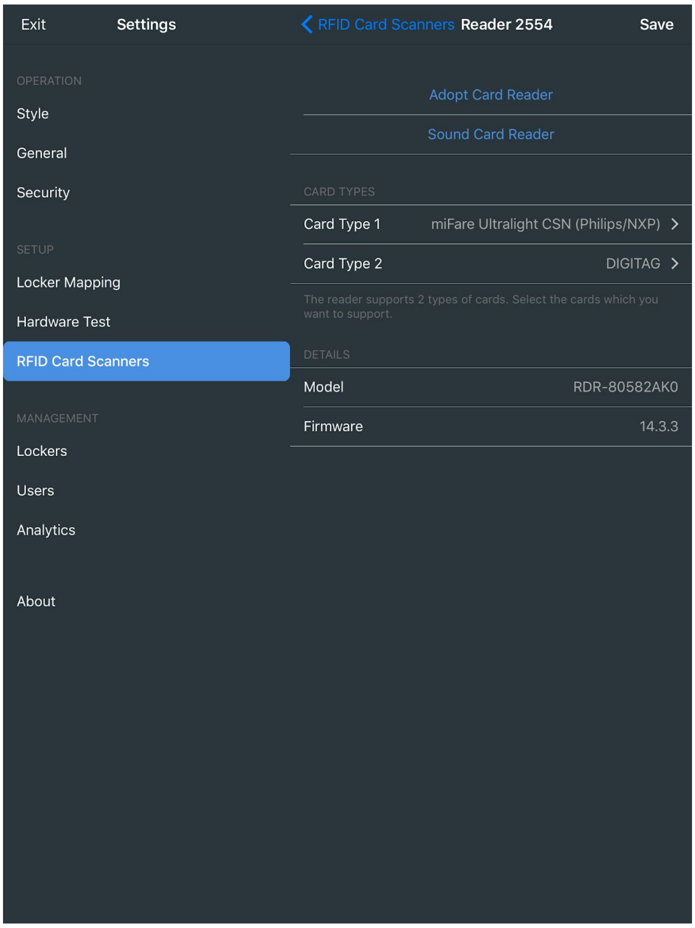
Default Duration of Reservation: 1 hour | [✓ 2 hours] | 8 hours | 1 day | 2 days | 7 days

Reservation Release Grace Period: None | [✓ 1 hour] | 2 hours | 4 hours | 1 day

Open Locker on Reservation (plus Grace) Expiry: ○

The General Settings allow for configuration of the following features typically used in a Card/Kiosk only deployment:

1) **Allow Adhoc Reservations** - allows users to obtain lockers on demand on a first in first served basis. Once all lockers have been assigned to users, this should be **disabled** by default
2) Set the maximum amount of lockers a single user (swipe card) can obtain - default is 2
3) Set the duration the reservation - the d**efault is 2 hours for adhoc. Fixed allocation lockers do not ever expire.**
4) Set a Grace period for if the user does not vacate (release) their locker before the end of the reservation time. **The default is none**. If a grace period is set it silently extends the reservation for the user so they can open the door 1 more time after expiry.
5) Set the action on the expiry of the reservation (plus any grace period) - **By default it will not open the locker**. The Administrator will have to open the locker via the Kiosk.



CARD TYPES

Card Type 1 miFare Ultralight CSN (Philips/NXP)

Card Type 2 DIGITAG

The reader supports 2 types of cards. Select the cards which you want to support.

DETAILS

Model RDR-80582AK0

Firmware 14.3.3

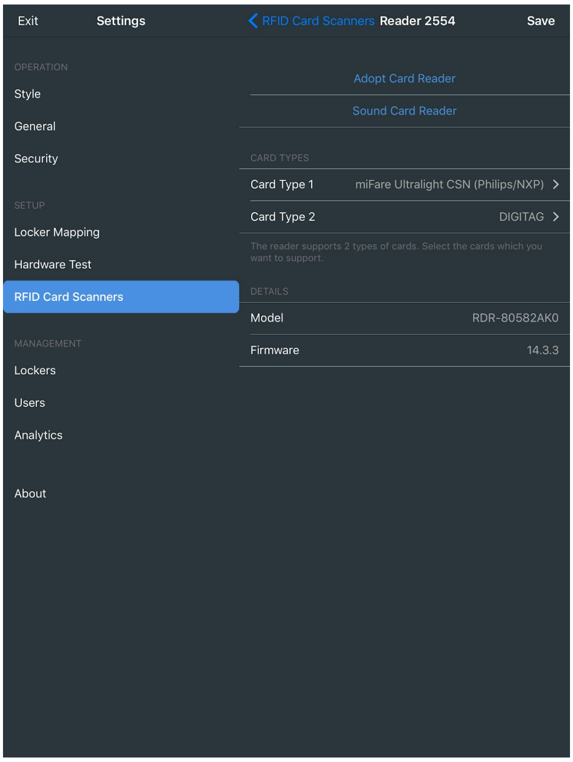
The RFID scanner section lets the Administrator change the card type read by the card reader, or add a second card type. Multiple readers can be attached to a Smartalock controller. In this example there is only 1 reader.

The “Card Type 1” is set during installation to match the customers building swipe cards. Only change this setting to add a second type of card - “Card Type 2” (for example to read cards from employees that work in a different building that has a different card type).

2.4.1 Card Reader Configuration Detail

The RFID scanner section lets the Administrator change the card type read by the card reader, or add a second card type. Multiple readers can be attached to a Smartalock controller. In this example there is only 1 reader.

Normally there will be no need to configure the card reader as it will have been pre-configured to match the customers flavour of building card during commissioning.



CARD TYPES

Card Type 1: miFare Ultralight CSN (Philips/NXP)

Card Type 2: DIGITAG

The reader supports 2 types of cards. Select the cards which you want to support.

DETAILS

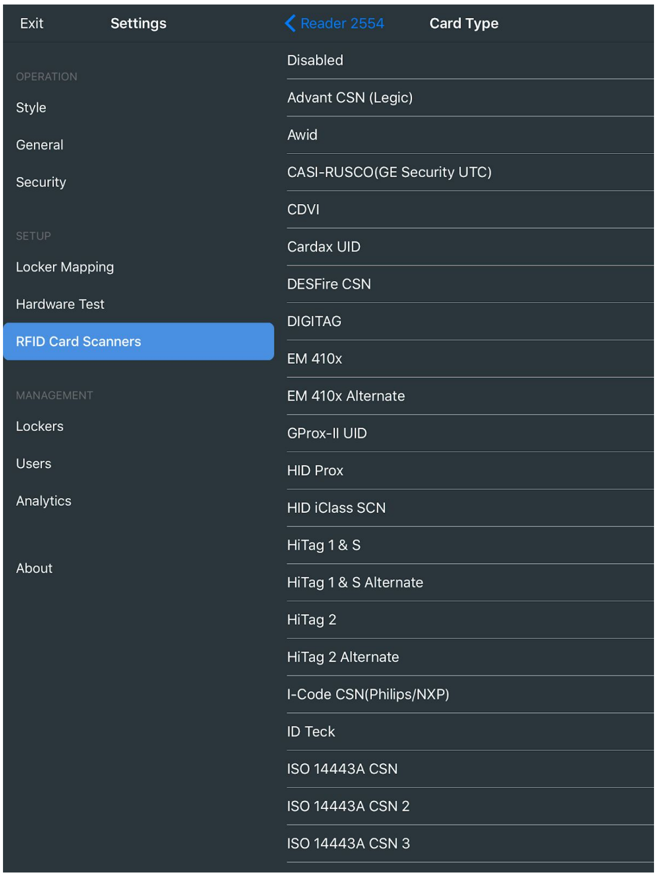
Model: RDR-80582AK0

Firmware: 14.3.3

The RFID scanner section lets the Administrator change the card type read by the card reader, or add a second card type. Multiple readers can be attached to a Smartalock controller. In this example there is only 1 reader.

Adopting a card reader means that events from the card reader will be displayed on this kiosk screen. Note that multiple kiosks can adopt a single reader or vice verse. A card reader does not have to be adopted, however without adoption the kiosk may not popup messages such as “Door XXX opened” when the card is swiped, even though the door will still open.

Sounding a card reader is useful for identifying which reader the kiosk is associated with when there is more than one.



Disabled
Advant CSN (Legic)
Awid
CASI-RUSCO(GE Security UTC)
CDVI
Cardax UID
DESFire CSN
DIGITAG
EM 410x
EM 410x Alternate
GProx-II UID
HID Prox
HID iClass SCN
HiTag 1 & S
HiTag 1 & S Alternate
HiTag 2
HiTag 2 Alternate
I-Code CSN(Philips/NXP)
ID Teck
ISO 14443A CSN
ISO 14443A CSN 2
ISO 14443A CSN 3

The Card reader supports many types of cards. Contact Smartalock support at support@smartalock.com for more information on setting the card type.

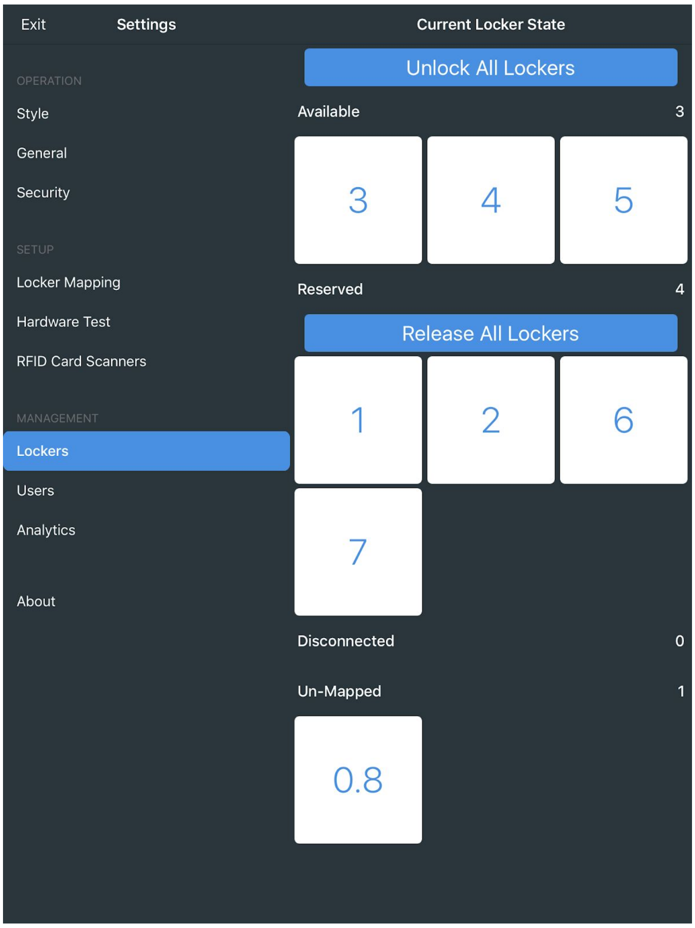
Note that the card reader can read the unencrypted unique Card Serial Number (CSN) from each card type in this list. It cannot read any encrypted / secure area of these cards. To read the encrypted content of a swipe card will require additional integration with the card reader system.

2.5 Locker Administration

The Locker section allows for the selection and management of individual lockers within the locker bank connected via this controller.

The first screen presents a list of the systems lockers, grouped into the following categories:

Available	Reserved	Disabled / Disconnected	Unmapped
These lockers are online and currently not assigned to any user. If adhoc reservations are enabled lockers will be allocated from this pool	These lockers are currently assigned to a user - either a fixed reservation, shared reservation or adhoc reservation	These lockers are connected to the system but have been administratively disabled - for example if the hardware has failed or the physical locker has been damaged	These are lockers that may or may not be currently connected to the system. If they are currently connected then they can be mapped to a locker number and made available



Available 3

3 4 5

Reserved 4

1 2 6

7

Disconnected 0

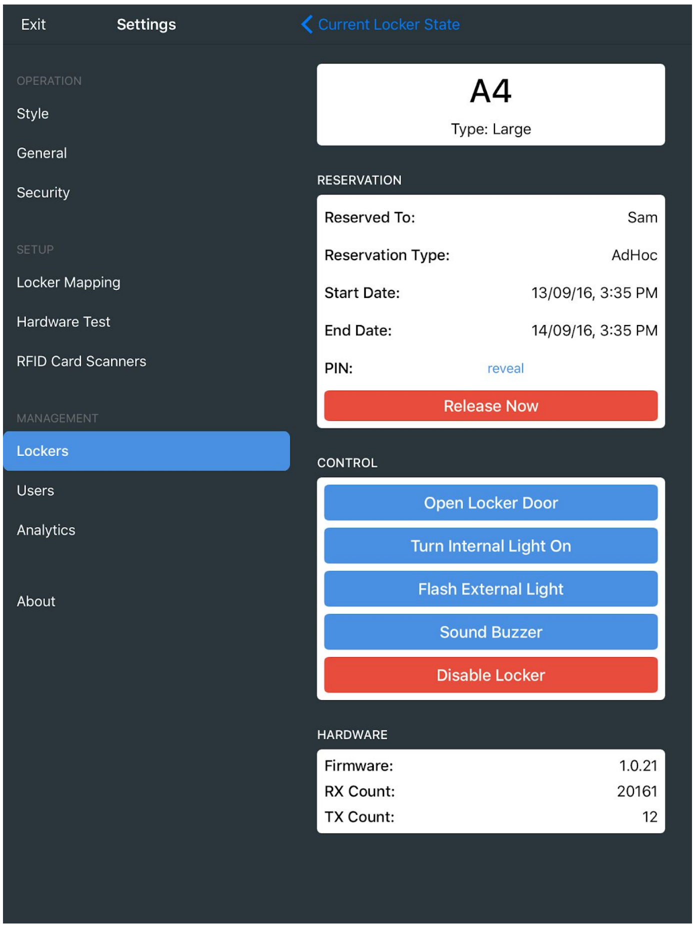
Un-Mapped 1

0.8

The Lockers tab shows a list of all the lockers and their current state:

- Available: currently un-allocated to a user
- Reserved: have current reservations
- Disconnected: Are currently offline due to a fault
- Un-Mapped: Lockers that are connected to the system but have not yet been provisioned

Tapping on a locker number will allow the Administrator to carry out various operations



A4

Type: Large

RESERVATION

Reserved To:	Sam
Reservation Type:	AdHoc
Start Date:	13/09/16, 3:35 PM
End Date:	14/09/16, 3:35 PM
PIN:	reveal

HARDWARE

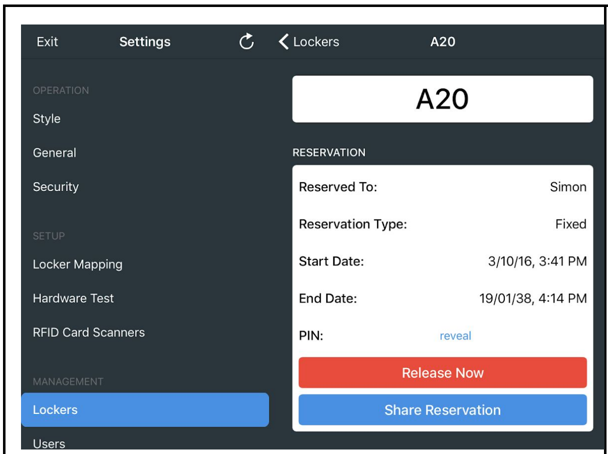
Firmware:	1.0.21
RX Count:	20161
TX Count:	12

Tapping on a locker number from the locker list will allow the Administrator to perform the following tasks:

- Release the reservation which will remove the locker from a users assignment
- Open the locker door
- Cause the external light to flash (useful to find the locker in large banks)
- Test the internal light and tamper alarm
- Disable the locker - this is used only when the locker has some hardware fault and should be replaced. Do not disable functional lockers. To ensure a locker is not available for allocation to a user, instead create a new user (see below) and allocate that user the locker

2.5.1 Sharing Lockers between Users

Often the Administrator may wish to share a single locker with multiple users. This feature is useful for lockers used as coat cupboards that all users have access to, or team lockers shared by a small subset of users.



A20

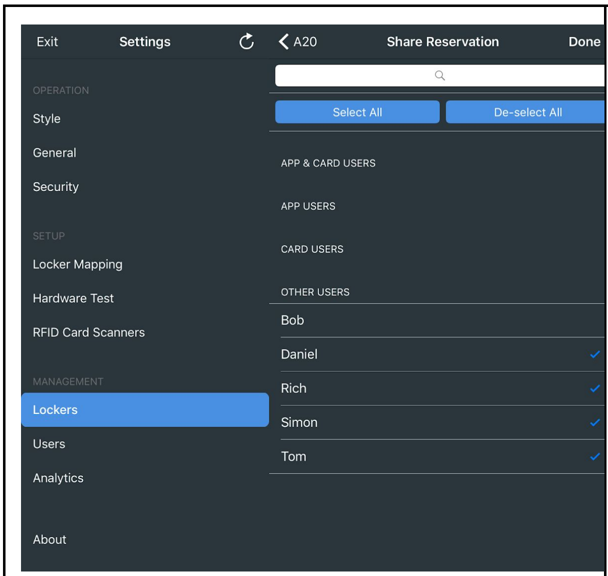
RESERVATION

Reserved To:	Simon
Reservation Type:	Fixed
Start Date:	3/10/16, 3:41 PM
End Date:	19/01/38, 4:14 PM
PIN:	reveal

Select the Locker to be shared from the Locker list. **The locker should already have a fixed reservation to a first user**. If the locker is unreserved then first reserve it to a single user first (follow instructions above).

Tap the Share Reservation button to bring up a list of users. If there are many users use the search function to search for them.

Tap each user that the locker should be shared with.
Each user that now has access to the locker will have a tick next to their name.



APP & CARD USERS

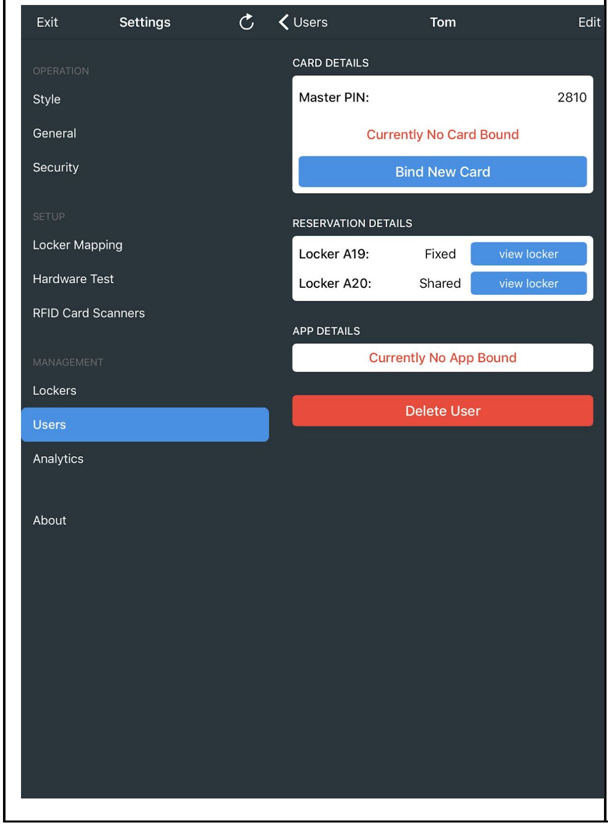
APP USERS

CARD USERS

OTHER USERS

Bob	
Daniel	✓
Rich	✓
Simon	✓
Tom	✓

Finally tap Done (top right) to save the sharing settings for the locker.



CARD DETAILS

Master PIN: 2810

Currently No Card Bound

RESERVATION DETAILS

Locker A19: Fixed

Locker A20: Shared

APP DETAILS

Currently No App Bound

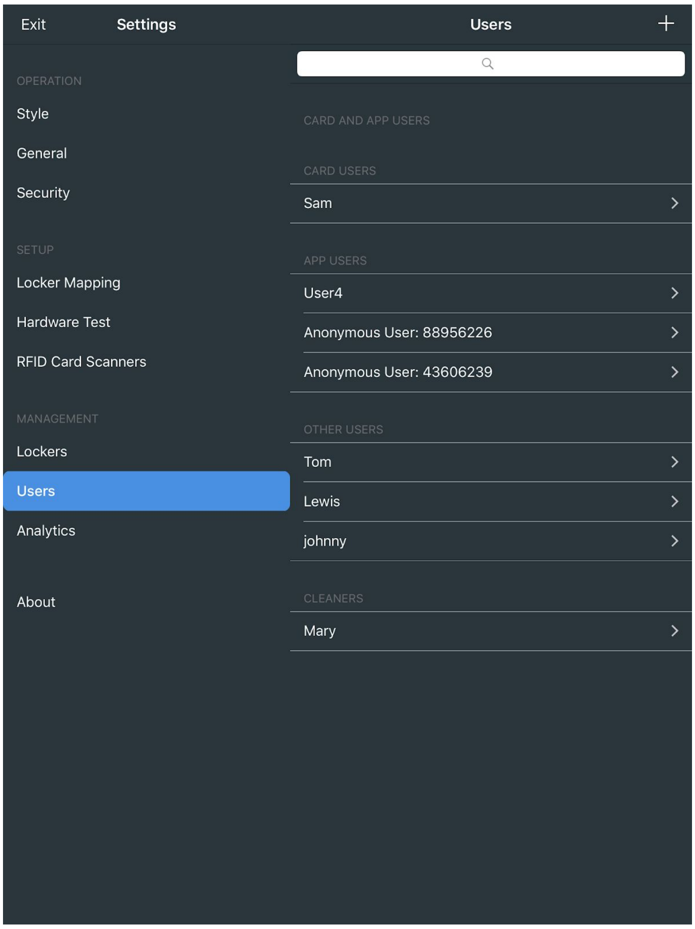
Selecting a User (see section 2.6 below for details on User tab) will show their lockers and whether they are Shared or Fixed. A Fixed reservation is owned directly by the user, a Shared reservation is owned by another user but shared with this user.

2.6 User Administration

The User section allows for the creation, deletion and management of individual users.

Users are grouped into the following types

Card and App	Card User	App User	Other User	Cleaner
A user that has both an access (swipe) card and also a Smartalock app registered as a single user on the system	A user that has a swipe card linked to their user name in the system.	A user of the Smartalock iOS or Android app that does not also have a Building access card linked. Note that app users maybe Anonymous as they are dynamically created when they reserve a locker in adhoc mode	A user that has been created on the system but does not have either a swipe card linked or an App linked. These users may just use the Kiosk with a PIN	A special card only user whos swipe card will open all the lockers



CARD AND APP USERS

CARD USERS

Sam

APP USERS

User4

Anonymous User: 88956226

Anonymous User: 43606239

OTHER USERS

Tom

Lewis

johnny

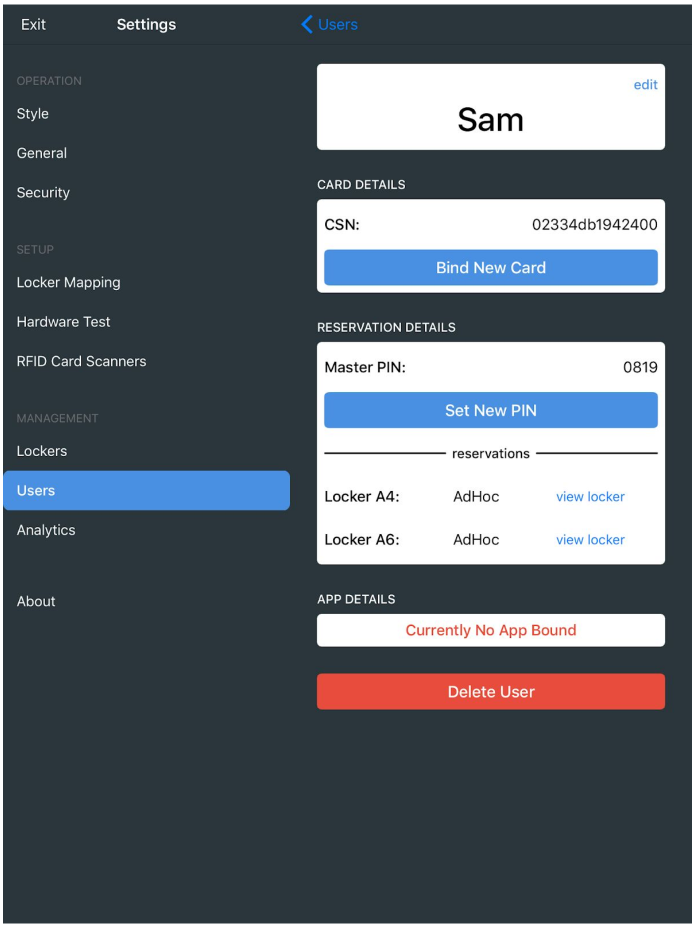
CLEANERS

Mary

The Users tab lists all the users currently enabled on the system. Note when a card is scanned and the system does not recognize that card belonging to any existing user it will create a new Anonymous User automatically that can then be named later (if required) by tapping on their user record.

Tapping the + sign top right allows for the Administrator to create new users in advance of their access to the system (Section 2.2 above). When a user is created but has not been mapped to a swipe card they will appear as an “Other User” in the user list

Cleaners are special types of users. Their Swipe card will open all the lockers. Use the switch “Is Cleaner” when creating a user to enable that user to have Open all locker rights.



Sam

CARD DETAILS

CSN: 02334db1942400

RESERVATION DETAILS

Master PIN: 0819

reservations

Locker A4:	AdHoc	view locker
Locker A6:	AdHoc	view locker

APP DETAILS

Currently No App Bound

The individual User page allows the Administrator to perform the following functions:

- Bind or update the swipe card assigned to the user
- Set a new PIN number for the user. This PIN can be used by the user to open any of their lockers if they have more than 1 locker
- View the users current locker allocations
- Rename the user
- Delete the user. Deleting the user will also delete their associated swipe card so it can be used again.

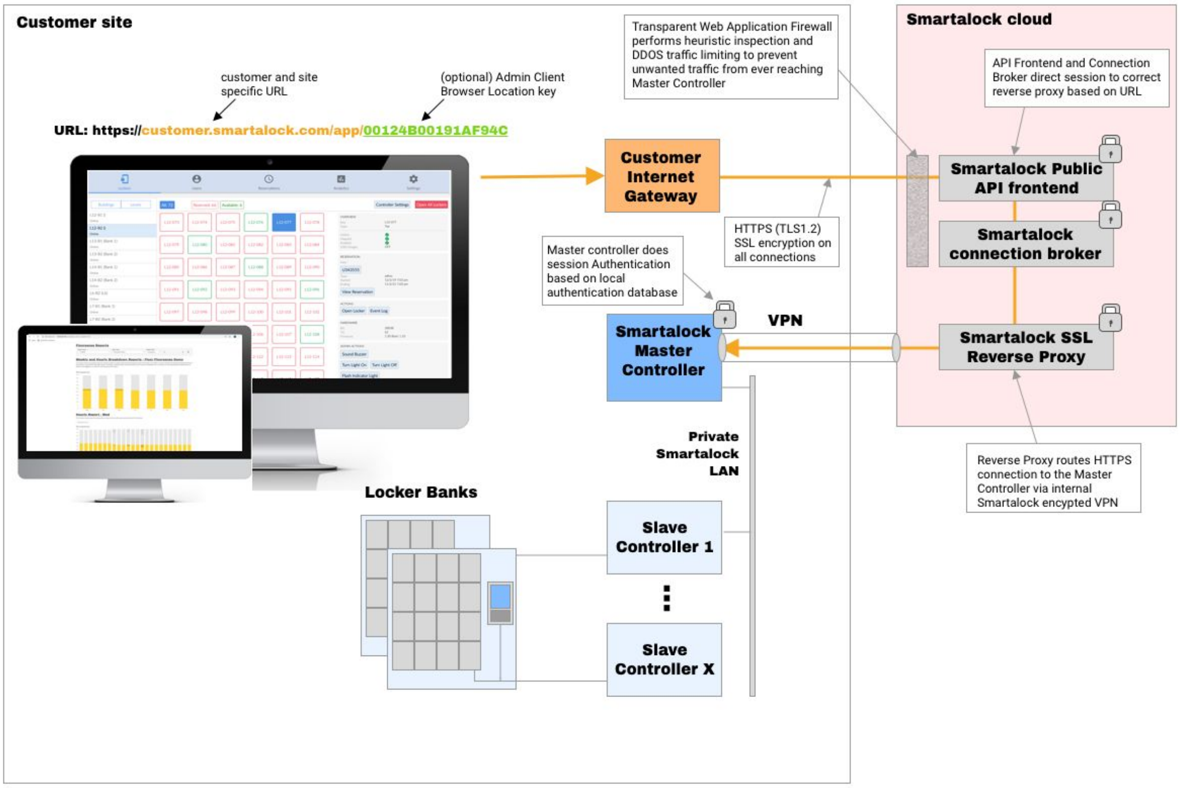
3.0 Master / Slave System Administration

This guide is for the Smartalock locker system administration via the web interface of the Smartalock Master controller. The Master controller generally has 2 methods for accessing its web interface

1) Via an external encrypted URL provided by Smartalock or the Smartalock reseller during commissioning - for example https://customername.smartalock.com
2) Via an internal IP address of the Master controller if it has been allowed to connect to the customers DMZ / Building Management network.

These access methods are shown in the below diagrams:

Access to Administration portal via the Smartalock cloud:



Customer site
URL: https://customer.smartalock.com/app/00124B00191AF94C
Customer Internet Gateway
Smartalock Master Controller
VPN
Private Smartalock LAN
Locker Banks
Slave Controller 1
Slave Controller X
Smartalock cloud
Smartalock Public API frontend
Smartalock connection broker
Smartalock SSL Reverse Proxy

customer and site specific URL

(optional) Admin Client Browser Location key

Transparent Web Application Firewall performs heuristic inspection and DDOS traffic limiting to prevent unwanted traffic from ever reaching Master Controller

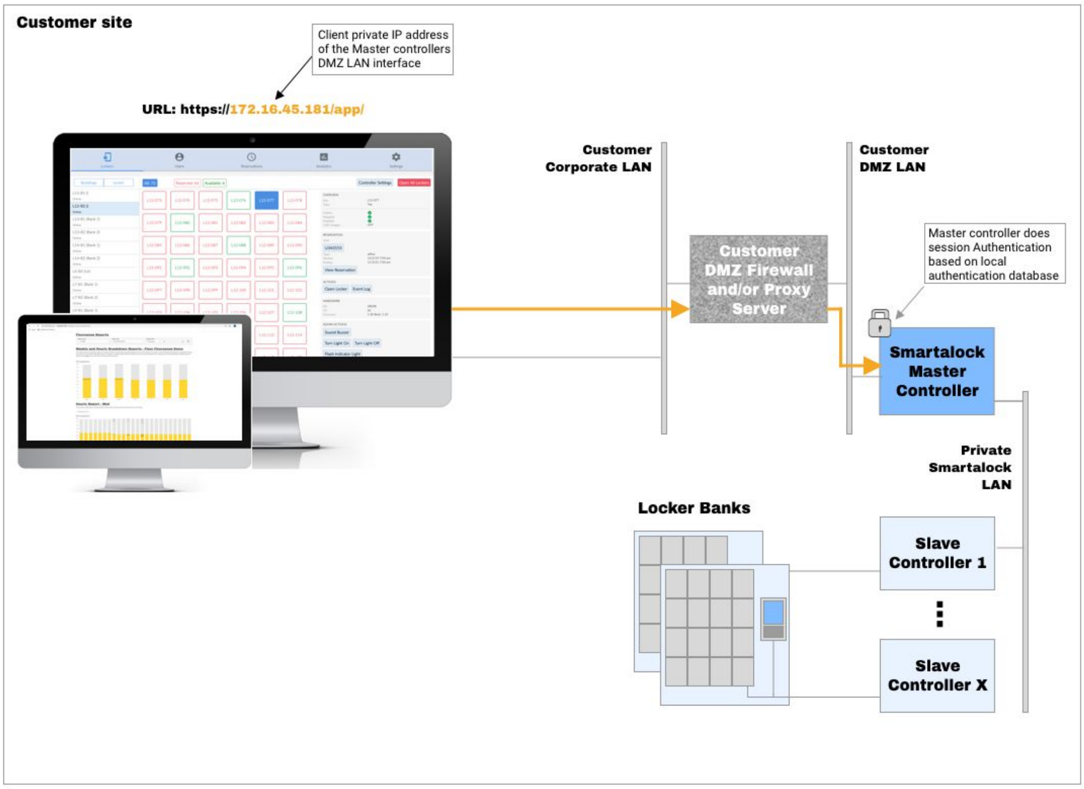
HTTPS (TLS1.2) SSL encryption on all connections

Master controller does session Authentication based on local authentication database

API Frontend and Connection Broker direct session to correct reverse proxy based on URL

Reverse Proxy routes HTTPS connection to the Master Controller via internal Smartalock encypted VPN

Access via internal IP address of the Master controller:



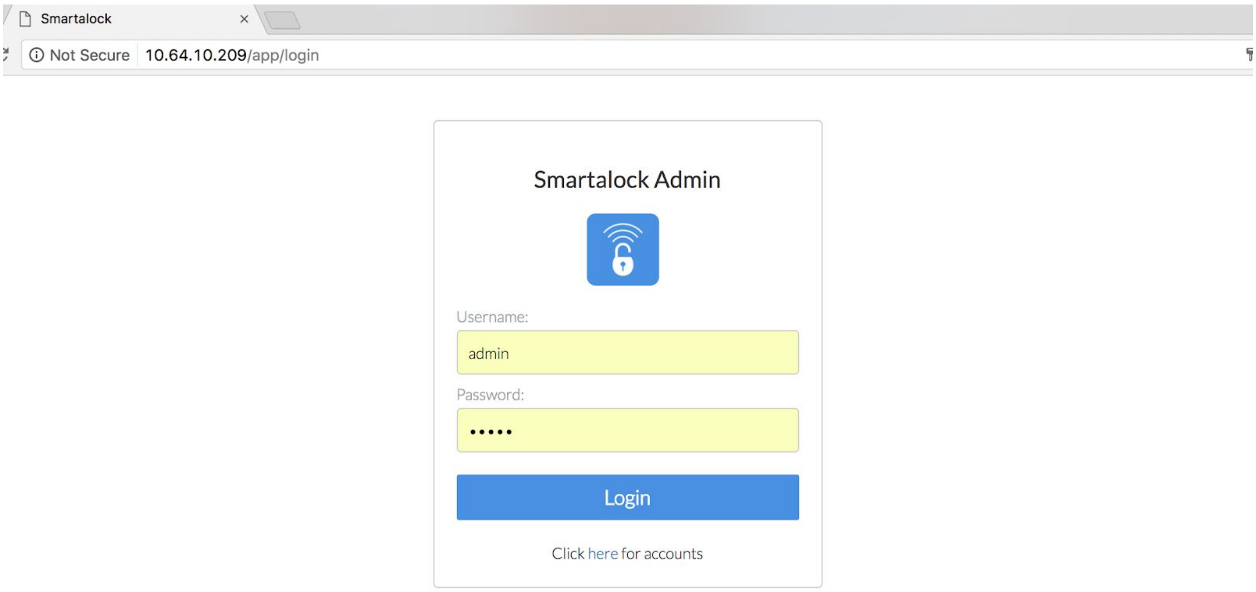
Client private IP address of the Master controllers DMZ LAN interface

Master controller does session Authentication based on local authentication database

3.1 Access to the Web Administration Interface

Smartalock requires **Google Chrome** for accessing the Web interface. Other browsers may not work correctly. In the Chrome browser, type in the IP address of the Master controller interface or the external public URL depending on the access method.

Enter the username and password. By default these are set to **admin**



Not Secure 10.64.10.209/app/login

Smartalock Admin

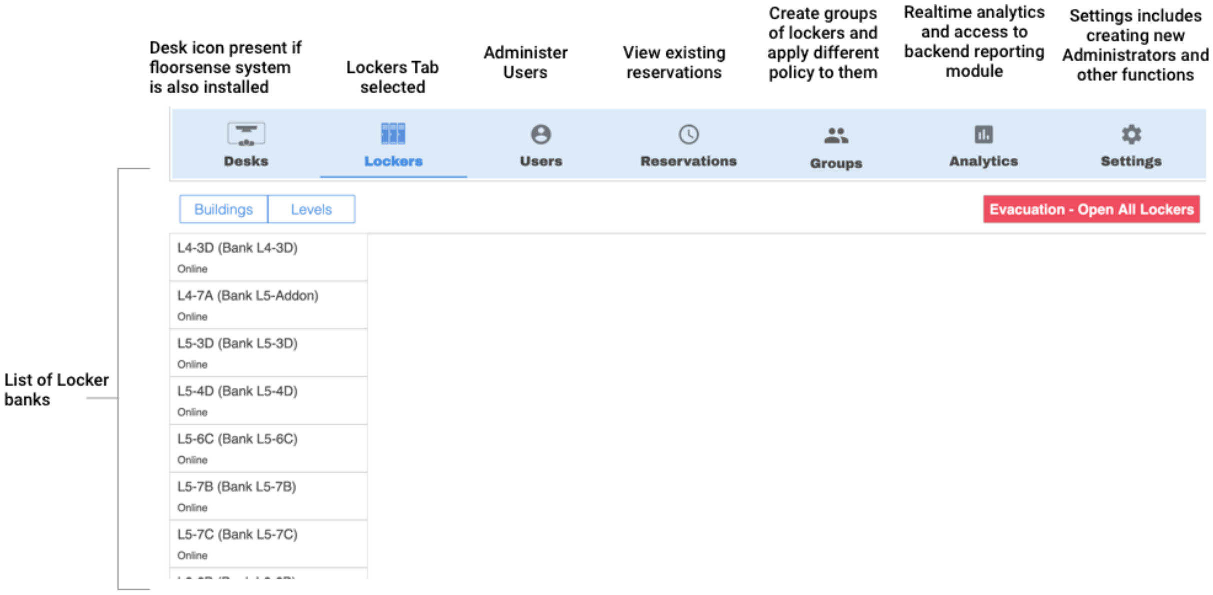
Username: admin

Password: •••••

3.2 Web Interface Overview

The Web interface defaults to the Locker Administration tab. The left hand column is for selecting the locker bank to administer. Tapping the Building / Level buttons filters by these areas to make identifying the locker banks easier.

The top bar is used to navigate to other Admin functions.



Desk icon present if floorsense system is also installed

Lockers Tab selected

Administer Users

View existing reservations

Create groups of lockers and apply different policy to them

Realtime analytics and access to backend reporting module

Settings includes creating new Administrators and other functions

List of Locker banks

L4-3D (Bank L4-3D)
Online

L4-7A (Bank L5-Addon)
Online

L5-3D (Bank L5-3D)
Online

L5-4D (Bank L5-4D)
Online

L5-6C (Bank L5-6C)
Online

L5-7B (Bank L5-7B)
Online

L5-7C (Bank L5-7C)
Online

The User tab is used to add, remove or lookup users on the system along with performing tasks such as assigning a swipe card or changing their locker PIN number.

The Reservations tab is used to review fixed locker reservations for users, or to release existing reservations to make the locker free for assigning to a new user. The fastest way to create a new locker reservation however is directly from the locker tab.

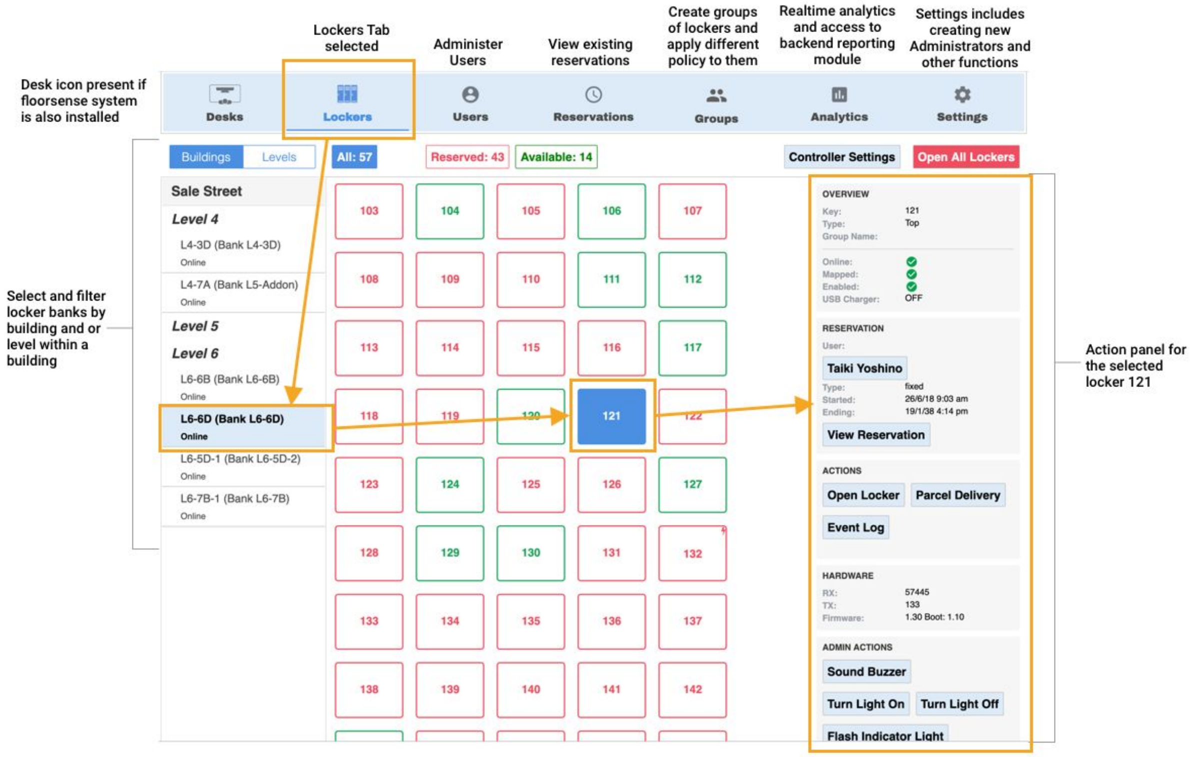
The Groups tab allows for the creation of groups of lockers within or across multiple locker banks and then assign different policy to who can get a locker within different groups, for how long etc.

The Analytics tab links to a statistics dashboard showing which lockers are heavily used, and which are free. It is useful to identify locker banks near capacity. This tab also links to the bank end reporting module which requires a second authentication (use same credentials). If the administrator account is granted reporting access the reporting backend pages will load

For systems that use dynamic allocation of lockers to users, the Analytics page will provide the average and peak duration of use which can help tune the default locker reservation length.

The Settings tab contains links to the backend system configuration (for example to create new administrator accounts, or to perform bulk imports of users and card numbers). This will require additional authentication to reach these pages. The tab may also link to the Parcel delivery module and floorplan tools for systems that have those features enabled. Finally this tab contains the Administrator logout button.

3.3 Locker Administration



Lockers Tab selected

Administer Users

View existing reservations

Create groups of lockers and apply different policy to them

Realtime analytics and access to backend reporting module

Settings includes creating new Administrators and other functions

Desk icon present if floorsense system is also installed

Select and filter locker banks by building and or level within a building

Action panel for the selected locker 121

OVERVIEW
Key: 121
Type: Top
Group Name:
Online: ✓
Mapped: ✓
Enabled: ✓
USB Charger: OFF

RESERVATION
User: Taiki Yoshino
Type: fixed
Started: 26/6/18 9:03 am
Ending: 19/1/38 4:14 pm

HARDWARE
RX: 57445
TX: 133
Firmware: 1.30 Boot: 1.10

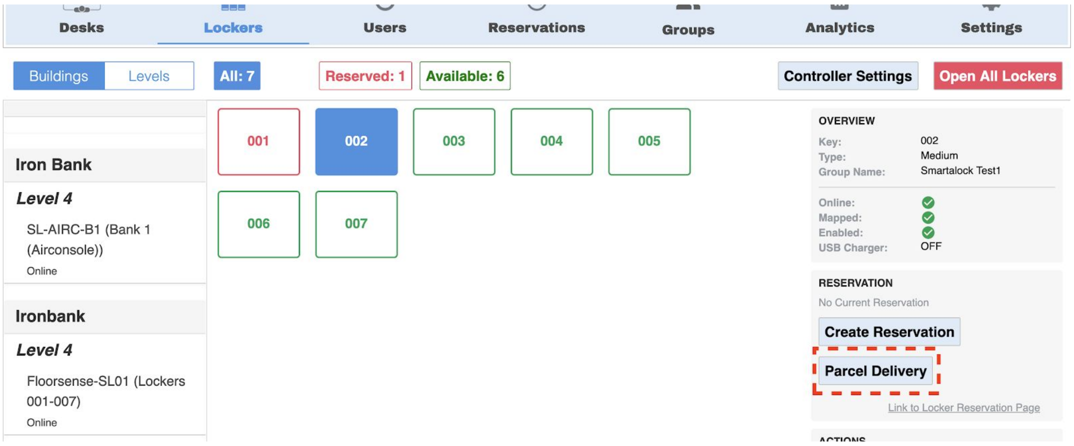
The Locker tab allows the Administrator to perform locker specific actions. The most common actions are viewing who is currently assigned this locker, what type of locker it is (if different locker types have been setup) and remotely opening the locker door (in the case where the user has lost their card and/or forgotten their PIN).

Like all tabs within the web user interface, actions are performed from the left of screen to right.

- 1) select the locker bank where the locker is located from the list of locker banks
- 2) Select a locker from within the bank. The Squares indicate the locker number within the bank. Red squares are currently reserved lockers, green are free.
- 3) in the Action panel, perform the required action.

If the locker is green, the Administrator can quickly create a reservation for an existing user without leaving the screen via the “Create Reservation” button.

A locker can also be designated as a temporary storage for packages. The “Parcel Delivery” button can be clicked and a Package Delivery Quick Form will pop up. After the form has been filled, a short message will be sent to the user’s email address consisting of a QR code to open the specific locker.



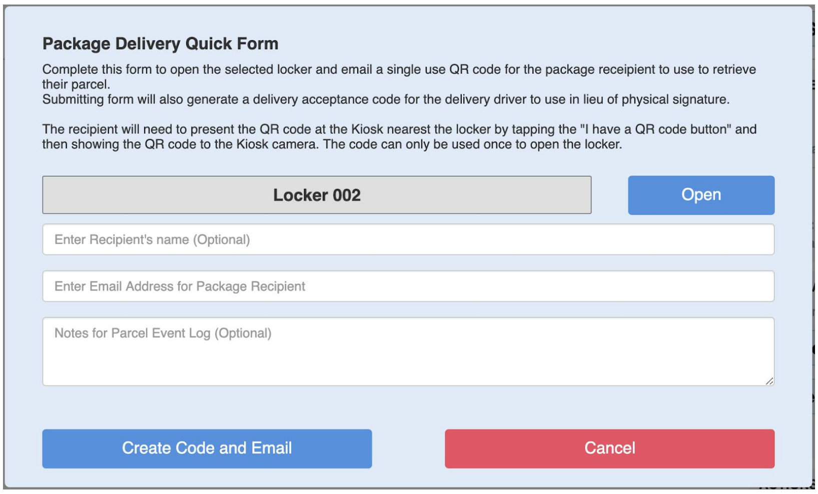
Iron Bank
Level 4
SL-AIRC-B1 (Bank 1 (Airconsole))
Online

Ironbank
Level 4
Floorsense-SL01 (Lockers 001-007)
Online

OVERVIEW

Key:	002
Type:	Medium
Group Name:	Smartalock Test1
Online:	✓
Mapped:	✓
Enabled:	✓
USB Charger:	OFF

RESERVATION
No Current Reservation



Package Delivery Quick Form

Complete this form to open the selected locker and email a single use QR code for the package receipient to use to retrieve their parcel.
Submitting form will also generate a delivery acceptance code for the delivery driver to use in lieu of physical signature.

The recipient will need to present the QR code at the Kiosk nearest the locker by tapping the "I have a QR code button" and then showing the QR code to the Kiosk camera. The code can only be used once to open the locker.

Locker 002

Open
Enter Recipient's name (Optional)
Enter Email Address for Package Recipient
Notes for Parcel Event Log (Optional)
Create Code and Email
Cancel

Once the recipient has received the email notification with the QR code, they would have to simply scan it on the Kiosk in order to unlock the locker and retrieve their package.

Apart from viewing the existing reservation and opening the locker door, the Admin can also perform the following functions:

Sound Buzzer - sounds the alarm within the locker - helpful for users trying to locate an unlabeled locker door that will not open for some reason, and also tests the tamper alarm.

Turn light on/off - this is the internal bright white LED. It generally automatically switches off when the locker door is closed, or after 15 seconds, but the Admin can use this action to make it stay on.

Flash indicator light - this is the front LED that may be visible if the locker system has the clear lens fitted to the locker door. This can be useful to locate an unmarked locker, or to test the light.

Reset / Disable locker - this is used to force an individual locker to reboot. There maybe times where this is required by Smartalock support.

3.3.1 Policy Setting Hierarchy

The Smartalock system has 3 different locations where a locker policy can be applied by the administrator. The policy is checked and applied when a locker reservation is created. These are checked in the below order:

- Group Level - policy that applies to a defined group of lockers which maybe either a subset of a single locker bank, or possible spans multiple locker banks. For example a group called “Visitor Lockers” may include 4 defined lockers on each of 3 different locker banks.
- Controller Level - this policy applies to all the lockers belonging to a single locker bank. There are some exceptions where a controller policy may apply to multiple locker banks that have been grouped together so that they are under the control of a single touchscreen kiosk - in this case the Controller level policy applies to all the lockers under the administration of the single touchscreen kiosk.
- Master Level - this policy applies to all the lockers in the entire system

The typical setup has the most restrictive policy at the Group level, and the most permissive at the Master level. For example a Group of lockers called “End of Trip” and the locker bank which hosts the End of Trip locker group has both a group and controller policy allowing 1 locker per user, but the Master Level policy allows 2 lockers. This would allow the user to reserve 1 End of Trip locker on a locker bank which has this group while still retaining their existing locker reservation on a different locker bank elsewhere.

Where any of these policies is in conflict, the default position is the more restrictive policy applies. For example a “Visitor” group policy may allow 2 lockers per user, whereas the controller and master policy only allow 1 locker per user. If a user that already has a locker on the system elsewhere on different locker bank attempts to create a reservation for a locker within the “Visitor” group of lockers, then while this would be acceptable to the group policy, and also the controller policy (as the users existing locker is not on this controller), the master policy would not be met so the reservation would fail with limit exceeded.

There is an alternative mode where the policy is checked in order of Group->Controller->Master and if the Group policy is met, then the reservation will be made without seeing if the new reservation will breach any other policy limits. This alternative mode can be set by Smartalock technicians by customer request.

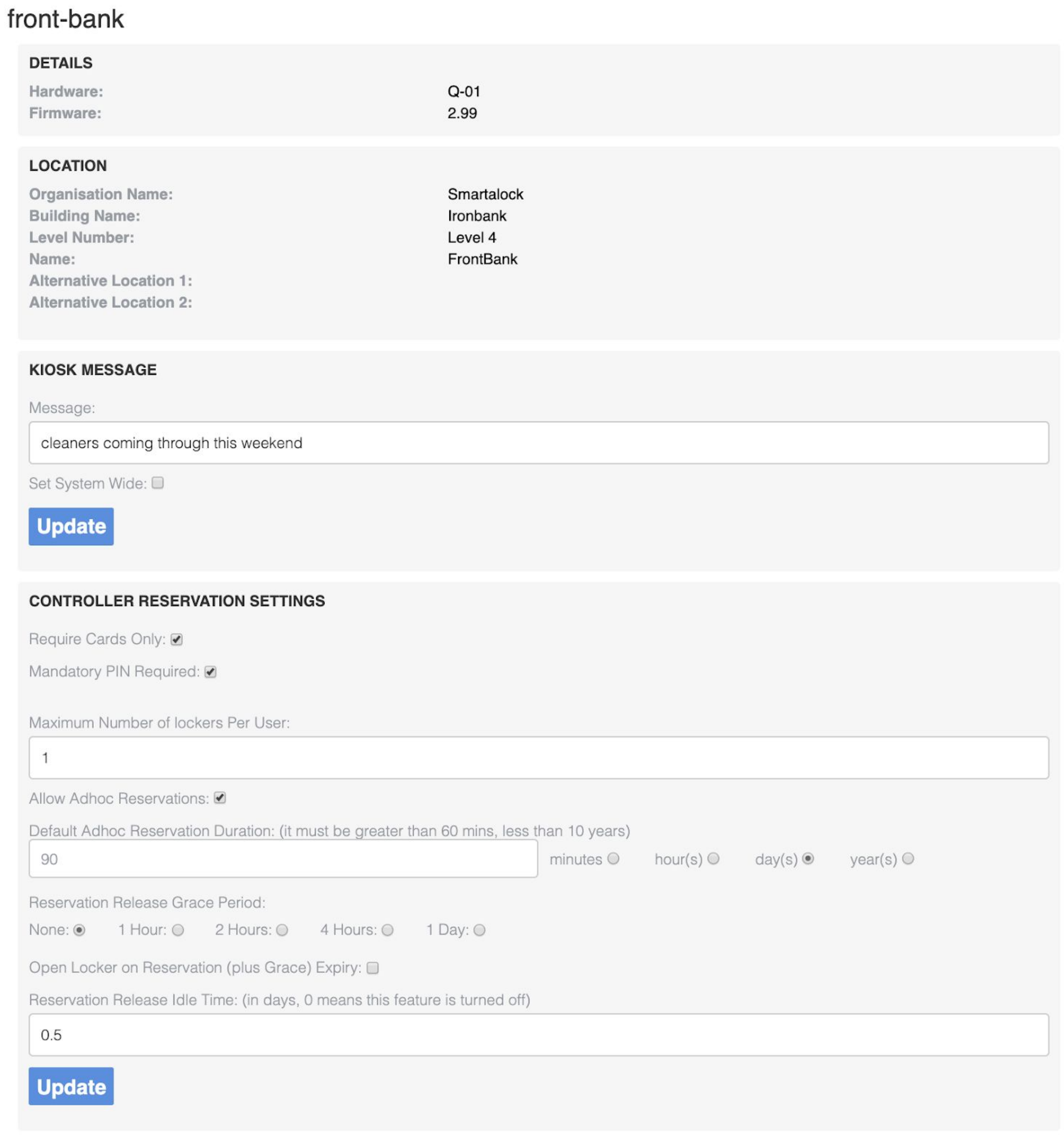
The typical policy elements for lockers include

- The number of lockers a single user can have
- Whether the lockers can be dynamically reserved on demand (ie adhoc) vs the Administrator performing the locker allocation to the user
- If Adhoc reservations are allowed, what is the reservation length
- Is there a grace period where the user can still open the locker one final time, even if the reservation has expired

- Should a locker reservation automatically be released if the user hasn't used the locker for a long time (idle time)

3.3.2 Controller Policy Settings

Tapping on Controller Settings takes Admin to a page where the individual locker bank controller policy settings can be adjusted.



front-bank

DETAILS

Hardware: Q-01

Firmware: 2.99

LOCATION

Organisation Name: Smartalock

Building Name: Ironbank

Level Number: Level 4

Name: FrontBank

Alternative Location 1:

Alternative Location 2:

KIOSK MESSAGE

Message: cleaners coming through this weekend

Set System Wide: □

CONTROLLER RESERVATION SETTINGS

Require Cards Only: ☑

Mandatory PIN Required: ☑

Maximum Number of lockers Per User: 1

Allow Adhoc Reservations: ☑

Default Adhoc Reservation Duration: (it must be greater than 60 mins, less than 10 years)

90 minutes ○ hour(s) ○ day(s) ● year(s) ○

Reservation Release Grace Period:

None: ● 1 Hour: ○ 2 Hours: ○ 4 Hours: ○ 1 Day: ○

Open Locker on Reservation (plus Grace) Expiry: □

Reservation Release Idle Time: (in days, 0 means this feature is turned off)

0.5

The most common setting to change is the Kiosk Message. This is the message that is shown on the screen of the locker kiosk when a user is not interacting with it. This can be set to anything such as "Locker Cleaning this weekend, Please clear lockers on Friday", or "See Joanne for tickets to Auckland Blues game" - it is a free text field designed to be used as a simple staff broadcast message location to all users that will pass by the locker bank during the day.

Note that the message will actually update on the locker kiosk screen after 1 interaction by a user - such as swiping a card to open locker, or simply touching the screen. If no users interact with the locker bank then the previous message will still be shown.

Other **locker bank specific settings** can also be changed on this screen. These are covered in the below table. Note that even if the locker bank settings such as “Maximum Lockers = 2” are configured, these could be overridden by a group or master policy depending on how the system is configured for policy hierarchy.

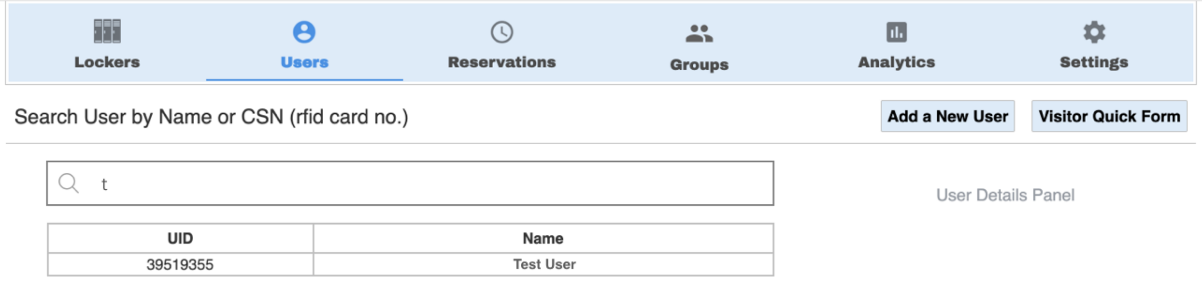
Setting	Default	Description
Allow Adhoc Reservations	On	Allows any user to obtain a locker by swiping card or tapping the Get a Locker button on the Kiosk. A locker will be dynamically allocated from the pool of currently unallocated lockers.
Require Cards Only	Off	The Get-a-Locker button is not shown on the kiosk screen, meaning only users with a valid swipe card will be able to dynamically obtain a free locker
Mandatory Pin Required	Off	The system will not dynamically allocate the user a locker until they also create and confirm a 4 digit PIN number at the time of locker allocation. This setting is designed to reduce the Admin overhead for users losing their swipe cards or locking their swipe cards in their lockers. If a PIN is set when the locker is allocated, then this can also be used to reopen the locker door
Maximum Lockers per User	2	The maximum number of lockers any single user can have at any one time over all connected locker banks.
Default Duration of Reservation	1 Day	For Adhoc (dynamic) locker allocations, this is the default length that the locker will be allocated to the user. After this time expires, if the reservation has not been released by the user, then various options are available to the Admin for handling - discussed below. Note this does not apply to Fixed allocations which last forever or until they

		are manually released by the Admin
Grace Period	None	This is an additional not disclosed period of time where after the adhoc reservation expires that the user will still be able to open their locker 1 more time to clear their locker contents.
Open door on reservation expiry	No	Admin can automatically open the locker door if the reservation expires before the user has released the locker. This is often used in universities where lockers are in high demand and the next user will empty an expired but full locker into a lost property bin. For corporate / gym deployments generally this is disabled and the user must contact the admin to open the locker if it has expired.

3.4 User Administration

The User tab allows the Admin to search for and administer existing users, along with creating new users individually or performing a bulk import of users from an external database.

Because the Master server may have tens of thousands of users, the initial User tab screen requires the Admin to enter some search terms such as a single letter to start finding users. Users can also be searched via their swipe card number.



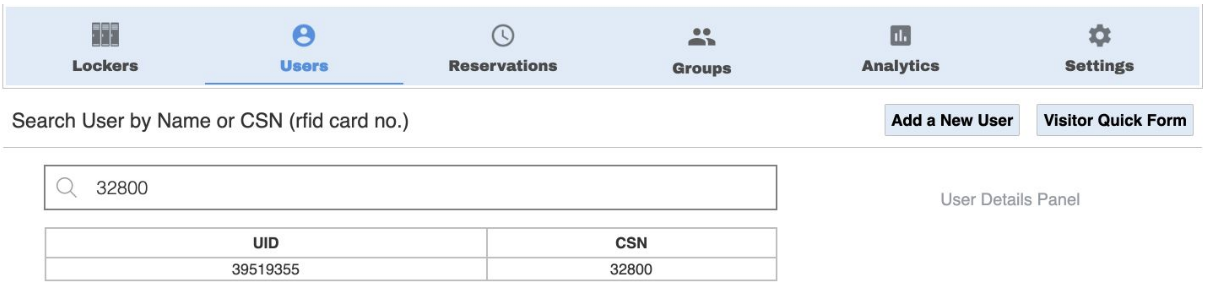
Search User by Name or CSN (rfid card no.)

t

UID	Name
39519355	Test User

Entering for example “t” will return all users with an “t” in their name. Note this is not case sensitive. The maximum results returned in a user search is 200, so more letters in the users name maybe required to find a user where the database is very large.

Searching by users building card number (CSN) requires the **full number to match** before any search results are returned.

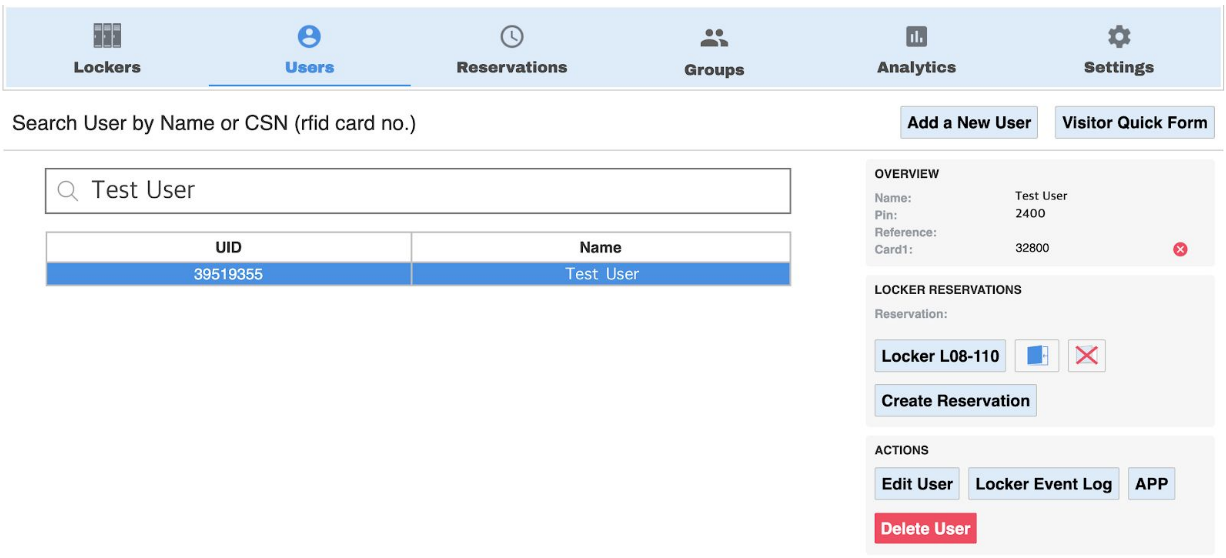


Search User by Name or CSN (rfid card no.)

32800

UID	CSN
39519355	32800

Tapping on a users name or UID will return their current locker reservations and other details if available.



UID	Name
39519355	Test User

OVERVIEW

Name: Test User
Pin: 2400
Reference:
Card1: 32800

LOCKER RESERVATIONS

Reservation:

ACTIONS

The above example shows a user with an existing locker allocated. On the right panel, the Overview, Locker Reservations, and Actions tab can be seen. The Overview shows general details of the selected user such as their name, the allocated pin for their locker, and their designated reference card (CSN).

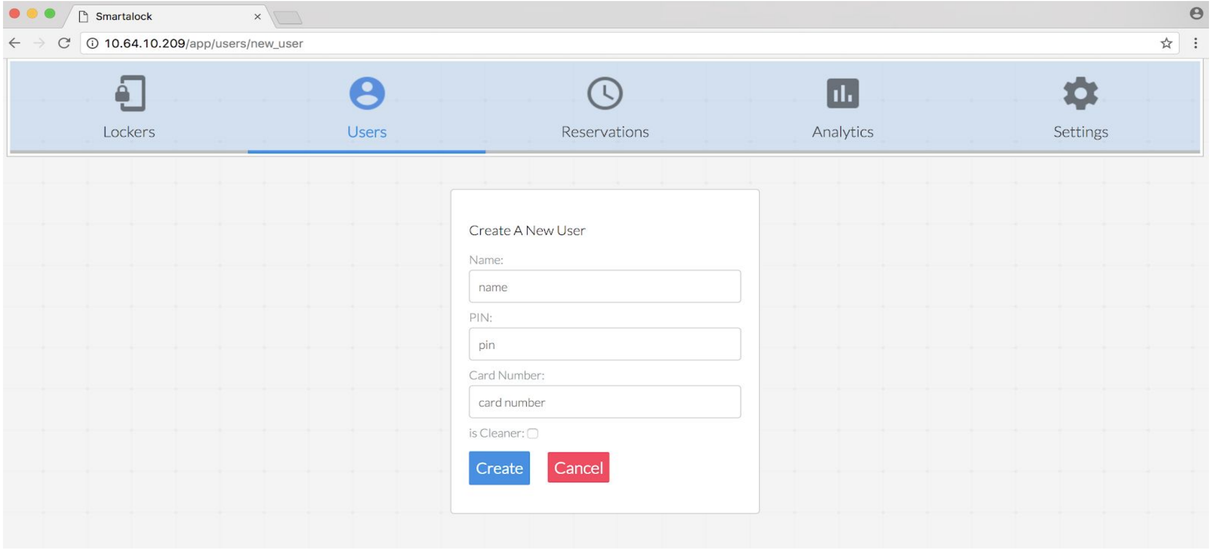
Under the Locker Reservations tab, the locker assigned to the user can be seen, in this case locker “L08-110”. The ◧ icon opens the specific locker, and the ✕ icon de-allocates the user from the current locker. Create Reservation will take the Admin to the Reservations tab with this user selected.

Under the Actions tab, clicking Edit User allows for changing the user’s name, PIN, and associated card number. Clicking on the Locker Event Log leads to a page consisting of the time logs a user has opened or closed the lockers.

Clicking on the APP leads to a page consisting of the QR code, Setup Code, and Activation Link of a specific locker which can be sent to the user by the Administrator. If Delete User is clicked, it will delete the user, along with any locker reservations they currently have.

3.4.1 Creating New Users

Tapping on Add a New User will bring up a modal window where a new user can be created. A new user just needs to have a name, however can also be allocated a PIN number and Swipe card at the same time.



Create A New User

Name:

name

PIN:

pin

Card Number:

card number

is Cleaner: □

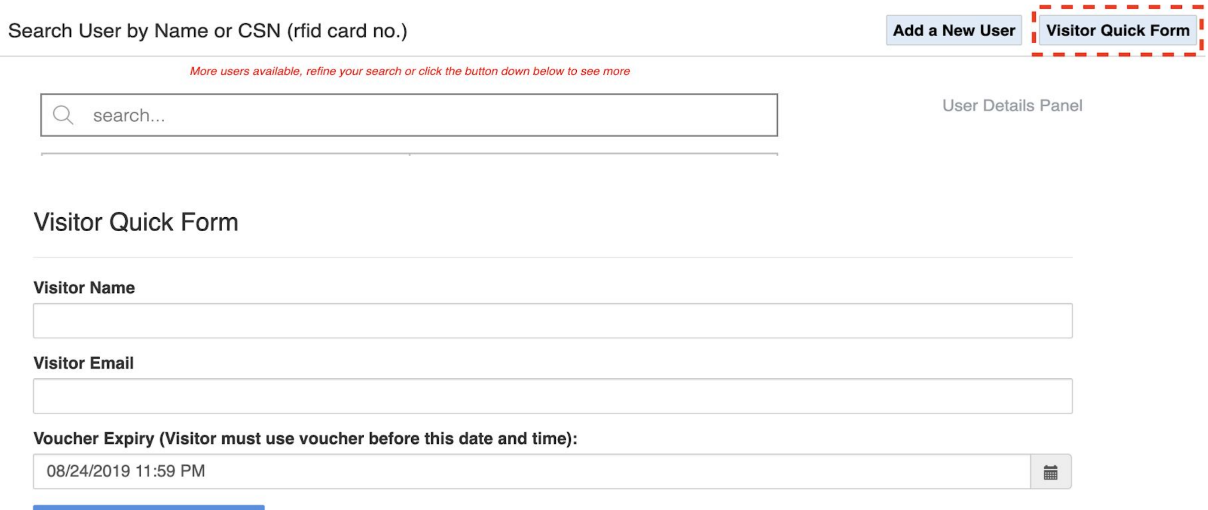
The Card Number field can be populated by scanning the users card onto a card reader supplied by Smartalock. This card reader should be attached to the PC or Mac where the Administrator is accessing the web interface. The card reader behaves just like a keyboard in that when a card is presented, it “types” the card number wherever the cursor is located.

The USB card reader is provided by Smartalock and will have been pre-tuned to return the same number format as would be returned by the Kiosk integrated card readers. It is important to not use any other card reader as the number format will most likely not match.

The “Is Cleaner” tickbox denotes this user as a special type of user who does not have a locker themselves, however their swipe card can open ALL the lockers in any single locker bank. Cleaners are required to have swipe cards - they cannot open all lockers with a PIN.

3.4.2 Visitor Quick Form

Clicking on Visitor Quick Form on the top right corner brings up a page where the administrator can add a visitor on site to the system for a period of time.


Search User by Name or CSN (rfid card no.)

More users available, refine your search or click the button down below to see more

search...

User Details Panel

Visitor Quick Form

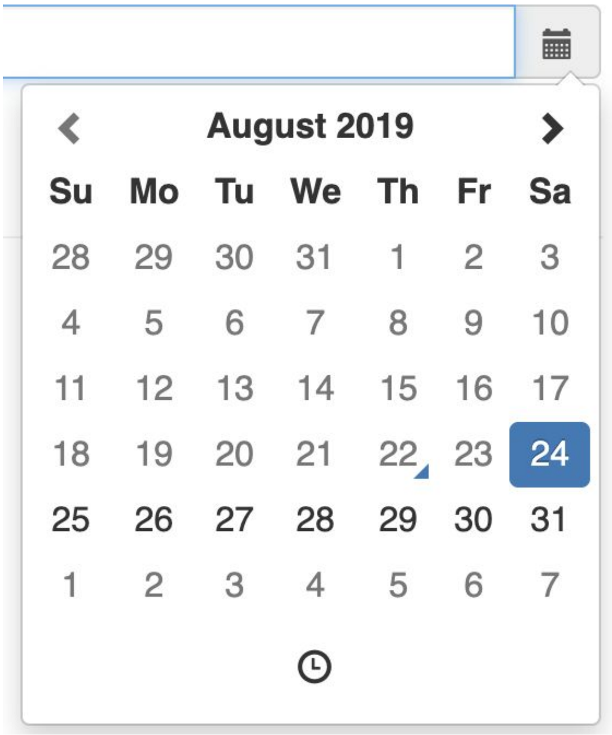
Visitor Name

Visitor Email

Voucher Expiry (Visitor must use voucher before this date and time):

08/24/2019 11:59 PM

Once the name and email fields have been filled, the administrator can then set the expiry date of this voucher by clicking on the calendar button 📅 ,which brings up an interactive calendar.



‹ August 2019 ›

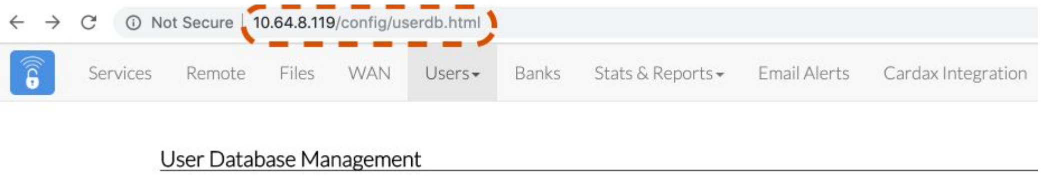
Su	Mo	Tu	We	Th	Fr	Sa
28	29	30	31	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31
1	2	3	4	5	6	7

Once the expiry date and time have been set, the administrator can then click on the “Create Voucher and Email” button which will send a notification and QR code to the visitor’s email address. In addition, this visitor will also be added to the database temporarily. The visitor can then use this QR code to open their designated locker via the kiosk.

3.4.3 Bulk Importing Users into System

Alternatively, users can be uploaded into the database in a bulk manner. A full guide on this can be found in the following link: http://support.smartalock.com/support/solutions/articles/5000746346-smartalock-integration-guide-for-3rd-party-card-systems.

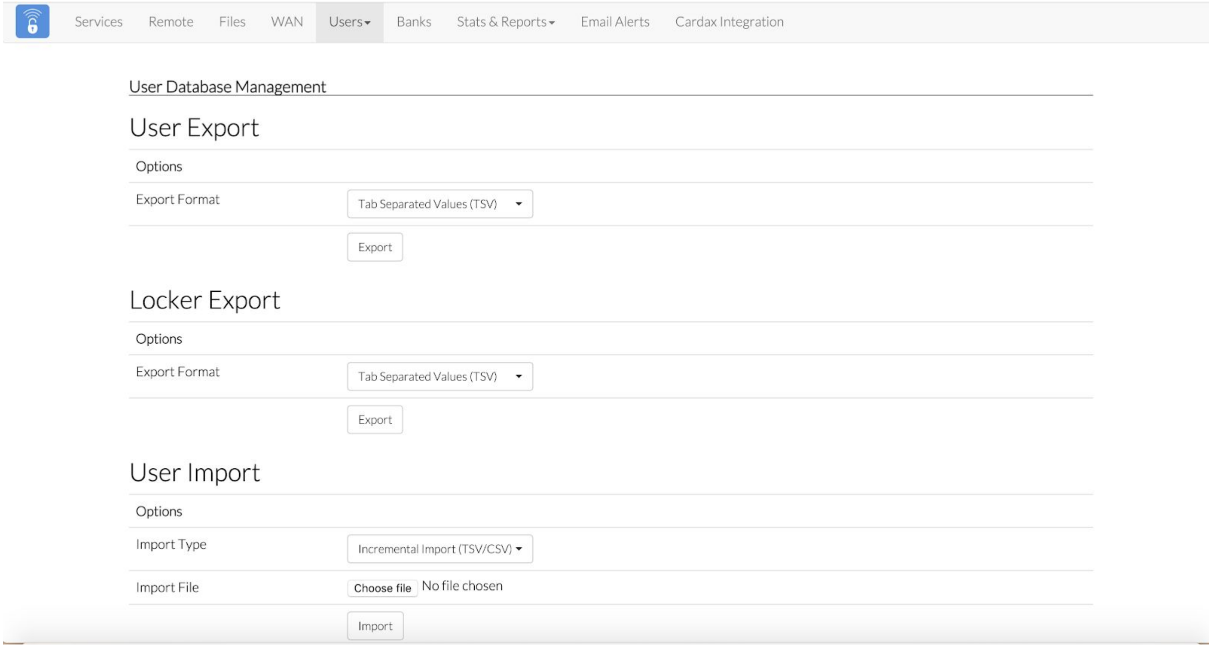
This feature can be accessed by typing the IP address of the master, followed by “config/userdb.html”. An example is as follows:



Not Secure 10.64.8.119/config/userdb.html

User Database Management

The following image shows the interface of the User Database Management page.



User Database Management

User Export

Options

Export Format: Tab Separated Values (TSV)

Export

Locker Export

Options

Export Format: Tab Separated Values (TSV)

Export

User Import

Options

Import Type: Incremental Import (TSV/CSV)

Import File: Choose file No file chosen

Import

The administrator will be able to access the following three tabs; User Export, Locker Export, and User Import.

The User Export section allows the administrator to export the current database, and only as a Tab-Separated Text File (.TSV). This TSV file can be edited manually and uploaded back into the database in the same file format, further explained later in the User Import section.

The Locker Export section is similar to the User Export, with the exception that it consists of the list of lockers, and the users currently assigned to them. This section however, can be ignored as it is irrelevant to the database management system.

Under the User Import section, two types of import can be chosen under Import Type:

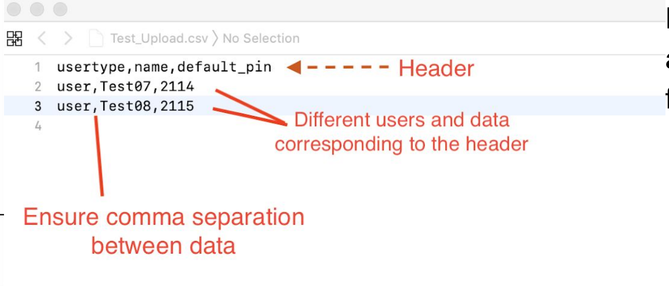
- **Incremental Import**: New users are added onto the database without altering existing ones, based on the TSV/CSV file's contents. An admin can export the existing database, add new users into it, and reupload the same file. They can also create a new CSV/TSV file with the same header format as the existing database, and upload it into the system.
- **Full Import:** This type of import completely replaces the existing database, with the one being imported. Any header formats or existing data will be overwritten.

Regardless of the import type, either a Tab-Separated Text File (.TSV) or a Comma-Separated Text File (.CSV) can only be imported into the database. By default, the system recognizes the following header formats for both CSV and TSV files:

usertype	name	firstname	lastname	default_pin	reference	mobilekey	expiry	cards	res_fixed	res_adhoc

If none of these headers are present, the system assumes that the database is in the above order for each line of users. If the headers are specified, only the “usertype”, and one of the “name”, “firstname”, “lastname”, “reference”, or “cards” fields will be necessary to create a user, while the other fields can be left blank. The following describes the fields above:

Field	Required?	Description
usertype	Required if no header row specified	Must be present and value for all rows is “**user**”
name	Either name or firstname/lastname must be populated	contains the users full name (as displayed by Smartalock) [note: for systems that cannot export full name in a single column, use firstname/lastname]
firstname	Either name or firstname/lastname must be populated	Contains the users firstname(s)
lastname	Either name or firstname/lastname must be populated	Contains the users lastname
default_pin	Optional	the user's default PIN to be used for new reservations - if specified then this will reset any user reservations to use this PIN, if not specified **and** this is a new user, a PIN will be automatically generated. If not specified and this is existing user, then PIN will not change.
reference	Optional	a reference into the customer's system - e.g. an employee number. This field is optional but see below for how import rows are matched to existing user records.
mobilekey	Optional	a system generated UUID that links this user record to the user's mobile phone app. If this is an existing user and this field is blank, the existing user's mobile key is not altered
expiry	Optional	a user expiry date after which a user record and associated cards and reservations will be deleted. Currently not implemented in Master software, but will be in later versions.
cards	Optional	A pipe separated list of card serial numbers (CSNs) associated with this user. If populated will replace current CSNs. Use "-" to delete existing cards and leave blank to retain existing list of cards
res_fixed	Optional	a pipe separated list of lockers to permanently reserve for this user. The locker format is
res_adhoc	Optional	

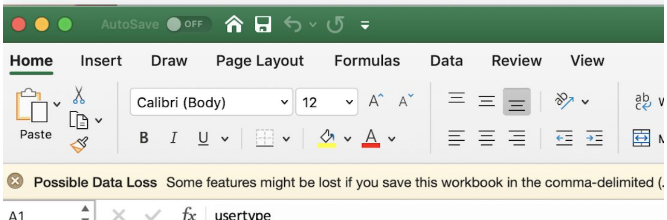

Test_Upload.csv 〉No Selection

```
usertype,name,default_pin
user,Test07,2114
user,Test08,2115
```

Header
Different users and data corresponding to the header
Ensure comma separation between data

Example of a valid CSV file:

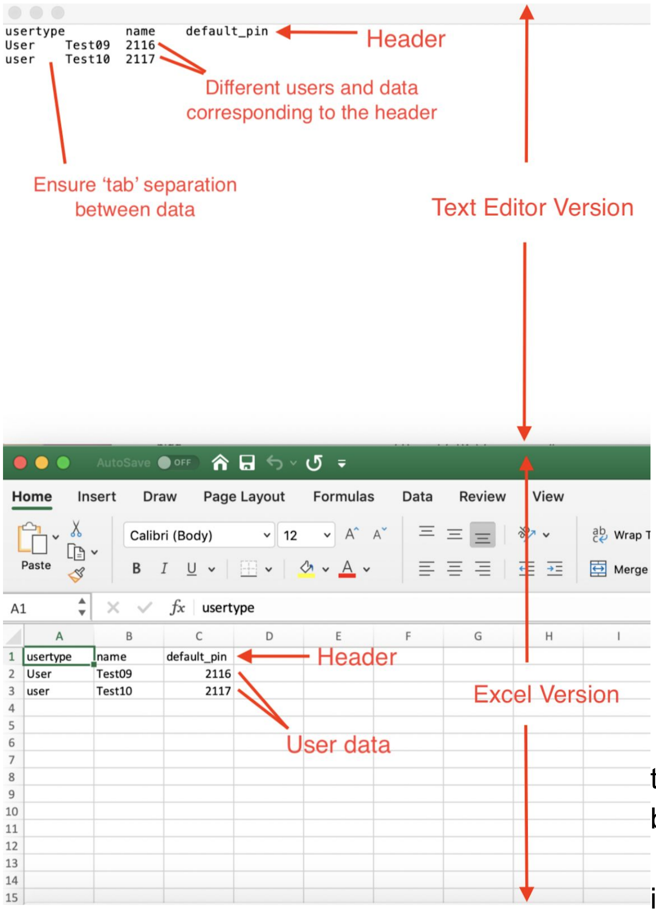
Text Editor version



Possible Data Loss Some features might be lost if you save this workbook in the comma-delimited (.

usertype

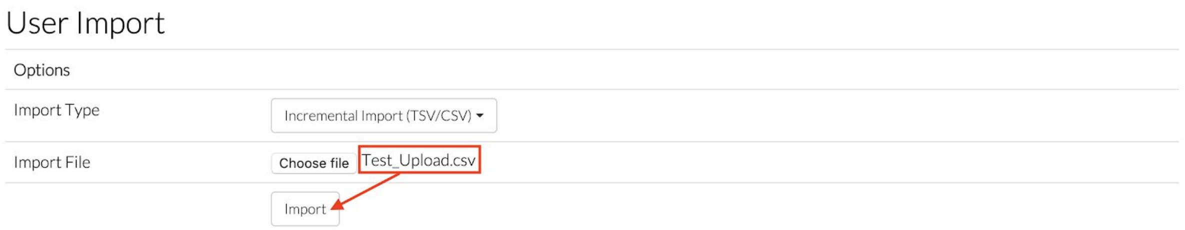
Example of a valid TSV file:



```
usertype        name    default_pin
User    Test09  2116
user    Test10  2117
```

	A	B	C
1	usertype	name	default_pin
2	User	Test09	2116
3	user	Test10	2117

It is recommended to export the existing database first as a backup before starting the process. If the administrator is ready to import their file, they can click the “Choose File” button to upload the database, followed by the “Import” button to start the importing process.



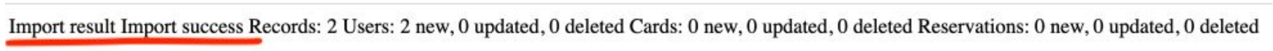
User Import

Options

Import Type: Incremental Import (TSV/CSV)

Import File: Test_Upload.csv

If an import was successful, the following message should appear:



Import result Import success Records: 2 Users: 2 new, 0 updated, 0 deleted Cards: 0 new, 0 updated, 0 deleted Reservations: 0 new, 0 updated, 0 deleted

To double check the changes, the new database can be exported.

Alternatively, the import process can be done using a Shell based command line from their terminal. This method is favourable if the customer plans on adding their own automated process.

1. Copy the CSV/TSV file into the master using the *scp* command:
   scp FileName root@MasterIpAddress:

   Replacing FileName with the full file name of your CSV/TSV file, and MasterIPAddress with the master's designated IP Address. Ensure the colon ":" is placed at the end of the command to ensure that the file's name remains the same when copied onto the master.

2. Next, log into the master using the *SSH* command:
   ssh root@MasterIpAddress

   Like in step 1, replace MasterIpAddress with the corresponding master's IP Address.

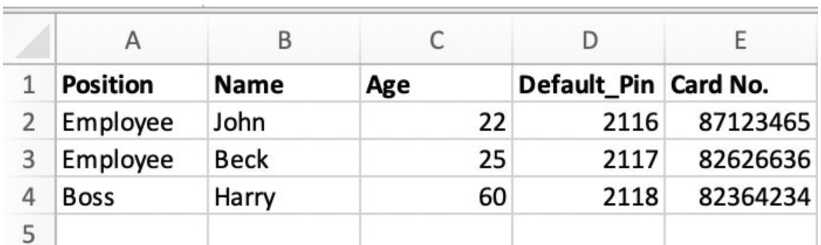
3. Lastly, run the *sladmin import* command to initiate the importing process using either:
   sladmin import -f FileName
   OR
   sladmin import -f FileName -l

   Where FileName is replaced by the file's full name. The first command runs the Incremental Import, while the second command runs the Full Import.

If the administrator wishes to upload a database exported from their system, they would have to configure the master using the terminal. **NOTE:** The exported data would have to be in data form; i.e. without any column headers, just the user data.

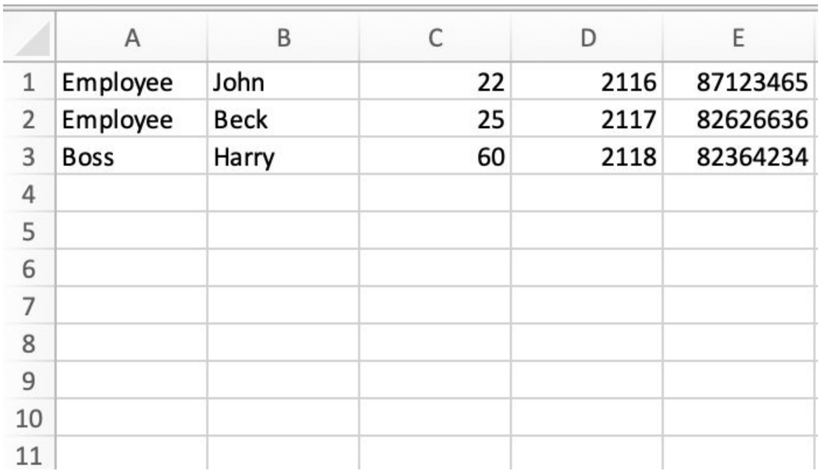
Using the NVRAM command, the master is able to create an empty buffer with column headers that match the exported data. An example is as follows.

Given the following exported data (from a TSV file) :



	A	B	C	D	E
1	**Position**	**Name**	**Age**	**Default_Pin**	**Card No.**
2	Employee	John	22	2116	87123465
3	Employee	Beck	25	2117	82626636
4	Boss	Harry	60	2118	82364234
5					

The column headers can be omitted either through excel or text editor, giving the following result:



	A	B	C	D	E
1	Employee	John	22	2116	87123465
2	Employee	Beck	25	2117	82626636
3	Boss	Harry	60	2118	82364234
4					
5					
6					
7					
8					
9					
10					
11					

Using a terminal, SSH into the master with the following command:

```
ssh root@MasterIpAddress
```

Replacing ‘MasterIpAddress’ with the designated master controller’s IP address.

Once in the master’s root directory, execute the following command:

```
nvram set import_columns=column1,column2,…..columnX
```

Replace ‘column1,column2…..columnX’ with the header columns that were omitted previously. Given the current example, this would be:

```
nvram set import_columns=Position,name,Age,default_pin,cards
```

Notice that variables *name*, *default_pin*, and *cards* are slightly different from the initial column headers. This is because they have been renamed to match the column headers that the master recognizes. Once the command has been executed, either one of the importing steps above can be used.

3.4.4 Smartphone App

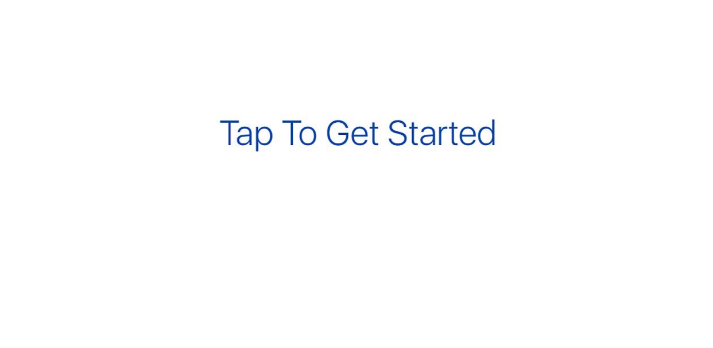
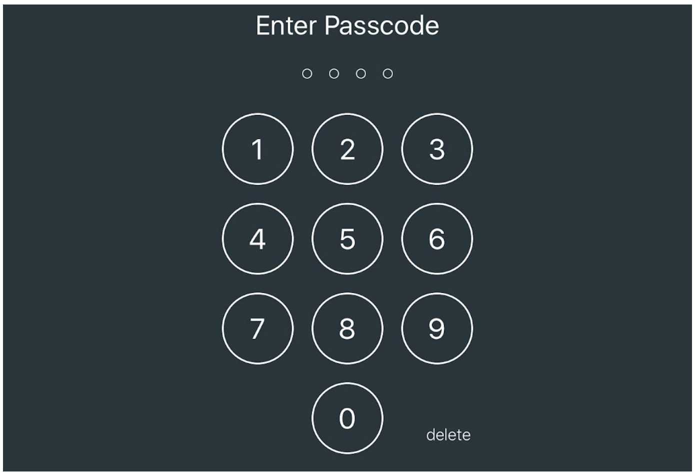
It is possible for a user created on the system, which has an existing locker allocation to link the Smartalock App to their user account. Once linked, an end user can open their locker(s) via their Smartphone in addition to or instead of using their Swipe card or PIN number.

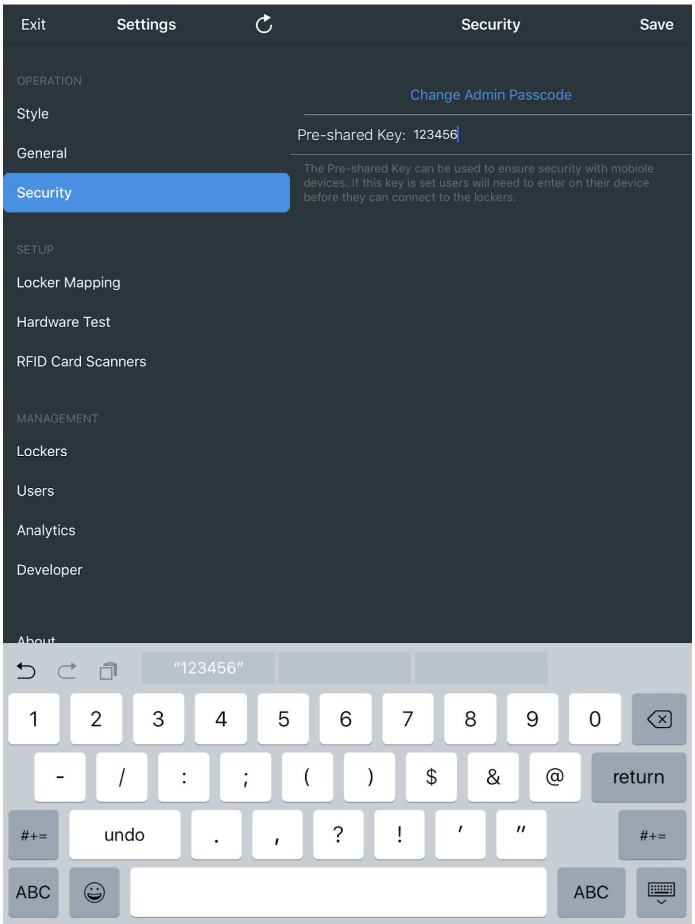
Enrolling users smartphones to link to their user account is not performed on the Master web interface by the Administrator, rather it is a self-service function that users can perform on their smartphone when standing next to the Kiosk where they have been assigned a locker.

The use of the Smartalock App including initial enrollment is contained in the **Smartalock App End User Guide** available from: http://support.smartalock.com/support/solutions/articles/5000708456-smartalock-mobile-app-user-guide .

The Administrator does not need to perform any configuration to enable smartphone use, however should the Administrator wish to secure access to any locker bank then a site code (password) can be added to each locker bank to require app users to enter this code prior to being able to connect via Bluetooth to any given locker bank.

To Set the site code to restrict Smartalock App use to just users that know the code, login to the Kiosk Admin interface and follow below workflow:

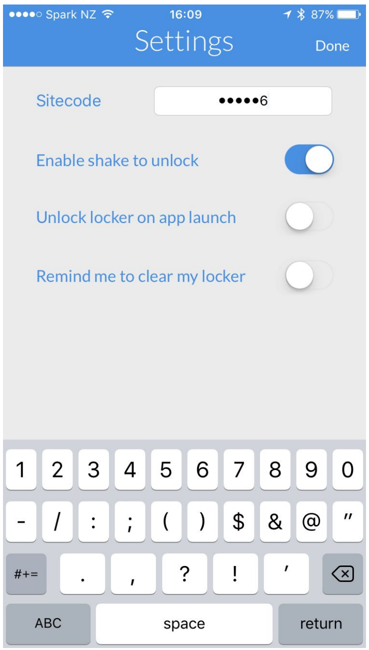
 Tap To Get Started	To enter Administrator mode, first wait unit the Kiosk Lock Screen appears. The screen will be all blue or white and say "Tap to Get Started" at the top. When this screen is visible firmly tap **twice** on the **center** of the screen
 Enter Passcode	If double tap was successful the screen will turn black and a PIN pad will appear. Enter the Administrators PIN code. By default this is **5555**



Pre-shared Key: 123456

The Pre-shared Key can be used to ensure security with mobiole devices. If this key is set users will need to enter on their device before they can connect to the lockers.

Tap the "**Security**" tab on the left hand side, and then tap the **Pre-shared key** box and enter a password in this field. The key can be a mixture of letters and numbers. Then tap **Save**



Sitecode ●●●●●6

Enable shake to unlock: ●

Unlock locker on app launch: ○

Remind me to clear my locker: ○

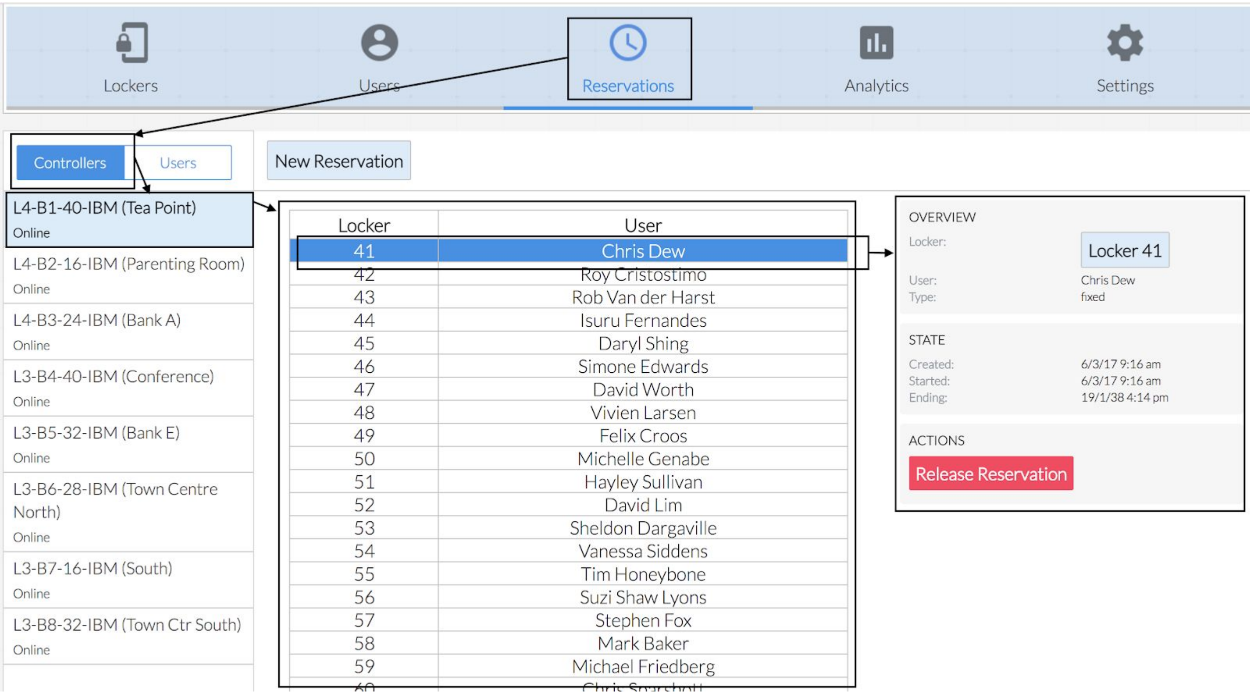
In the Smartalock App, the user will need to enter the same Pre-shared key into the "Site Code" box in the App settings.

The site code is currently set on each Locker bank via the Kiosk

3.5 Locker Reservations

The Reservation tab allows the Admin to create and release locker reservations for users. As with the Locker tab, the workflow for this page works from left to right, however the new reservation process can start from either a locker or user perspective.

3.5.1 Viewing and Releasing Existing Reservations from Locker Bank Perspective



L4-B1-40-IBM (Tea Point)
Online

L4-B2-16-IBM (Parenting Room)
Online

L4-B3-24-IBM (Bank A)
Online

L3-B4-40-IBM (Conference)
Online

L3-B5-32-IBM (Bank E)
Online

L3-B6-28-IBM (Town Centre North)
Online

L3-B7-16-IBM (South)
Online

L3-B8-32-IBM (Town Ctr South)
Online

Locker	User
41	Chris Dew
42	Roy Cristostimo
43	Rob Van der Harst
44	Isuru Fernandes
45	Daryl Shing
46	Simone Edwards
47	David Worth
48	Vivien Larsen
49	Felix Croos
50	Michelle Genabe
51	Hayley Sullivan
52	David Lim
53	Sheldon Dargaville
54	Vanessa Siddens
55	Tim Honeybone
56	Suzi Shaw Lyons
57	Stephen Fox
58	Mark Baker
59	Michael Friedberg

OVERVIEW

Locker: Locker 41
User: Chris Dew
Type: fixed

STATE

Created: 6/3/17 9:16 am
Started: 6/3/17 9:16 am
Ending: 19/1/38 4:14 pm

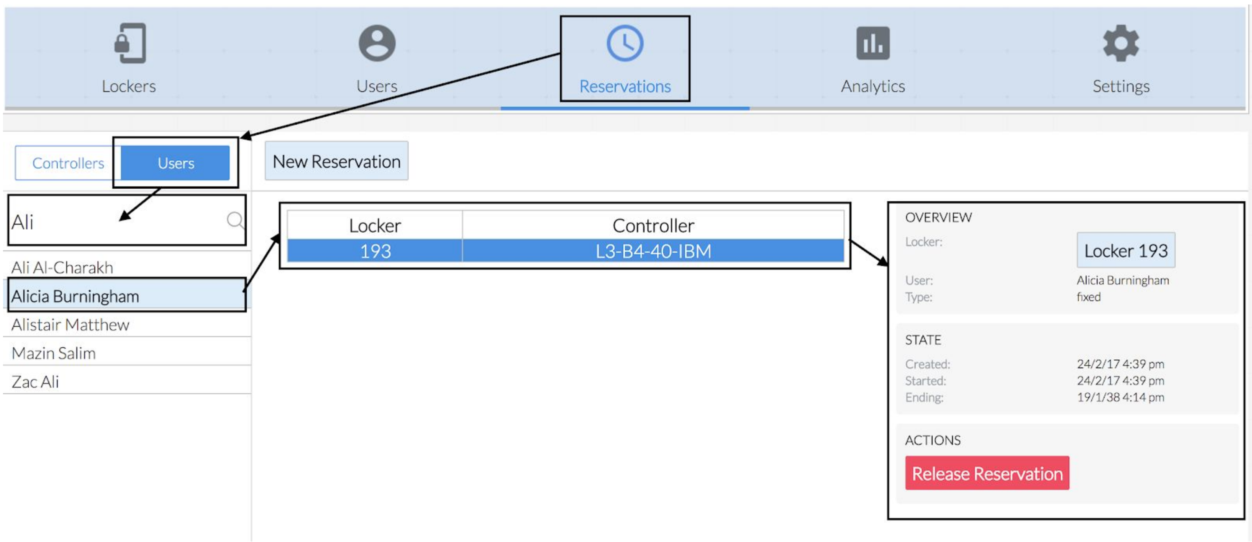
ACTIONS

To view all reservations on a single locker bank, tap the Reservations tab on the top row. The default is “Controllers” view which is each locker bank. Select a locker bank from the left hand list which will then bring up all the locker reservations for that bank. Selecting on an individual locker will populate the right hand pane with details about this particular reservation.

The right hand action panel allows for the reservation to be released from the user or clicking on the Locker button within this panel will take the Admin to the Locker details for the selected locker.

3.5.2 Viewing and Releasing Existing Reservations from User Perspective

To view all reservations which belong to a single user, tap the Reservations tab on the top row. In the left hand panel switch the view to “Users” and then start typing some of the users name and then the enter key to search for the user.



Ali

Ali Al-Charakh
Alicia Burningham
Alistair Matthew
Mazin Salim
Zac Ali

Locker	Controller
193	L3-B4-40-IBM

OVERVIEW
Locker: Locker 193
User: Alicia Burningham
Type: fixed

STATE
Created: 24/2/17 4:39 pm
Started: 24/2/17 4:39 pm
Ending: 19/1/38 4:14 pm

ACTIONS

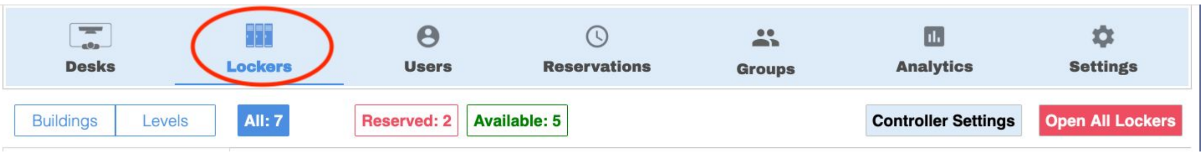
Select a user from the search results in the left hand pane will bring up their current locker reservations in the center panel. Tapping on a locker listed in the center panel will provide details in the right hand action panel.

The details include the type of reservation (Fixed vs Adhoc). Fixed Allocations will have an expiry date some 20 years from today, whereas Adhoc allocations will show an expiry date much sooner. The Adhoc (dynamic) reservation period is controlled on the individual locker bank Controller settings as described in Section 3.3.2 above - generally 1 day.

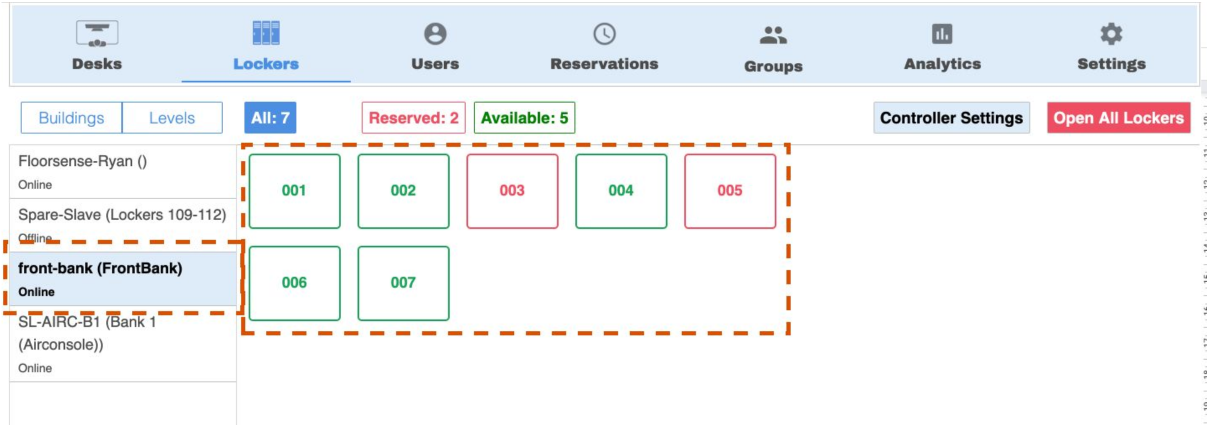
From the Action panel the reservation can be released or the locker button can be tapped to get further details on the locker itself.

3.5.3 Creating New Reservations - Method 1 (Master version > 2.6)

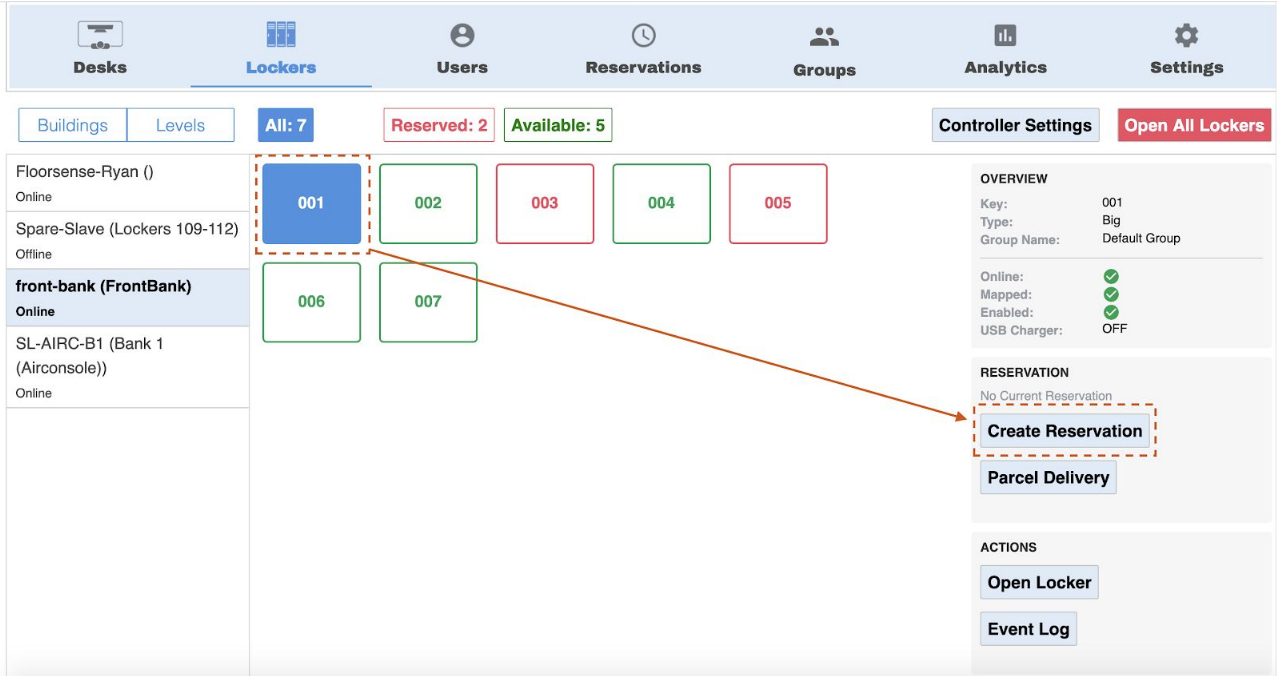
The fastest way to create reservation is via the “Locker” tab in the top panel.



Select a locker bank to bring up the locker interface.



Select a free (green) locker, and click the “Create Reservation” button on the right panel.

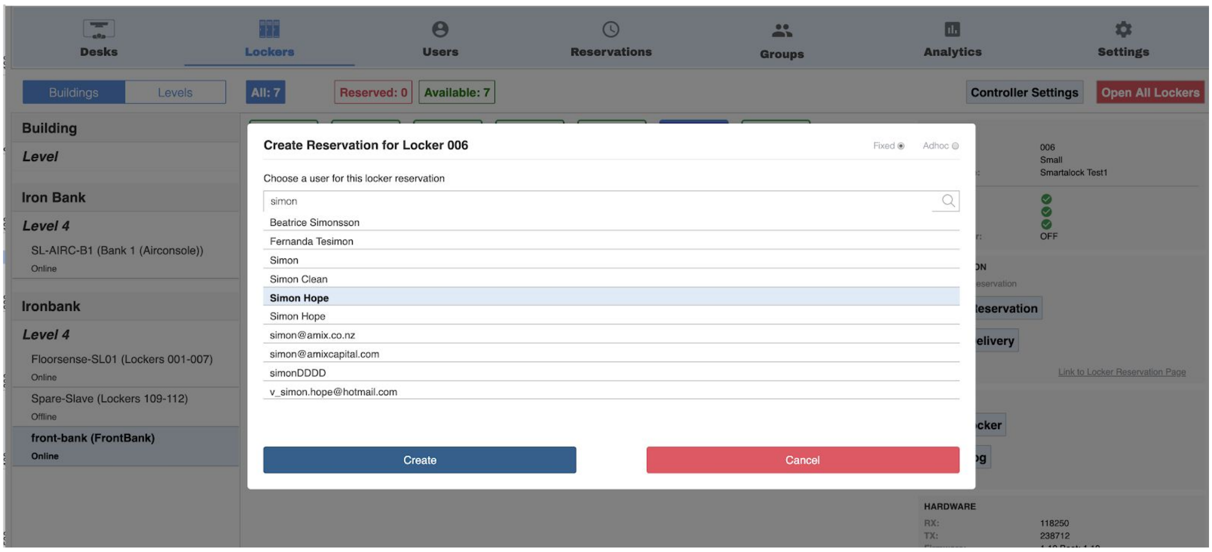


Key: 001
Type: Big
Group Name: Default Group

Online: ✓
Mapped: ✓
Enabled: ✓
USB Charger: OFF

No Current Reservation

Once clicked a pop-over appears to search for a user, highlight the selected user and then click on “Create”



Create Reservation for Locker 006

Fixed ● Adhoc ○

Choose a user for this locker reservation

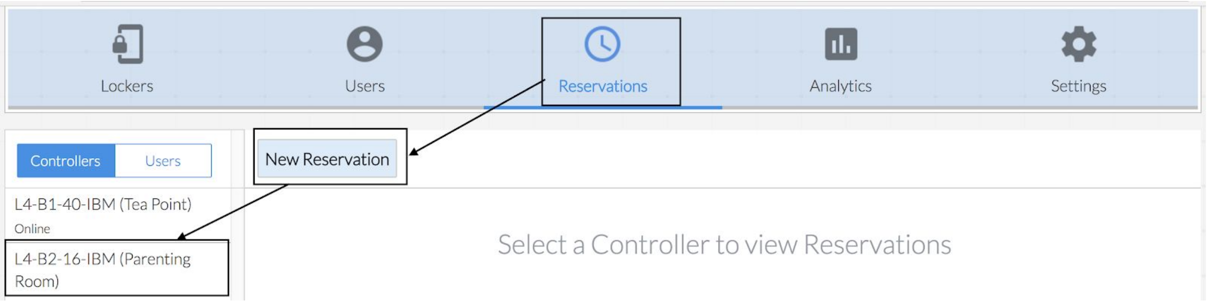
simon

Beatrice Simonsson
Fernanda Tesimon
Simon
Simon Clean
Simon Hope
Simon Hope
simon@amix.co.nz
simon@amixcapital.com
simonDDDD
v_simon.hope@hotmail.com

This method allows for creation of both fixed or adhoc locker reservations via the radio button on the top right of the popover form.

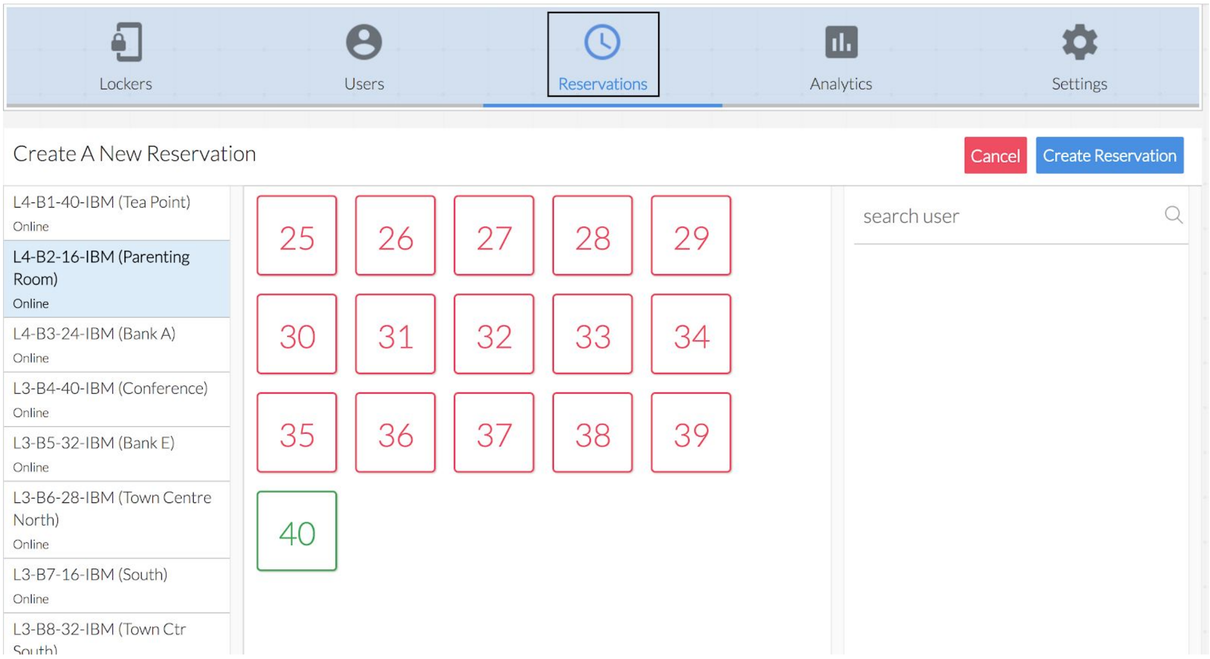
3.5.4 Creating New Reservations - Method 2 (Master version < 2.6)

For Master controllers earlier than version 2.6, the below alternative method maybe used to create new locker reservations:



To create a new locker reservation tap the New Reservations button, and then select a locker bank from the left hand panel.

The middle panel will show the lockers within the selected locker bank. Red lockers are already reserved to an existing user. Green lockers are available.



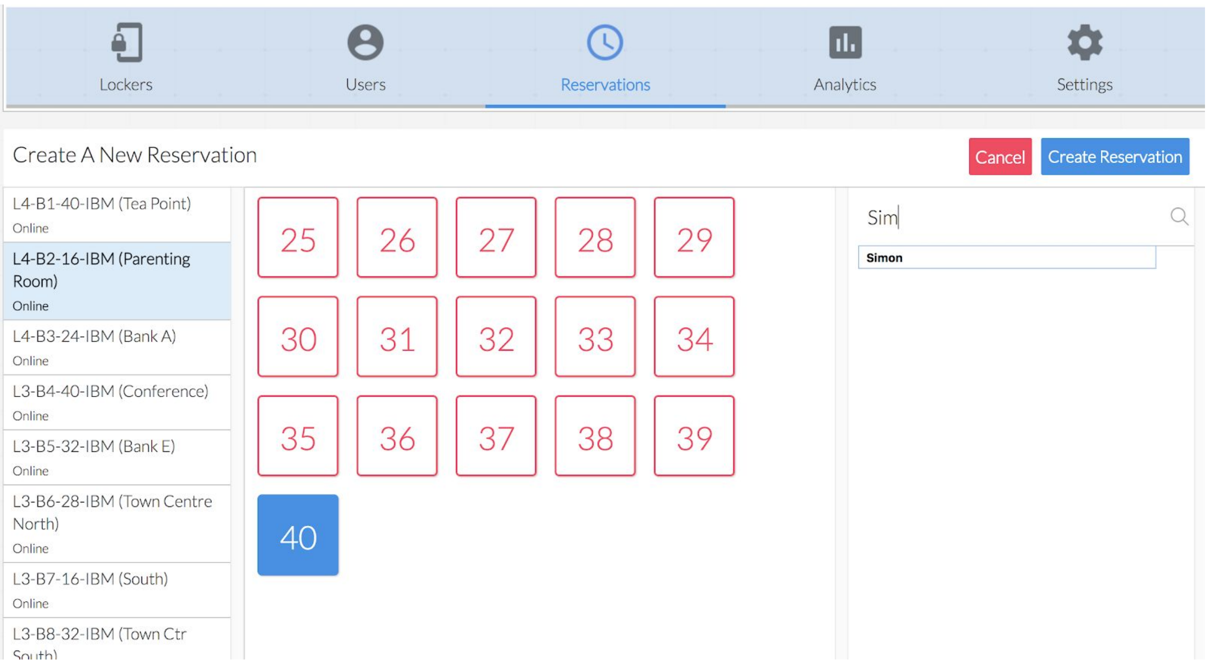
Create A New Reservation

L4-B1-40-IBM (Tea Point)
Online
L4-B2-16-IBM (Parenting Room)
Online
L4-B3-24-IBM (Bank A)
Online
L3-B4-40-IBM (Conference)
Online
L3-B5-32-IBM (Bank E)
Online
L3-B6-28-IBM (Town Centre North)
Online
L3-B7-16-IBM (South)
Online
L3-B8-32-IBM (Town Ctr South)

25 26 27 28 29
30 31 32 33 34
35 36 37 38 39
40

search user

In this example, selecting locker 40 which is free then move to the right hand panel to search for a user to assign the locker to.



Create A New Reservation

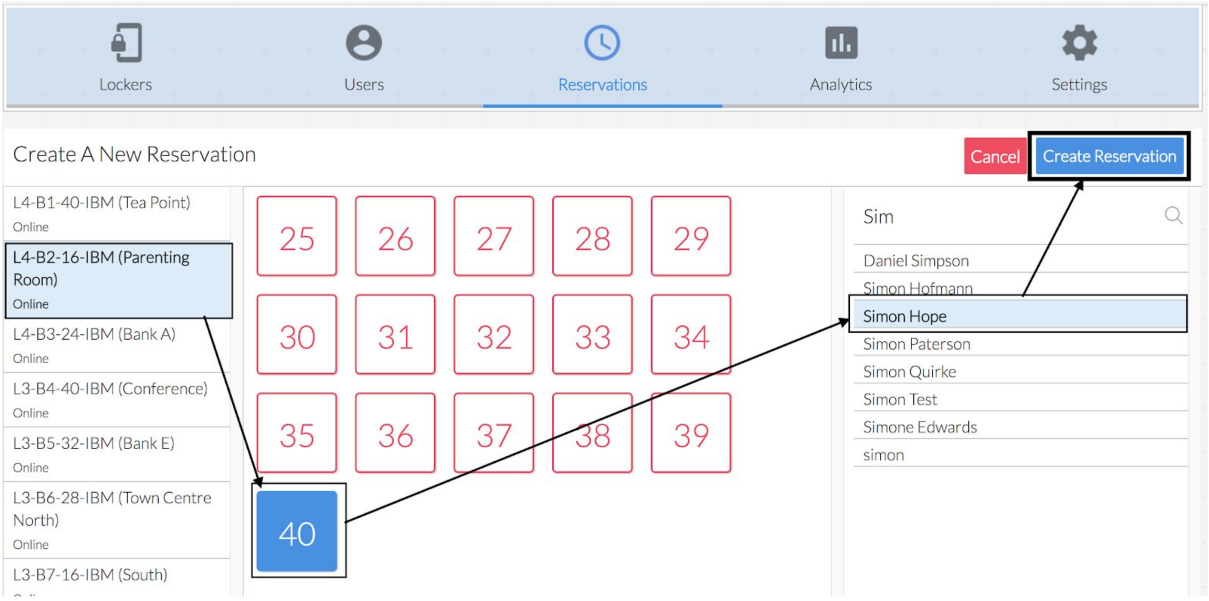
L4-B1-40-IBM (Tea Point)
Online
L4-B2-16-IBM (Parenting Room)
Online
L4-B3-24-IBM (Bank A)
Online
L3-B4-40-IBM (Conference)
Online
L3-B5-32-IBM (Bank E)
Online
L3-B6-28-IBM (Town Centre North)
Online
L3-B7-16-IBM (South)
Online
L3-B8-32-IBM (Town Ctr South)

25 26 27 28 29
30 31 32 33 34
35 36 37 38 39
40

Sim

Simon

Select the user from the search results panel and then finally tap the **Create Reservation** button. Do not forget to tap the Create Reservation button or the reservation will not be created. A confirmation modal window will display once the reservation is created.



Create A New Reservation

L4-B1-40-IBM (Tea Point)
Online

L4-B2-16-IBM (Parenting Room)
Online

L4-B3-24-IBM (Bank A)
Online

L3-B4-40-IBM (Conference)
Online

L3-B5-32-IBM (Bank E)
Online

L3-B6-28-IBM (Town Centre North)
Online

L3-B7-16-IBM (South)

Sim

Daniel Simpson
Simon Hofmann
Simon Hope
Simon Paterson
Simon Quirke
Simon Test
Simone Edwards
simon

The locker can now be opened via the users swipe card or PIN number, or if they use the Smartalock App they can open their locker via their Apple or Android smartphone if it is bound to their user account.

Note that the “Create New Reservation” workflow can also be completed by searching for a user and selecting the user first in the right hand panel, and then selecting the bank and free locker in the left and center panel. It does not matter the order which the selections are made, so long as there is a User and individual locker selected before the Create Reservation button is pressed.

3.5.5 Sharing a Locker between Users

As with the Standalone Kiosk mode, the Master/Slave configuration (from version 1.1) also allows for sharing of a single lockers between 1 or more users.

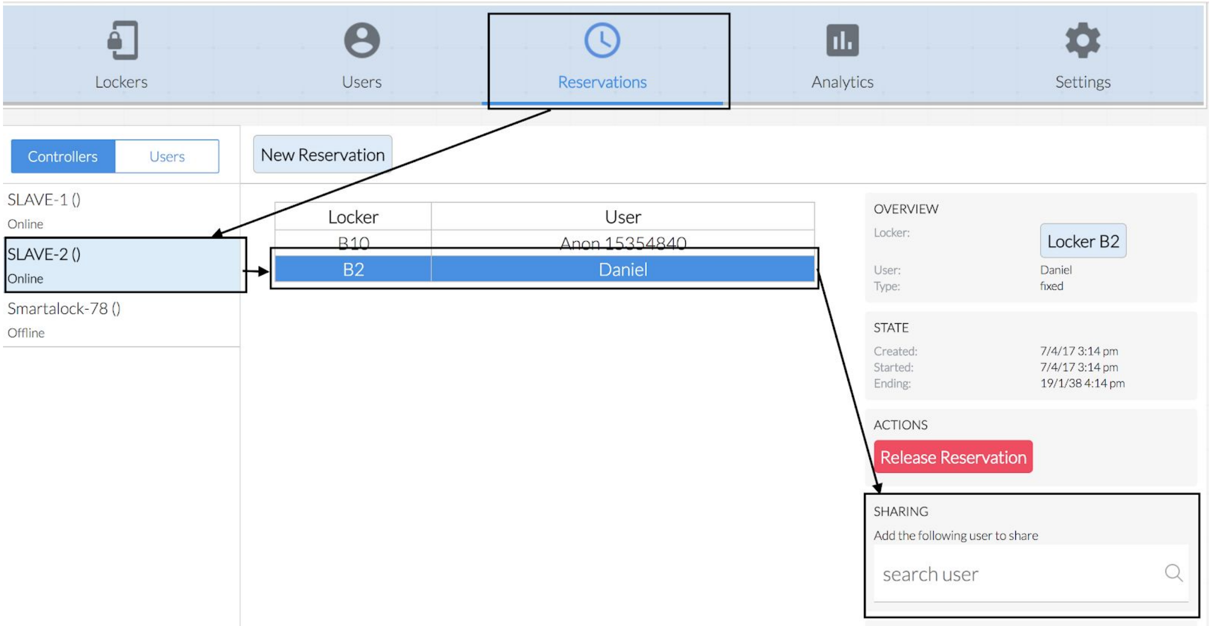
This feature is useful for lockers used as coat cupboards that all users have access to, or team lockers shared by a small subset of users.

With any reservation type (Fixed or Adhoc) a locker always has 1 and only 1 **owner**. This user is the **sharer.** Other system users can also be granted shared access to the same locker. These **sharee** users have limited rights to the locker - they can basically open the locker door via their swipe card, PIN code or Smartalock App. A sharee user cannot on-share the locker with any other user, nor can they release the reservation from the owner.

When the owners reservation expires or is released, then all sharee users of the locker will have their share access released as well.

To avoid possible problems for communal lockers it is best practice to create a dummy **user** account for the locker itself - called “Coat Cupboard” or “Shared Locker”, and make this user be the owner of the locker on a fixed reservation. All actual end users would be sharees of the locker so can be added and removed without interrupting the primary owner.

To share a locker between users use the below workflow:



Lockers | Users | Reservations | Analytics | Settings

Controllers | Users

New Reservation

SLAVE-1 ()
Online

SLAVE-2 ()
Online

Smartalock-78 ()
Offline

Locker	User
B10	Anon 15354840
B2	Daniel

OVERVIEW
Locker: Locker B2
User: Daniel
Type: fixed

STATE
Created: 7/4/17 3:14 pm
Started: 7/4/17 3:14 pm
Ending: 19/1/38 4:14 pm

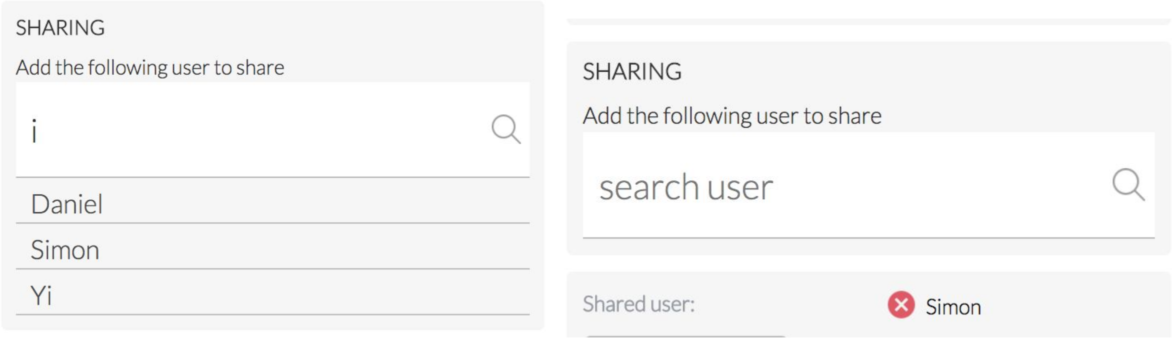
ACTIONS
Release Reservation

SHARING
Add the following user to share
search user

Select reservations (Sharing a locker is only possible from an existing reservation, so if the locker has no reservation, create a reservation for the owner user first).

Select the locker bank where the locker is locked, and then select the locker from the list of currently reserved lockers on that locker bank.

The Sharing panel will appear on right hand action panel. To start sharing with another user, start typing the name in the search box then press enter.



SHARING
Add the following user to share
i
Daniel
Simon
Yi

SHARING
Add the following user to share
search user

Shared user: Simon

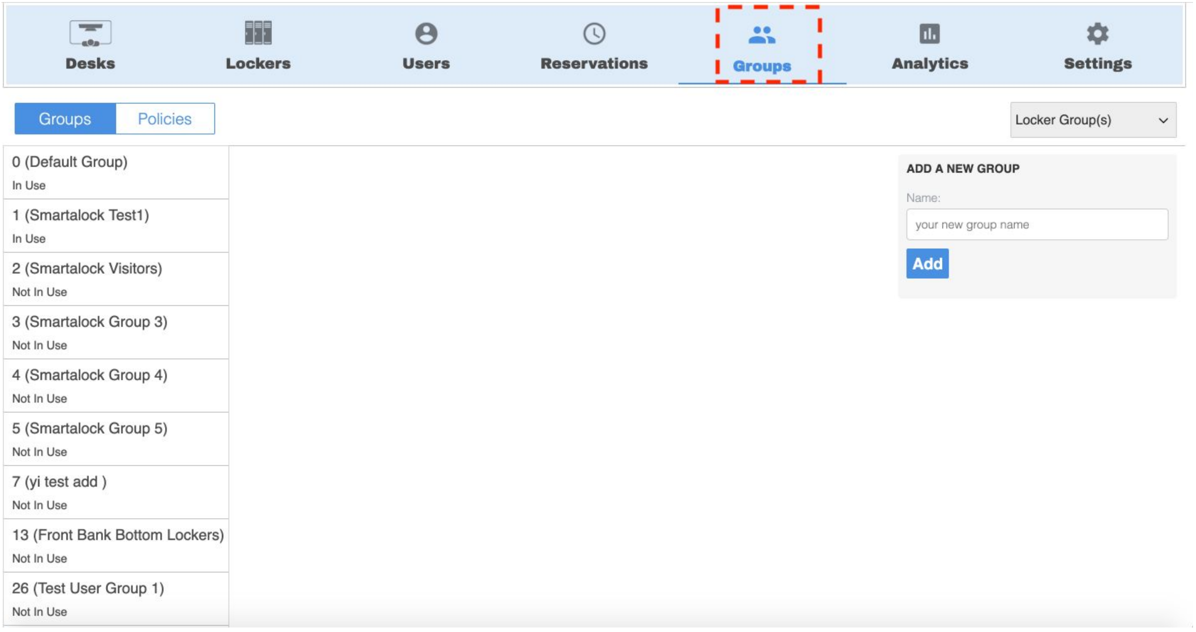
A short list of users names will appear. Clicking on any of the users will immediately share the locker with this user.

To un-share a locker press the red X button next to their name

Note that Sharee users cannot use PIN code to open a shared locker. PIN codes only work on lockers the user **owns**. Sharee’s must open a shared locker via the Smartalock App or their building swipe card.

3.6 Locker Groups

When the Groups tab is selected, a list of current locker groups is displayed. By default, only the Default Group will exist if no other group has been created. Depending on the user's preference, lockers can be grouped by size, sections, or by teams. An example of this interface, with groups already made, is as follows:



0 (Default Group)
In Use

1 (Smartalock Test1)
In Use

2 (Smartalock Visitors)
Not In Use

3 (Smartalock Group 3)
Not In Use

4 (Smartalock Group 4)
Not In Use

5 (Smartalock Group 5)
Not In Use

7 (yi test add)
Not In Use

13 (Front Bank Bottom Lockers)
Not In Use

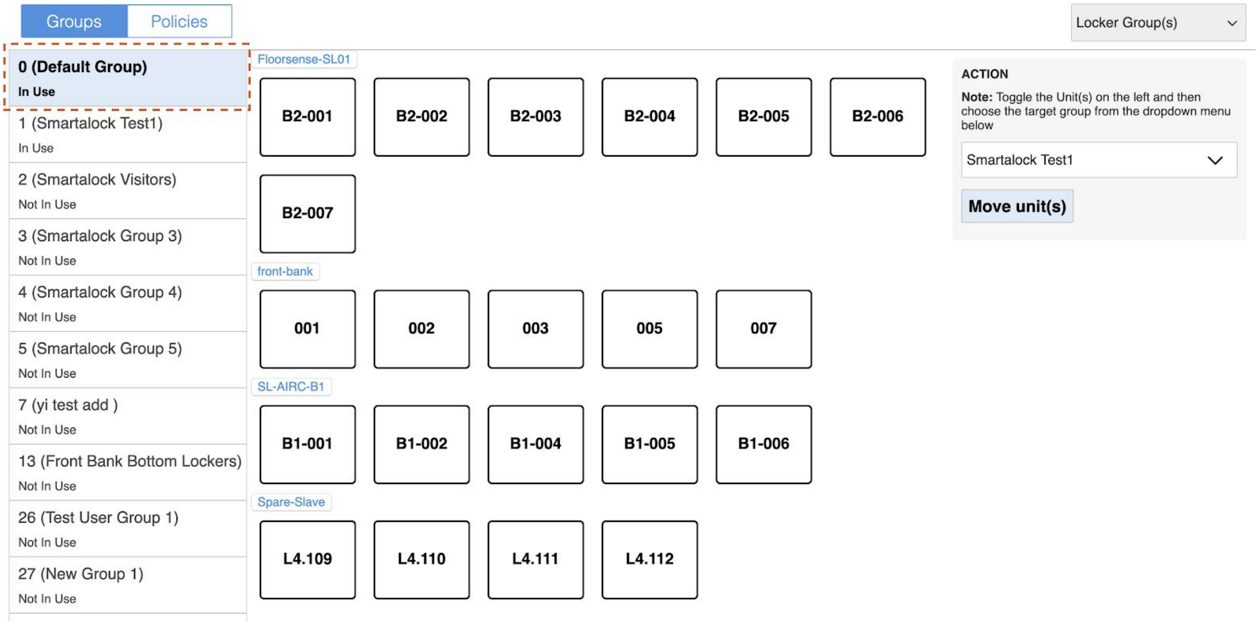
26 (Test User Group 1)
Not In Use

ADD A NEW GROUP

Name:

your new group name

By clicking on the Default Group, a list of locker banks will be displayed, and the administrator will be able to move specific lockers into groups in an interactive manner.



0 (Default Group)
In Use

1 (Smartalock Test1)
In Use

2 (Smartalock Visitors)
Not In Use

3 (Smartalock Group 3)
Not In Use

4 (Smartalock Group 4)
Not In Use

5 (Smartalock Group 5)
Not In Use

7 (yi test add)
Not In Use

13 (Front Bank Bottom Lockers)
Not In Use

26 (Test User Group 1)
Not In Use

27 (New Group 1)
Not In Use

Floorsense-SL01

B2-001 B2-002 B2-003 B2-004 B2-005 B2-006 B2-007

front-bank

001 002 003 005 007

SL-AIRC-B1

B1-001 B1-002 B1-004 B1-005 B1-006

Spare-Slave

L4.109 L4.110 L4.111 L4.112

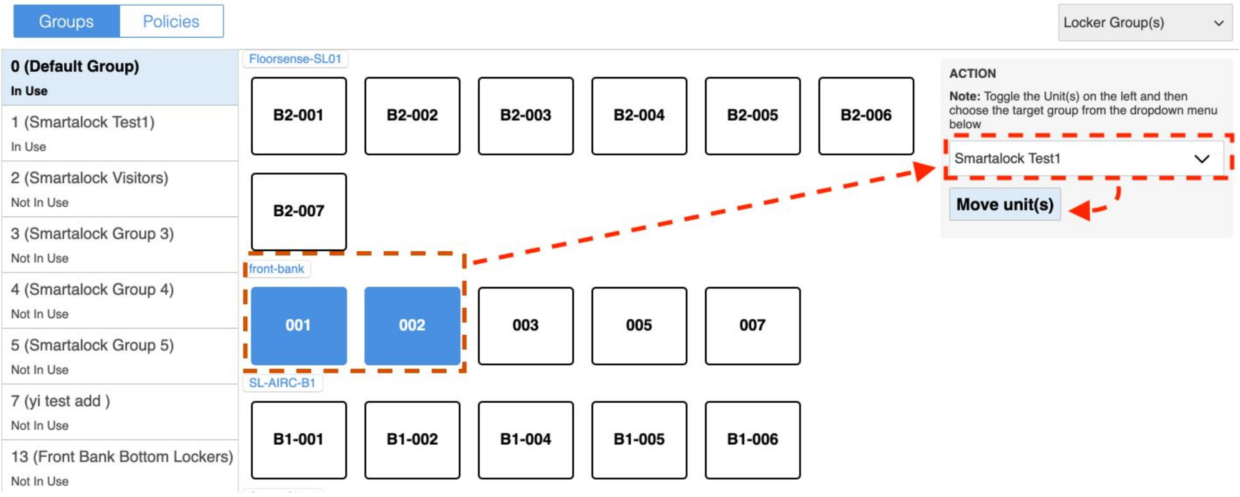
ACTION

Note: Toggle the Unit(s) on the left and then choose the target group from the dropdown menu below

Smartalock Test1

When a box is clicked, it gets highlighted in blue. This indicates that the associated locker is ready to be moved into another group. To unselect a locker, simply click on the box again to undo the highlight.

After selecting the lockers, the administrator can choose the target group from the drop-down menu, found in the “Action” window on the top right. When the target group has been selected, the lockers can then be moved into the designated group by clicking the “Move unit(s)” button.

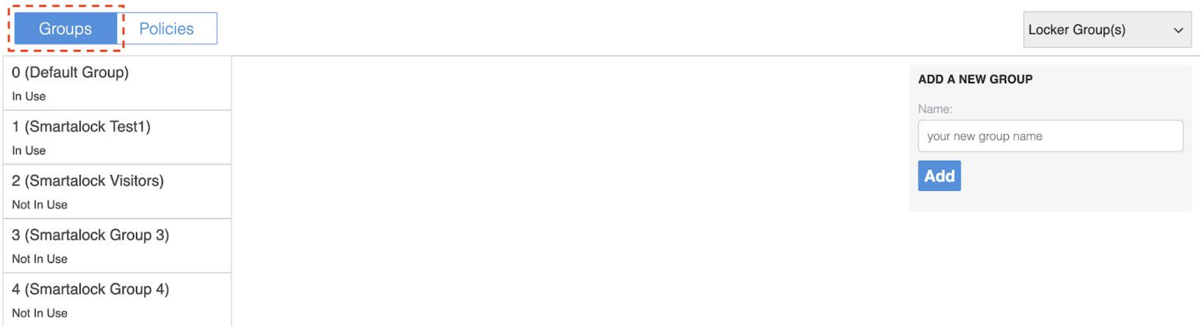


ACTION

Note: Toggle the Unit(s) on the left and then choose the target group from the dropdown menu below

Smartalock Test1

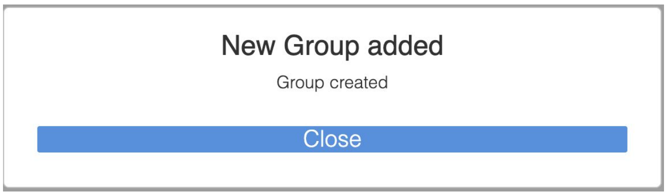
To create a new group, simply click on the Groups tab found in the top left corner. This leads the administrator back to the default Groups page.



ADD A NEW GROUP

Name: your new group name

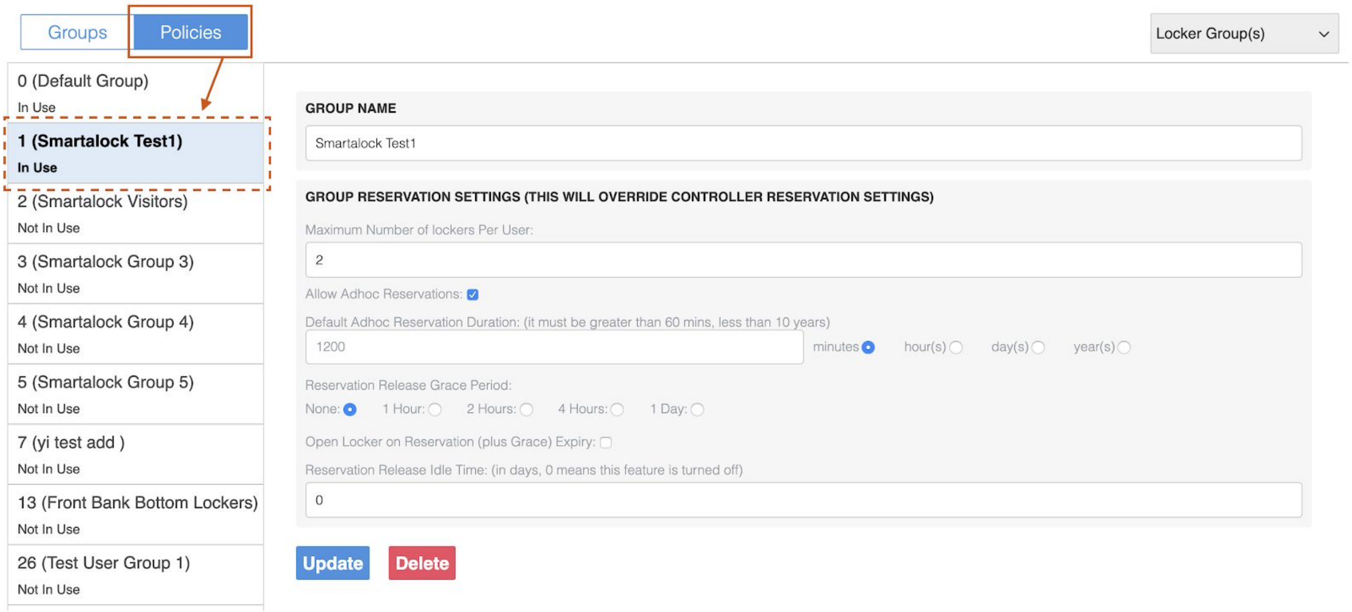
On the top right corner, a small window called “Add A New Group” exists that allows an administrator to create a new type of group. When a new group has been added, the following message should appear.



New Group added

Group created

When the close button is clicked, the administrator will be led to the Group Policies tab. In this tab, an administrator will be able to edit each group’s reservation settings such as reservation duration, the number of lockers reservable by each user etc. Note that these settings will be applied to each locker assigned to that group.



Groups | Policies

Locker Group(s)

0 (Default Group)
In Use

1 (Smartalock Test1)
In Use

2 (Smartalock Visitors)
Not In Use

3 (Smartalock Group 3)
Not In Use

4 (Smartalock Group 4)
Not In Use

5 (Smartalock Group 5)
Not In Use

7 (yi test add)
Not In Use

13 (Front Bank Bottom Lockers)
Not In Use

26 (Test User Group 1)
Not In Use

GROUP NAME

Smartalock Test1

GROUP RESERVATION SETTINGS (THIS WILL OVERRIDE CONTROLLER RESERVATION SETTINGS)

Maximum Number of lockers Per User:

2

Allow Adhoc Reservations: ☑

Default Adhoc Reservation Duration: (it must be greater than 60 mins, less than 10 years)

1200 minutes ● hour(s) ○ day(s) ○ year(s) ○

Reservation Release Grace Period:

None: ● 1 Hour: ○ 2 Hours: ○ 4 Hours: ○ 1 Day: ○

Open Locker on Reservation (plus Grace) Expiry: □

Reservation Release Idle Time: (in days, 0 means this feature is turned off)

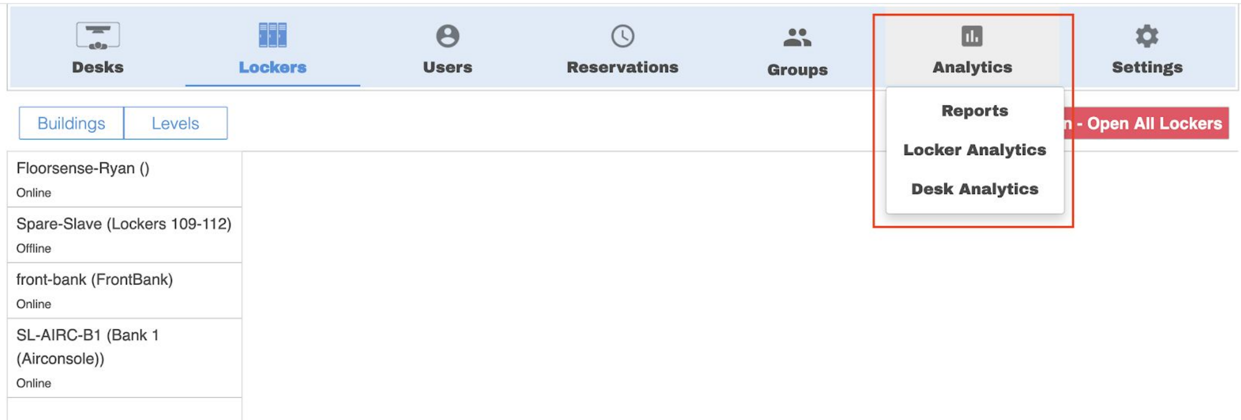
0

Update Delete

As per section 3.3, the group policy should generally be more restrictive than a controller (entire locker bank) policy otherwise there maybe a conflict between policies. To avoid policy conflicts, make the controller and master policy more permissive than the group policy as they policy check is performed in the group->controller->site order.

3.7 System Analytics

Clicking on the Analytics tab brings out three sections; Reports, Locker Analytics, and Desk Analytics. Desk Analytics are only applicable if the floorsense system is also installed.



Desks | Lockers | Users | Reservations | Groups | Analytics | Settings

Reports
Locker Analytics
Desk Analytics

Buildings | Levels

n - Open All Lockers

Floorsense-Ryan ()
Online

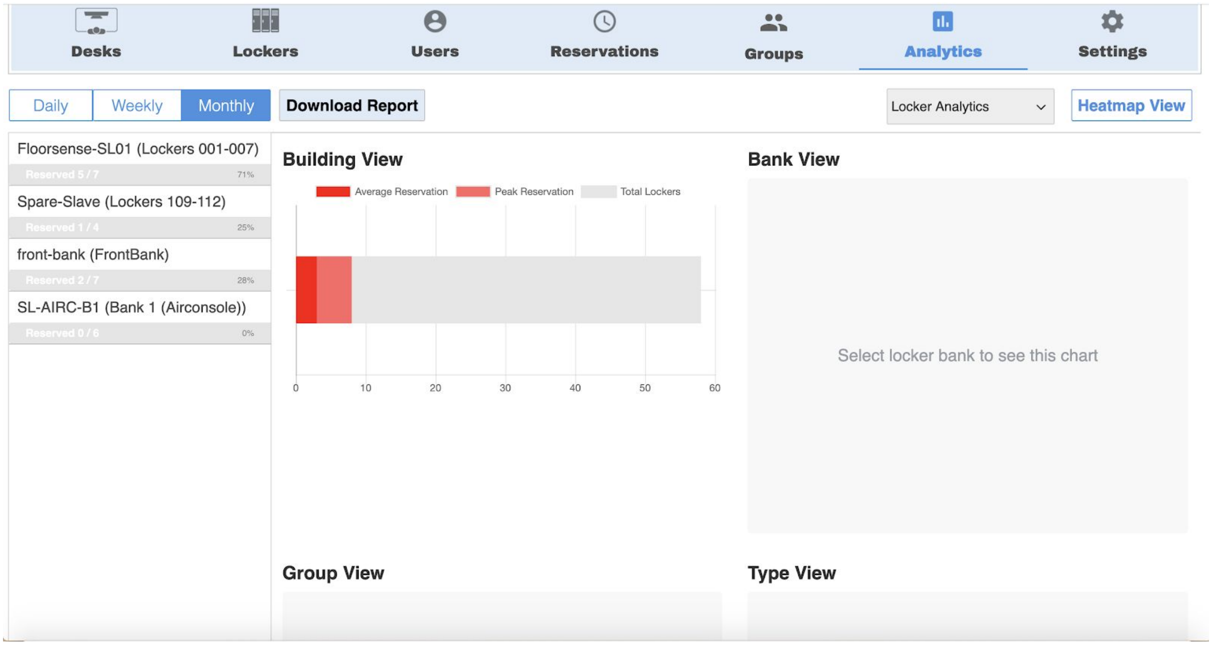
Spare-Slave (Lockers 109-112)
Offline

front-bank (FrontBank)
Online

SL-AIRC-B1 (Bank 1 (Airconsole))
Online

Clicking on the Reports section brings up a page consisting of different types of reports that can be exported as a CSV file.

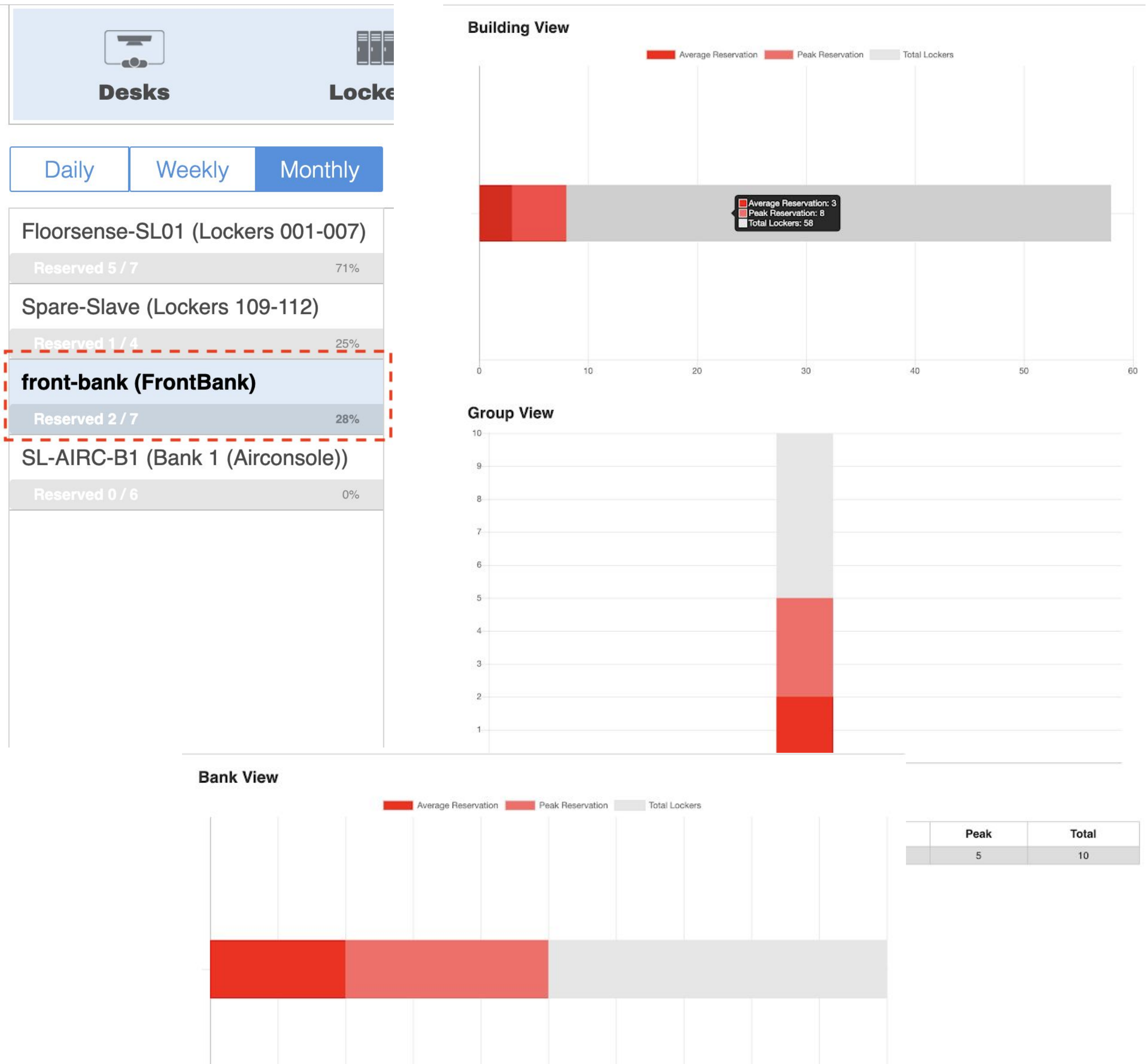
Clicking on the Locker Analytics section brings up the following page:



Floorsense-SL01 (Lockers 001-007)
Reserved 5 / 7 71%
Spare-Slave (Lockers 109-112)
Reserved 1 / 4 25%
front-bank (FrontBank)
Reserved 2 / 7 28%
SL-AIRC-B1 (Bank 1 (Airconsole))
Reserved 0 / 6 0%

The Locker Analytics section essentially displays the occupancy, and the frequency of reservation for each locker in the form of a bar chart. By default, the page will only show a chart of the Building View section on a monthly basis.

By selecting a bank on the left panel, the different “View” sections will be filled with bar charts as seen below.



Floorsense-SL01 (Lockers 001-007)
Reserved 5 / 7 71%
Spare-Slave (Lockers 109-112)
Reserved 1 / 4 25%
front-bank (FrontBank)
Reserved 2 / 7 28%
SL-AIRC-B1 (Bank 1 (Airconsole))
Reserved 0 / 6 0%

Average Reservation: 3
Peak Reservation: 8
Total Lockers: 58

Peak	Total
5	10

Building View: An overall report on all the locker banks present in the building, as seen by the master controller.

Group View: A chart based on the frequency of reservation, based on the locker groups that have been created.

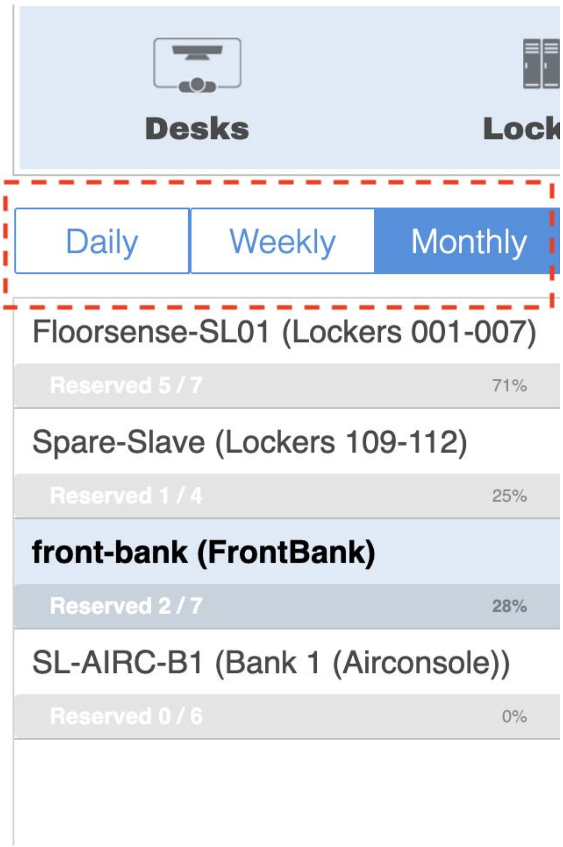
Reservation (Below Group View): A numerical report based on the frequency of reservation for each group.

Bank View: A report on the locker bank that is currently selected, i.e. the bank that was chosen on the left panel.

Type View: As lockers are often of different types (Top/Middle/Bottom sections, Big/Medium/Small etc.), this view displays a report based on the different types of lockers being used.

Reservation (Below Type View): Summarises the chart from Type View in numerical form as a table.

At the top of the left panel, the tabs Daily, Weekly, and Monthly can be selected. As it implies, these options change the figures of the report based on either a daily, weekly, or monthly basis. The current option selected will be highlighted in blue, which can be seen in the example below.



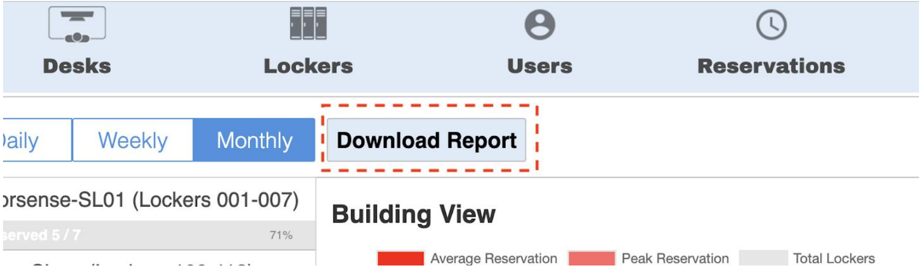
Floorsense-SL01 (Lockers 001-007)
Reserved 5 / 7 71%

Spare-Slave (Lockers 109-112)
Reserved 1 / 4 25%

front-bank (FrontBank)
Reserved 2 / 7 28%

SL-AIRC-B1 (Bank 1 (Airconsole))
Reserved 0 / 6 0%

Right next to the Daily/Weekly/Monthly tabs is the Download Report button:

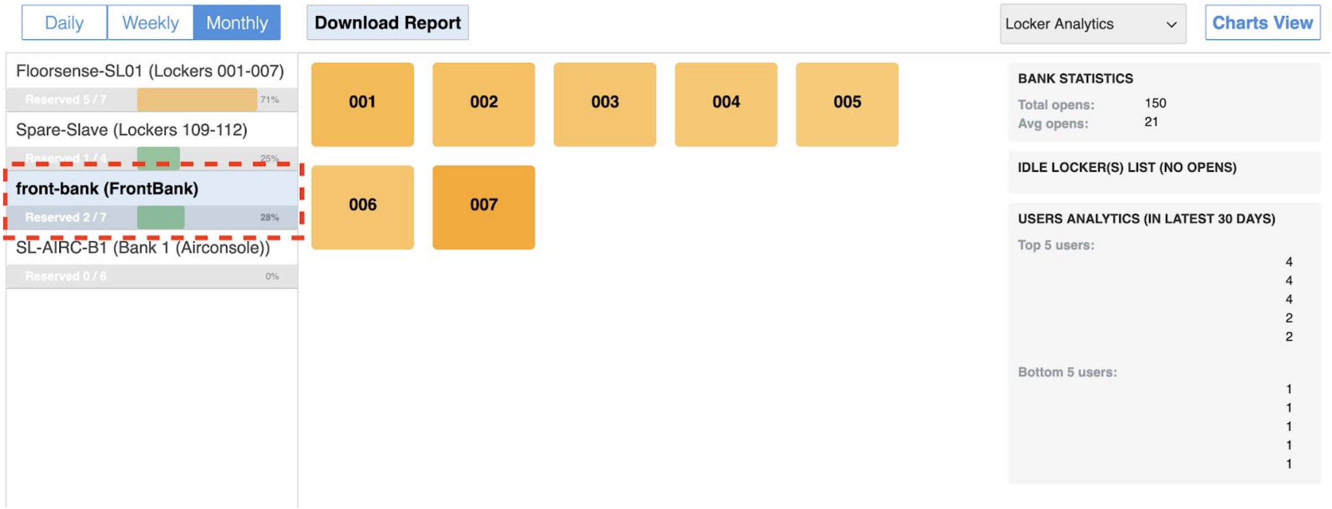


ɔrsense-SL01 (Lockers 001-007)
ɛrved 5 / 7 71%

This essentially leads to the aforementioned Reports page mentioned at the beginning of this section.

At the top right panel, the user is able to switch the display from graphical, to a heat map format. In the heat map interface, the same statistics can be viewed but a map with varying color intensity is displayed instead of a chart.

Select a locker bank on the left panel to view its heat map. By default, the statistics are on a monthly basis.



Floorsense-SL01 (Lockers 001-007)
Reserved 5 / 7 71%

Spare-Slave (Lockers 109-112)
Reserved 1 / 4 25%

front-bank (FrontBank)
Reserved 2 / 7 28%

SL-AIRC-B1 (Bank 1 (Airconsole))
Reserved 0 / 6 0%

BANK STATISTICS
Total opens: 150
Avg opens: 21

IDLE LOCKER(S) LIST (NO OPENS)

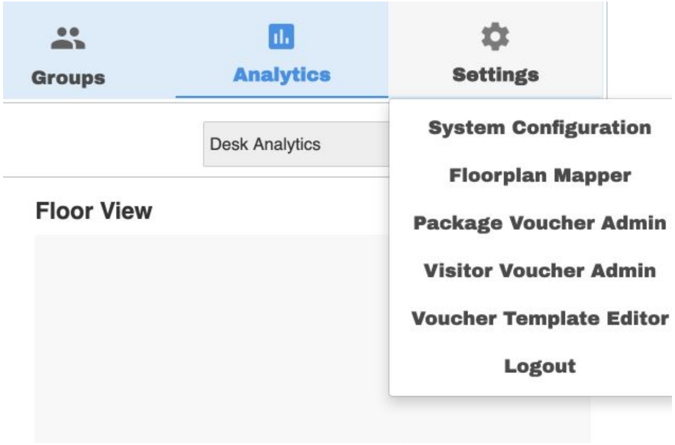
USERS ANALYTICS (IN LATEST 30 DAYS)
Top 5 users:
4
4
4
2
2
Bottom 5 users:
1
1
1
1
1

The middle panel shows the heat maps of each locker bank. A darker color indicates a locker that is being used frequently, whereas a locker with a brighter color indicates otherwise. The panel on the right shows a report on the usage of lockers in a particular bank. It also displays the 5 most frequent and infrequent locker users, and the total number of times they have opened their locker in a month.

3.8 System Settings

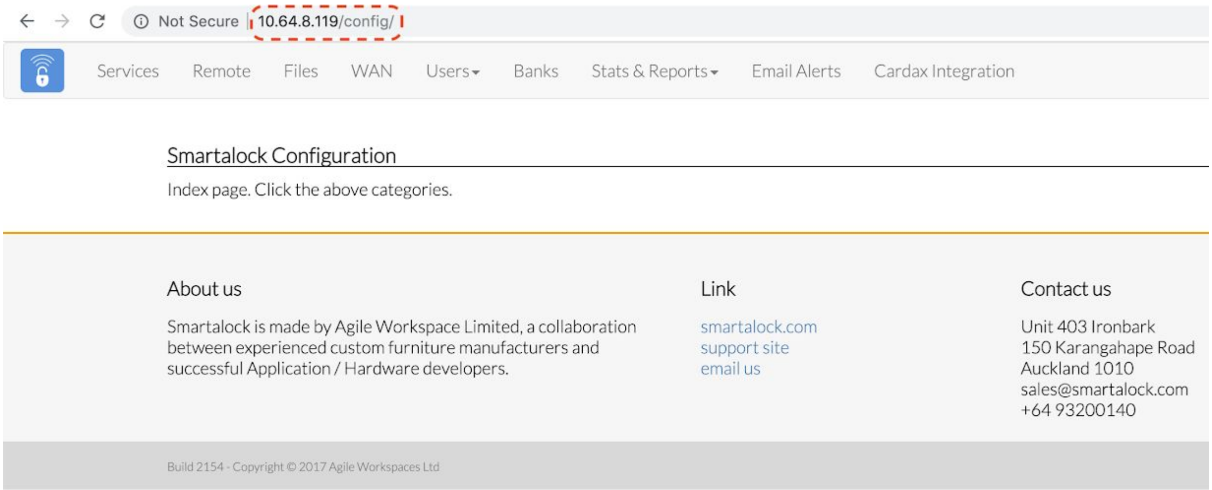
Clicking on the ‘Settings’ tab brings out the following options:

- System Configuration
- Floorplan Mapper (Applicable for Floorsense/sight units only)
- Package Voucher Admin
- Visitor Voucher Admin
- Voucher Template Editor
- Logout



3.8.1 System Configuration

Clicking on this tab brings the user to the Configuration page. This can alternately be accessed by typing the master controller’s IP address, followed by a ‘/config’ in the address bar. Typically, only the **Users**, **Banks**, and **Stats & Reports**, are of interest for the administrator.



Smartalock Configuration

Index page. Click the above categories.

About us

Smartalock is made by Agile Workspace Limited, a collaboration between experienced custom furniture manufacturers and successful Application / Hardware developers.

Link

smartalock.com
support site
email us

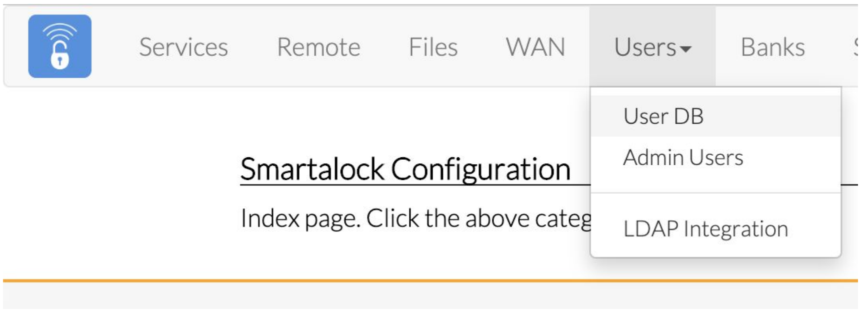
Contact us

Unit 403 Ironbark
150 Karangahape Road
Auckland 1010
sales@smartalock.com
+64 93200140

Build 2154 - Copyright © 2017 Agile Workspaces Ltd

Users

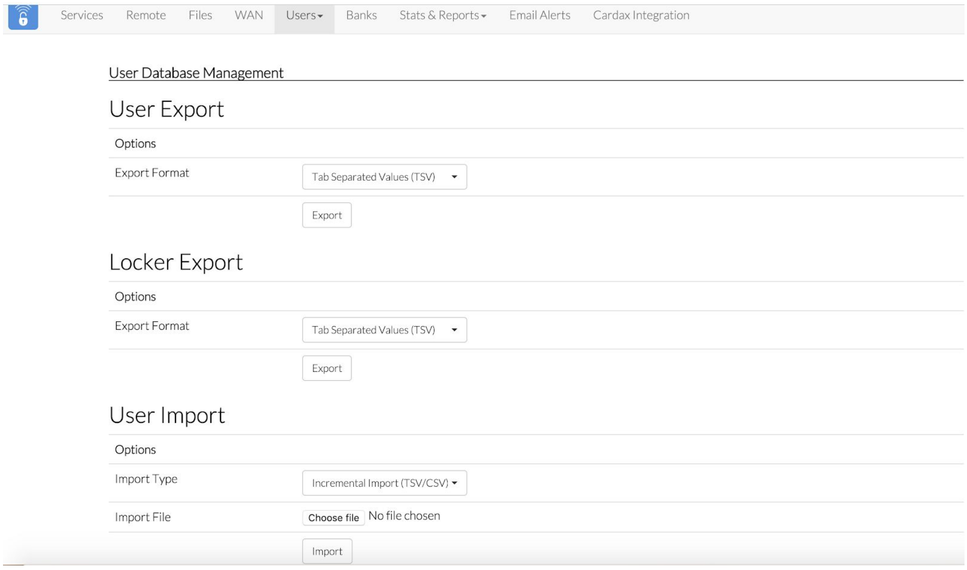
The **Users** tab displays three options: **User DB**, **Admin Users**, and **LDAP Integration**.



Smartalock Configuration

Index page. Click the above categ

Clicking on User DB leads to the User Database Management, which essentially allows the user to do either a bulk import of the user database, or an export of either the user or locker database.



User Database Management

User Export

Options

Export Format: Tab Separated Values (TSV)

Locker Export

Options

Export Format: Tab Separated Values (TSV)

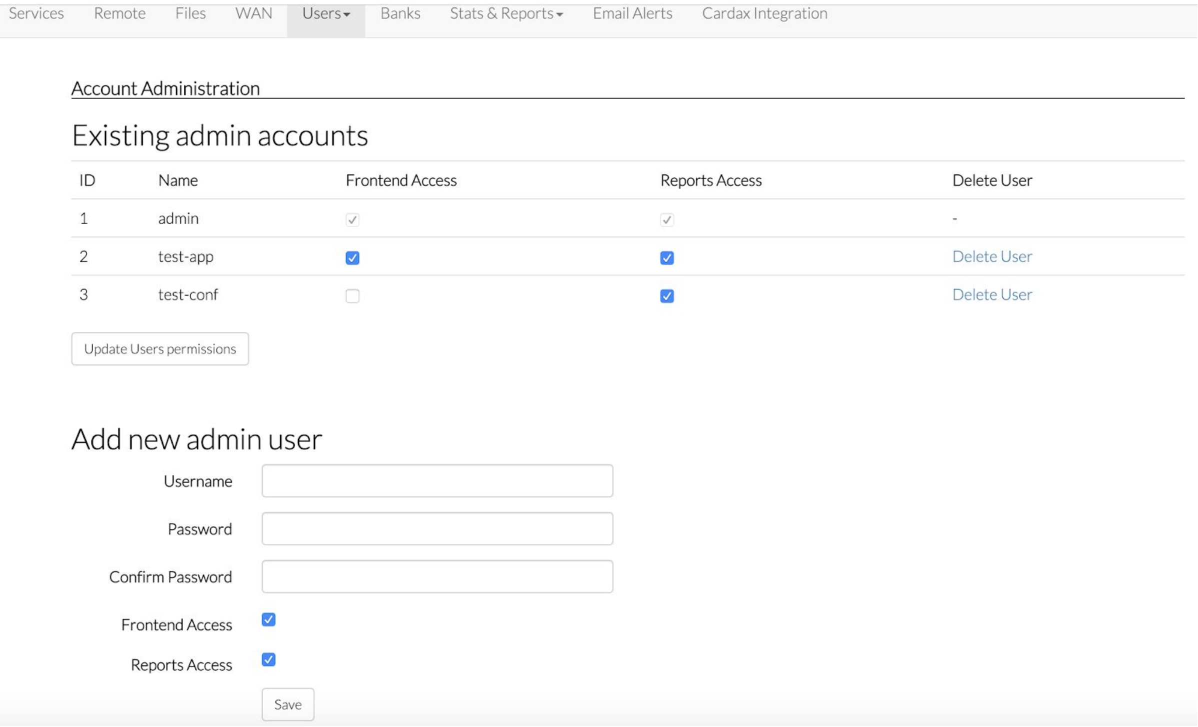
User Import

Options

Import Type: Incremental Import (TSV/CSV)

Import File: Choose file No file chosen

Clicking on Admin Users allows different users to be added as administrators to access either the Frontend (the default interactive webapp), and/or the Reports page.



Account Administration

Existing admin accounts

ID	Name	Frontend Access	Reports Access	Delete User
1	admin	✓	✓	-
2	test-app	☑	☑	Delete User
3	test-conf	☐	☑	Delete User

Add new admin user

Username

Password

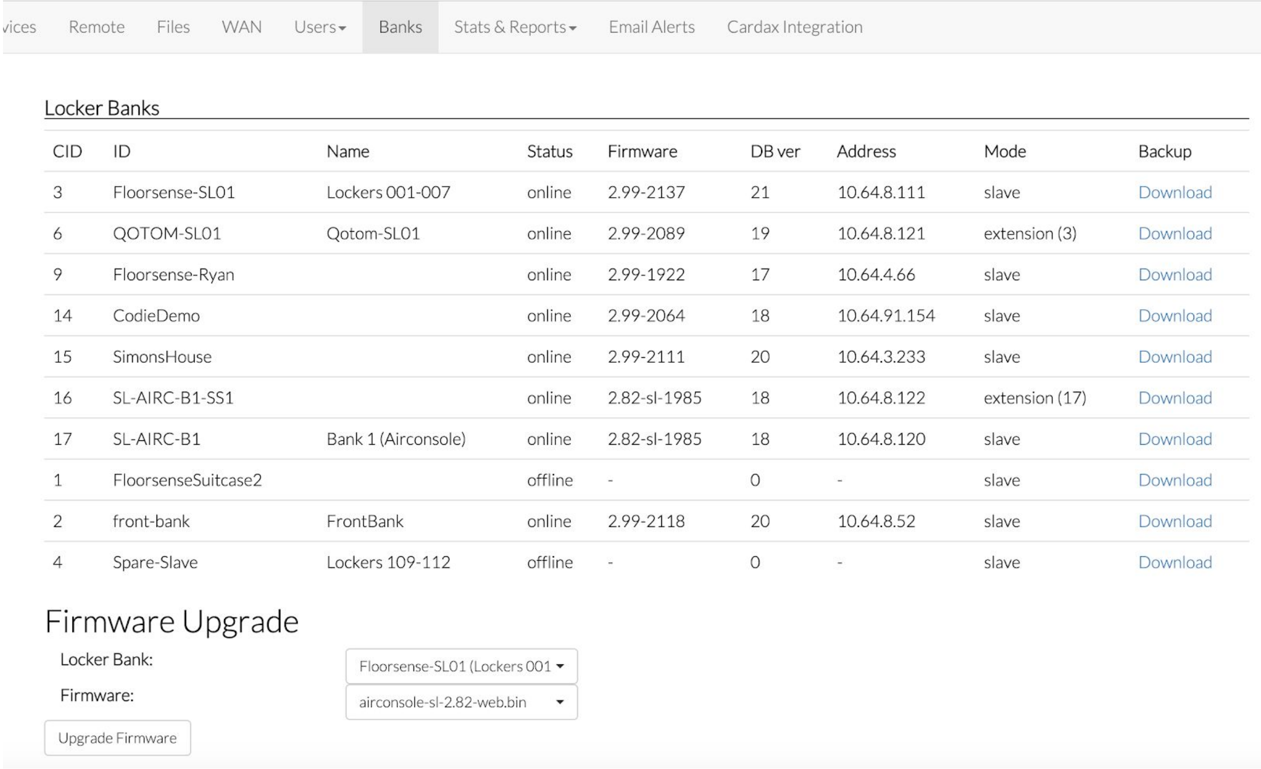
Confirm Password

Frontend Access ☑

Reports Access ☑

Banks

The **Banks** tab essentially displays the locker banks that are present on site. An option to backup each bank is present, in case the respective controller fails and important data needs to be transferred to the replacement controller. The option to update the firmware is also present however this can be normally ignored.



Locker Banks

CID	ID	Name	Status	Firmware	DB ver	Address	Mode	Backup
3	Floorsense-SL01	Lockers 001-007	online	2.99-2137	21	10.64.8.111	slave	Download
6	QOTOM-SL01	Qotom-SL01	online	2.99-2089	19	10.64.8.121	extension (3)	Download
9	Floorsense-Ryan		online	2.99-1922	17	10.64.4.66	slave	Download
14	CodieDemo		online	2.99-2064	18	10.64.91.154	slave	Download
15	SimonsHouse		online	2.99-2111	20	10.64.3.233	slave	Download
16	SL-AIRC-B1-SS1		online	2.82-sl-1985	18	10.64.8.122	extension (17)	Download
17	SL-AIRC-B1	Bank 1 (Airconsole)	online	2.82-sl-1985	18	10.64.8.120	slave	Download
1	FloorsenseSuitcase2		offline	-	0	-	slave	Download
2	front-bank	FrontBank	online	2.99-2118	20	10.64.8.52	slave	Download
4	Spare-Slave	Lockers 109-112	offline	-	0	-	slave	Download

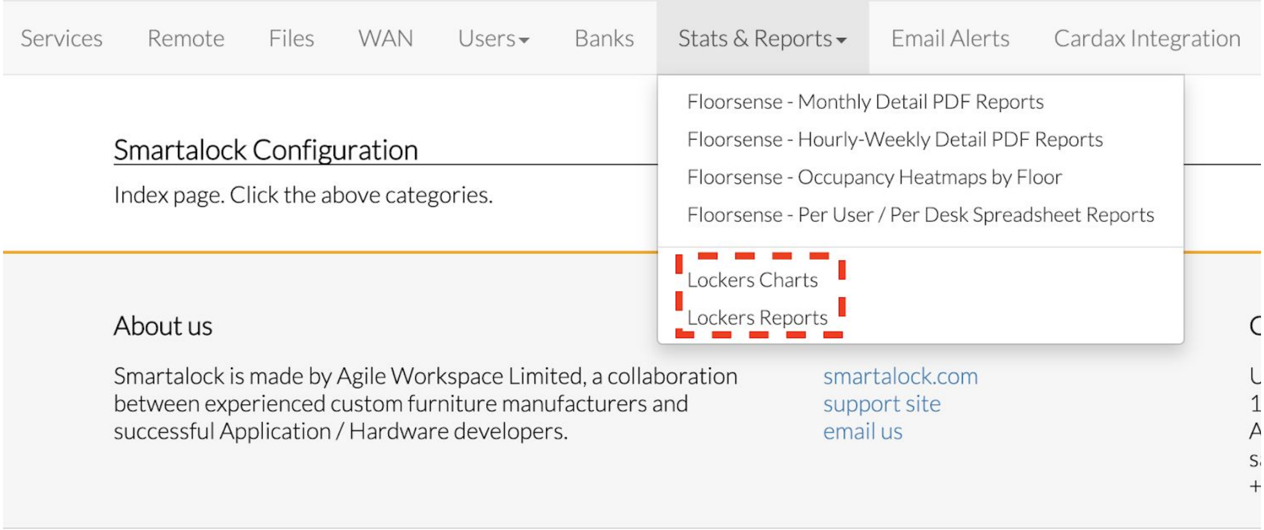
Firmware Upgrade

Locker Bank: Floorsense-SL01 (Lockers 001 ▾

Firmware: airconsole-sl-2.82-web.bin ▾

Stats & Reports

Clicking on the **Stats & Reports** tab brings up a few sections. The Floorsense sections are only applicable if Floorsense units are available on site. For locker related reports, click on either the **Lockers Charts** or the **Lockers Reports** section.



Services
Remote
Files
WAN
Users
Banks
Stats & Reports
Email Alerts
Cardax Integration
Floorsense - Monthly Detail PDF Reports
Floorsense - Hourly-Weekly Detail PDF Reports
Floorsense - Occupancy Heatmaps by Floor
Floorsense - Per User / Per Desk Spreadsheet Reports
Lockers Charts
Lockers Reports

Smartalock Configuration

Index page. Click the above categories.

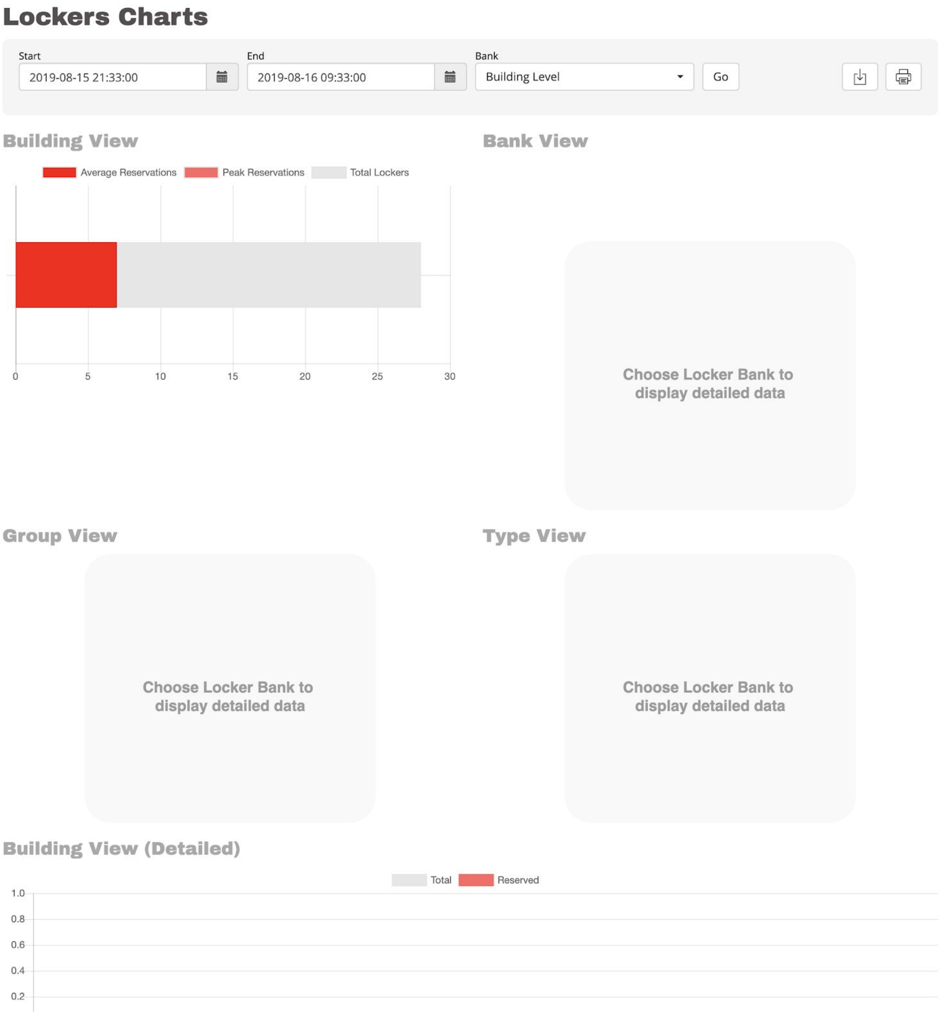
About us

Smartalock is made by Agile Workspace Limited, a collaboration between experienced custom furniture manufacturers and successful Application / Hardware developers.

smartalock.com
support site
email us

C
U
1
A
S
+

Clicking on **Lockers Charts** leads to a page that displays a group of charts based on the reservation statistics of each locker bank.

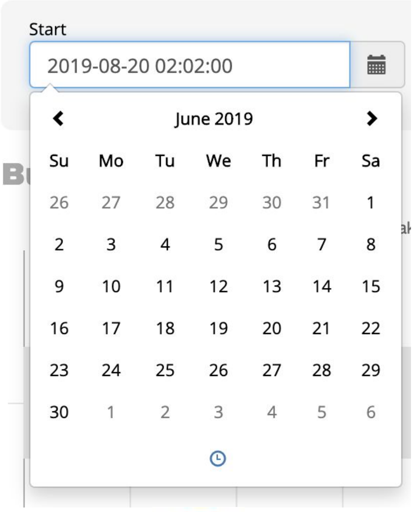


Lockers Charts

Start: 2019-08-15 21:33:00
End: 2019-08-16 09:33:00
Bank: Building Level

By default only the chart for Building View will be displayed, and the Start and End intervals are of the previous day and the current day respectively. In order to change this, thefollowing steps should be applied at the top:

1. Change the Start date by clicking on the calendar button 📅 which brings up a calendar for the user to pick a day.



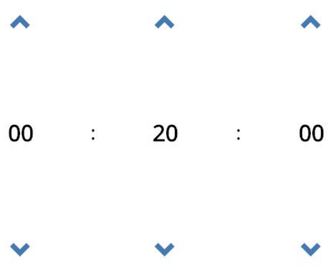
Start

2019-08-20 02:02:00

< June 2019 >

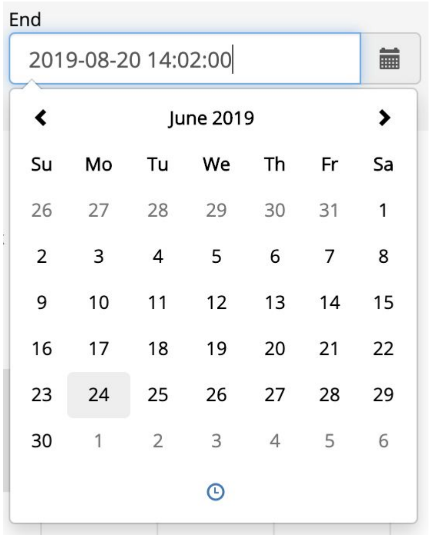
Su	Mo	Tu	We	Th	Fr	Sa
26	27	28	29	30	31	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	1	2	3	4	5	6

Clicking on the clock icon 🕒 at the bottom allows the user to pick the time.



00 : 20 : 00

2. The End date can also be changed through the same method as step 1.



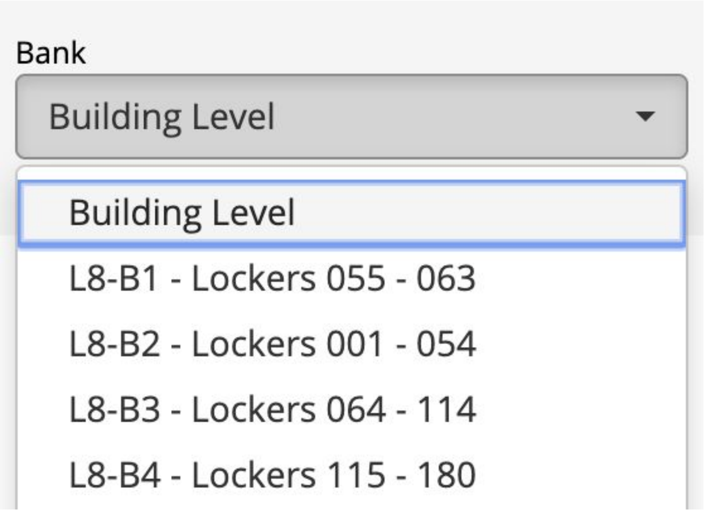
End

2019-08-20 14:02:00

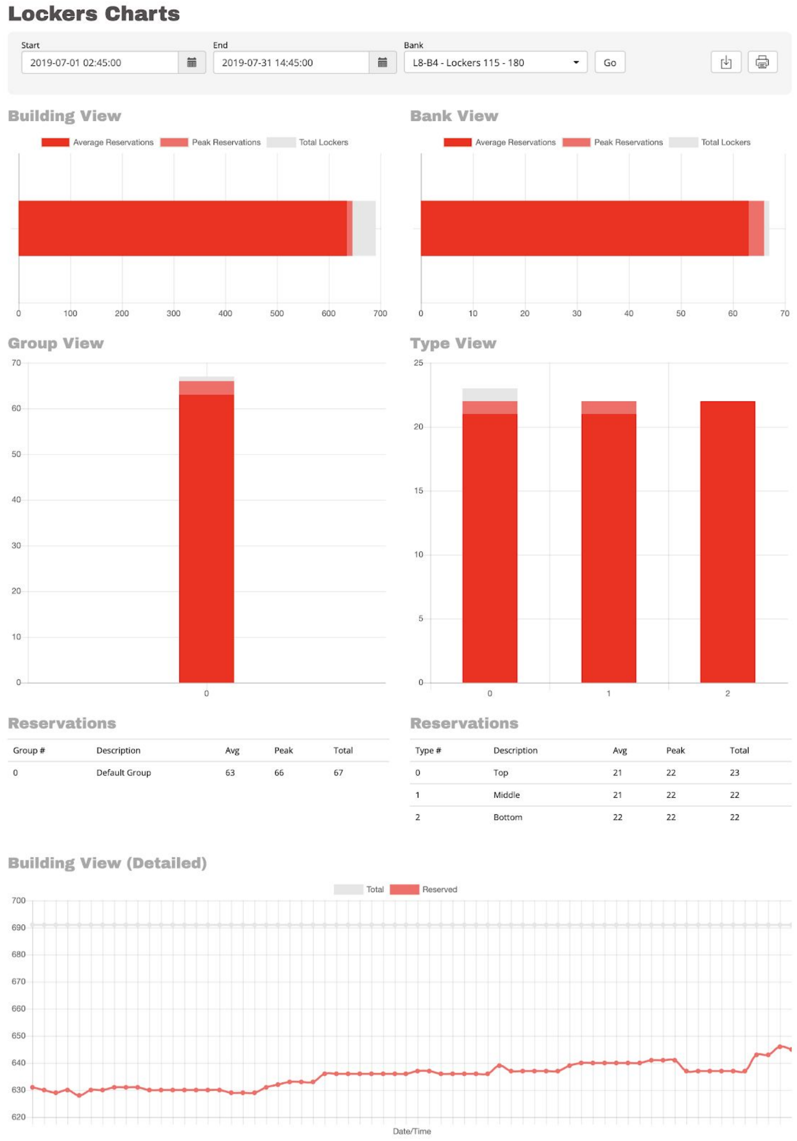
< June 2019 >

Su	Mo	Tu	We	Th	Fr	Sa
26	27	28	29	30	31	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	1	2	3	4	5	6

3. By clicking the Bank drop-down tab, choose the bank of interest.


Bank
Building Level
Building Level
L8-B1 - Lockers 055 - 063
L8-B2 - Lockers 001 - 054
L8-B3 - Lockers 064 - 114
L8-B4 - Lockers 115 - 180

After editing the tabs using the steps above, the administrator can either view the charts directly via the GO button Go or download a CSV report via the download button ⤓ or print the charts via the print button 🖶. The following is an example of a completed chart.


Lockers Charts

Start: 2019-07-01 02:45:00
End: 2019-07-31 14:45:00
Bank: L8-B4 - Lockers 115 - 180

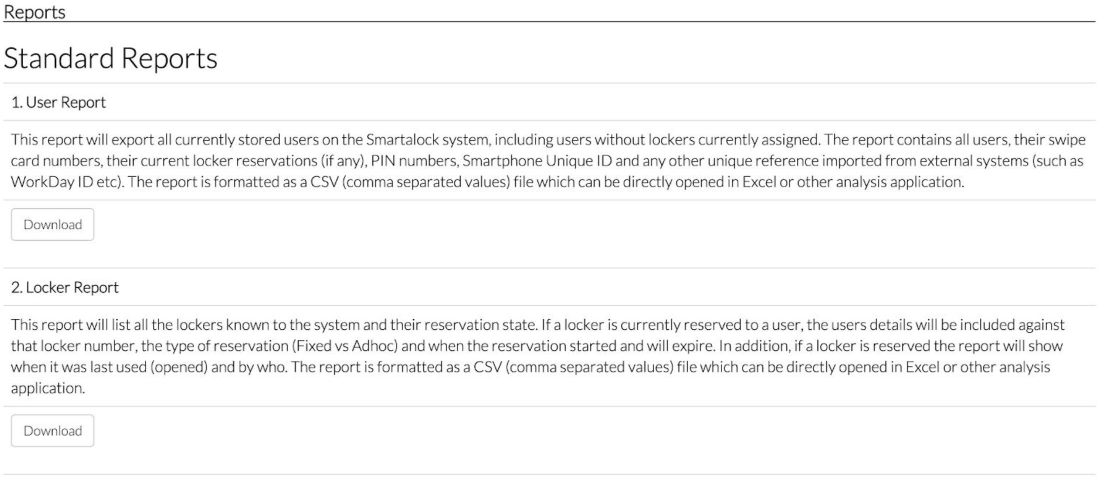
Reservations

Group #	Description	Avg	Peak	Total
0	Default Group	63	66	67

Reservations

Type #	Description	Avg	Peak	Total
0	Top	21	22	23
1	Middle	21	22	22
2	Bottom	22	22	22

In contrast, clicking on the **Lockers Reports tab** simply leads to the Standard Reports page consisting of data that can be exported as a CSV file.



Reports

Standard Reports

1. User Report

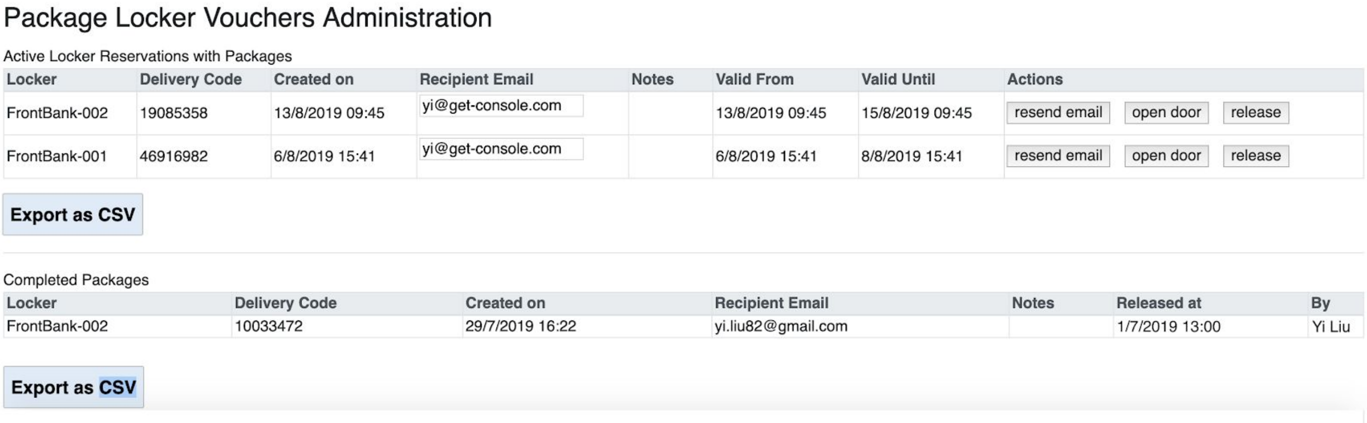
This report will export all currently stored users on the Smartalock system, including users without lockers currently assigned. The report contains all users, their swipe card numbers, their current locker reservations (if any), PIN numbers, Smartphone Unique ID and any other unique reference imported from external systems (such as WorkDay ID etc). The report is formatted as a CSV (comma separated values) file which can be directly opened in Excel or other analysis application.

2. Locker Report

This report will list all the lockers known to the system and their reservation state. If a locker is currently reserved to a user, the users details will be included against that locker number, the type of reservation (Fixed vs Adhoc) and when the reservation started and will expire. In addition, if a locker is reserved the report will show when it was last used (opened) and by who. The report is formatted as a CSV (comma separated values) file which can be directly opened in Excel or other analysis application.

3.8.2 Package Voucher Admin

Clicking on this section allows the administrator to view and manage package vouchers that were created via the Package Delivery Quick Form.



Package Locker Vouchers Administration

Active Locker Reservations with Packages

Locker	Delivery Code	Created on	Recipient Email	Notes	Valid From	Valid Until	Actions
FrontBank-002	19085358	13/8/2019 09:45	yi@get-console.com		13/8/2019 09:45	15/8/2019 09:45	resend email open door release
FrontBank-001	46916982	6/8/2019 15:41	yi@get-console.com		6/8/2019 15:41	8/8/2019 15:41	resend email open door release

Completed Packages

Locker	Delivery Code	Created on	Recipient Email	Notes	Released at	By
FrontBank-002	10033472	29/7/2019 16:22	yi.liu82@gmail.com		1/7/2019 13:00	Yi Liu

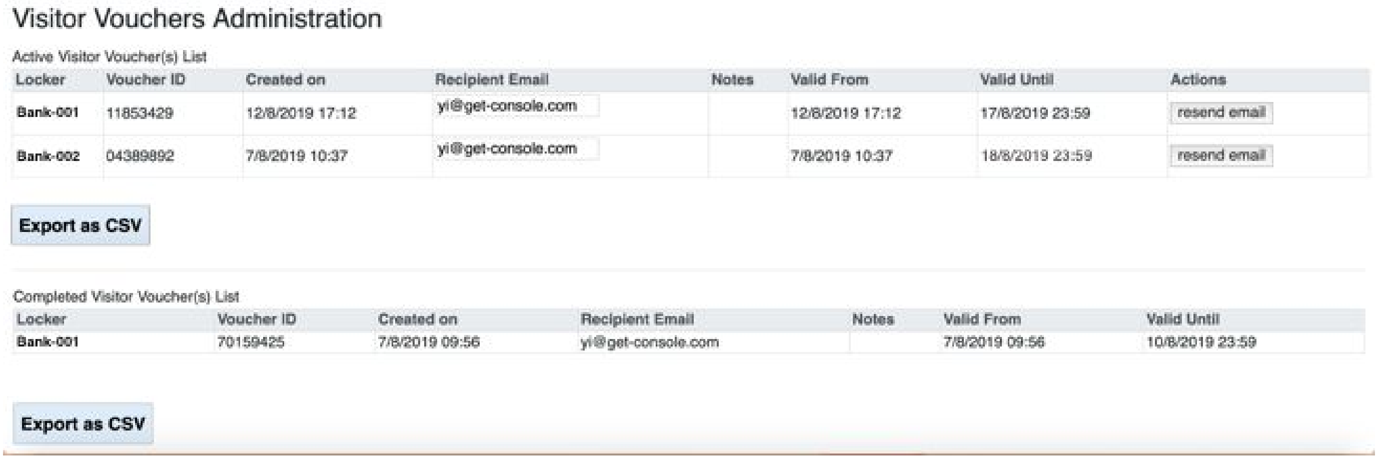
If there are packages awaiting to be picked up, they will fall under **“Active Locker Reservations with Packages**”. An administrator could choose to either edit the recipient's address, resend a notification email to the affected user, open the locker, or release the reserved package from the locker.

In contrast once a package has been released either by a user (via their card or pin) or an admin, they would fall under “**Completed Packages**”. A date will be displayed under the “Released at” column, followed by the user or admin’s credentials under the “By” column.

An option to export these data as a CSV file is also available by clicking the “Export as CSV” button.

3.8.3 Visitor Voucher Admin

Similar to Package Voucher Admin, clicking on Visitor Voucher Admin allows the admin to manage and edit the current visitor vouchers created via the Visitor Quick Form.



Visitor Vouchers Administration

Active Visitor Voucher(s) List

Locker	Voucher ID	Created on	Recipient Email	Notes	Valid From	Valid Until	Actions
Bank-001	11853429	12/8/2019 17:12	yi@get-console.com		12/8/2019 17:12	17/8/2019 23:59	resend email
Bank-002	04389892	7/8/2019 10:37	yi@get-console.com		7/8/2019 10:37	18/8/2019 23:59	resend email

Completed Visitor Voucher(s) List

Locker	Voucher ID	Created on	Recipient Email	Notes	Valid From	Valid Until
Bank-001	70159425	7/8/2019 09:56	yi@get-console.com		7/8/2019 09:56	10/8/2019 23:59

This page also features two sections; the **Active Visitor Vouchers List**, and the **Completed Visitor Vouchers List**.

The former shows the current visitor vouchers that have been created, and allows the admin to edit the recipient's email address and resend a notification email to the visitor in question.

The Completed Visitor Vouchers List shows vouchers that have been used (i.e, the QR code has been scanned).

Like the Package Voucher Admin section, data from the Visitor Voucher Admin section can be exported as a CSV file.

3.8.4 Voucher Template Editor

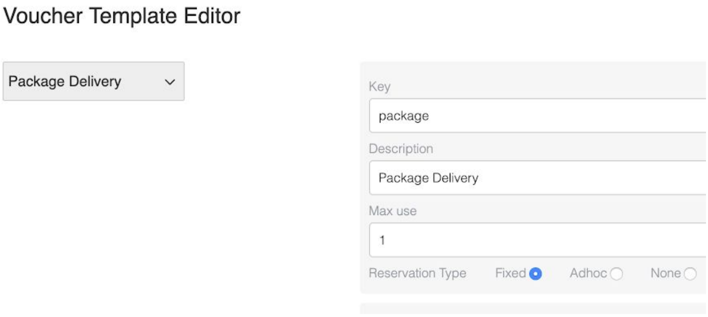
Clicking on this section allows the administrator to edit the process of unlocking the lockers and the message to be sent via email, when either a Package Voucher or a Visitor Voucher is created.

Two templates can be edited, namely the **Package Delivery** and **Visitor Pass**. The administrator can choose between these templates via the drop-down menu on the top left.

The first box essentially consists of general details. Although the field "Key" cannot be edited, the "Description" field is omittable. This just changes the title of the template, which in this case is either "Package Delivery" or "Visitor Pass".

The "Max use" field indicates the number of times a user can make use of a voucher's QR code. A **Package Delivery** voucher should only have a value of 1 as a user will only be using it to obtain their package from the locker. A **Visitor Pass** voucher should have a value of 0 as a visitor should be able to open their locker as many times as they can within the time period.

The option “Reservation Type” changes the type of reservation the locker will have upon creating the voucher. A fixed reservation indicates a locker that will be used for a longer period, which is suitable for cases such as package deliveries to allow recipients time to obtain their package. Adhoc reservation indicates a locker that will be used for a fixed period of time, which is suitable for visitors as they will only be using the locker on a short term.


Voucher Template Editor

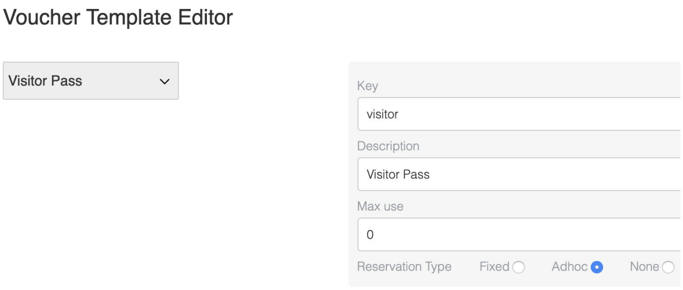
Package Delivery

Key: package

Description: Package Delivery

Max use: 1

Reservation Type: Fixed ● Adhoc ○ None ○


Voucher Template Editor

Visitor Pass

Key: visitor

Description: Visitor Pass

Max use: 0

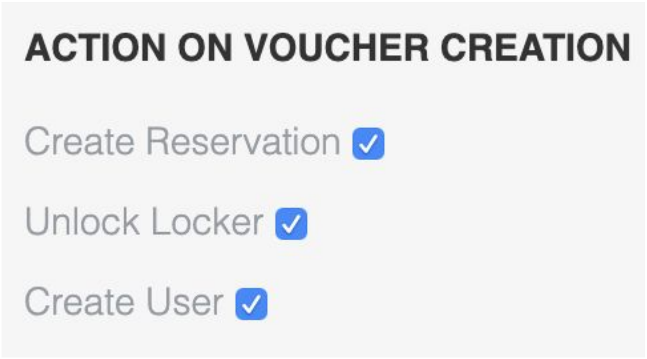
Reservation Type: Fixed ○ Adhoc ● None ○

The second box “Activation On Voucher Creation” dictates the actions taken when a voucher has just been created based on the boxes ticked.

- Create Reservation: Creates a locker reservation in the system with the user’s credentials
- Unlock Locker: Unlocks the locker door.
- Create User: Creates a temporary user in the system’s database based on the details in the form.

A **Package Delivery** voucher when created, should be able to create a reservation to prevent anyone else from reserving the locker. It should also unlock the locker initially in order to allow the courier to place the package inside.

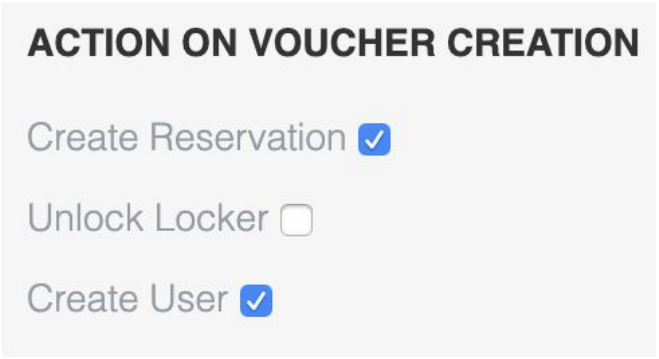
A **Visitor Pass** voucher when created, should only be able to create a temporary user into the database. It should not be able to create a reservation or unlock a locker like a normal user, as they will only be around for a short period and not even use the voucher.


ACTION ON VOUCHER CREATION

Create Reservation ☑

Unlock Locker ☑

Create User ☑


ACTION ON VOUCHER CREATION

Create Reservation ☑

Unlock Locker □

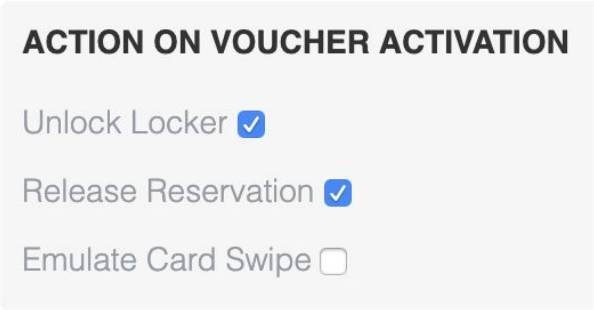
Create User ☑

The third box “Action On Voucher Activation” dictates the actions taken when a voucher has just been activated based on the boxes ticked, similar to Action On Voucher Creation.

- Unlock Locker: Unlocks the locker door.
- Release Reservation: Releases the current reservation from the locker.
- Emulate Card Swipe: Essentially makes the QR code behave like a swipe card, without a CSN number.

A **Package Delivery** voucher when activated, should unlock the locker to allow the user to pick up their package. It should also release the reservation that was created when the voucher was created to free up the locker. There is no need to emulate a card swipe as the locker will only be unlocked once.

A **Visitor Pass** voucher when activated, should only emulate a card swipe as the visitor will be using the locker on a continuous basis until the expiry date of the voucher.

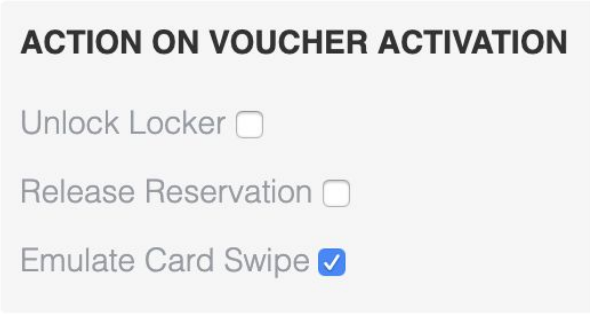


ACTION ON VOUCHER ACTIVATION

Unlock Locker ☑

Release Reservation ☑

Emulate Card Swipe □



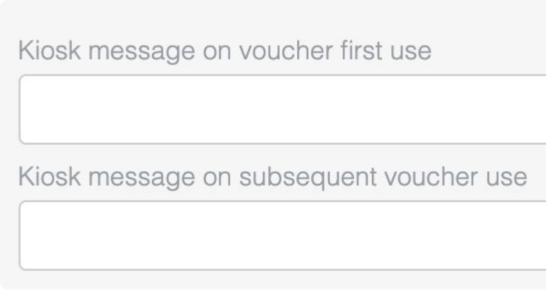
ACTION ON VOUCHER ACTIVATION

Unlock Locker □

Release Reservation □

Emulate Card Swipe ☑

The fourth box essentially allows the administrator to add in broadcast messages onto the Kiosk when the vouchers have been used for the first and subsequent times.

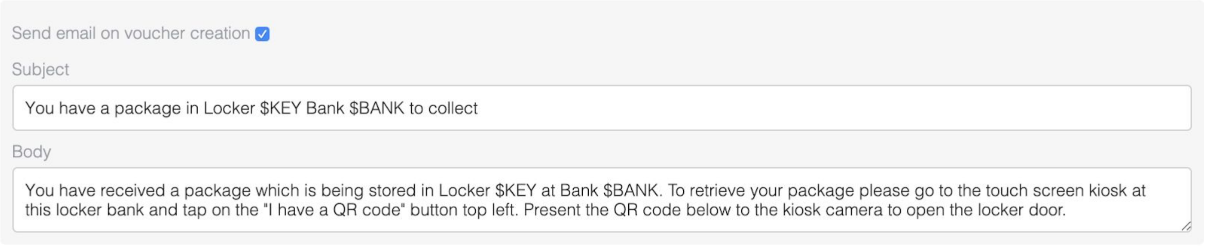


Kiosk message on voucher first use

Kiosk message on subsequent voucher use

The fifth box essentially contains the fields to send a notification email to the user i.e. the Subject and the Body.

Note that under the **Package Delivery** template, the words “$KEY” and “$BANK” are present. Although the contents of the message can be edited in the Subject and Body fields, those two words **SHOULD NOT BE OMITTED** as these are key words for the program when the email is sent. “$KEY” refers to the associated locker number, and “$BANK” refers to the associated Locker Bank name.



Send email on voucher creation ☑

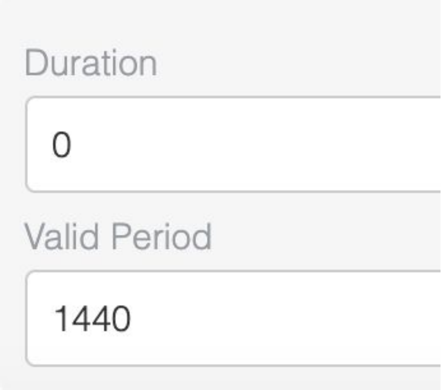
Subject

You have a package in Locker $KEY Bank $BANK to collect

Body

You have received a package which is being stored in Locker $KEY at Bank $BANK. To retrieve your package please go to the touch screen kiosk at this locker bank and tap on the "I have a QR code" button top left. Present the QR code below to the kiosk camera to open the locker door.

The last box contains Duration and Valid Period fields. These indicate the validity of the voucher prior to it being activated. Note that the Valid Period field is in minutes.



Duration

0

Valid Period

1440

4.0 System Maintenance

This section describes how to test and replace any failed locks within a locker bank.

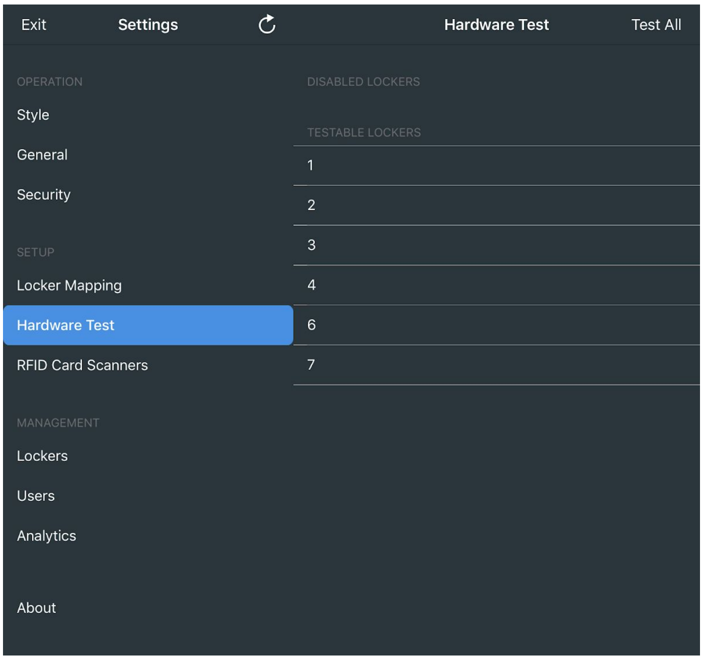
4.1 Locker Hardware Testing

Hardware testing is invoked on a per locker basis and carried out via the kiosk interface where the locker is physically located.

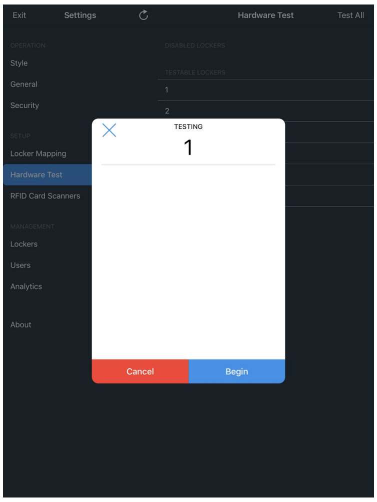
Hardware testing allows user to test the individual features of a single locker in order to prove fully operational. If the locker fails any of the tests the user can mark the locker *disabled* to take it out of pool of available lockers while a replacement locker can be sourced and installed.

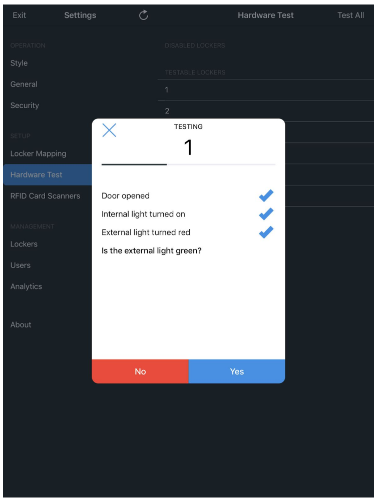
To test a locker select the locker then confirm each operation works in order. If any fail then the system will ask if the locker should be placed in Disabled mode.

Login to the Kiosk Admin interface as per the method described in section 2.1 above, then follow the below workflow:



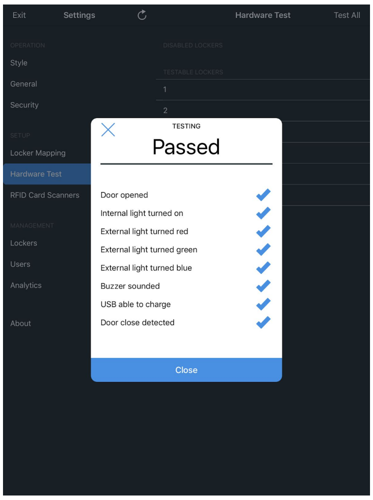
Select locker to perform hardware test on from list of testable lockers.



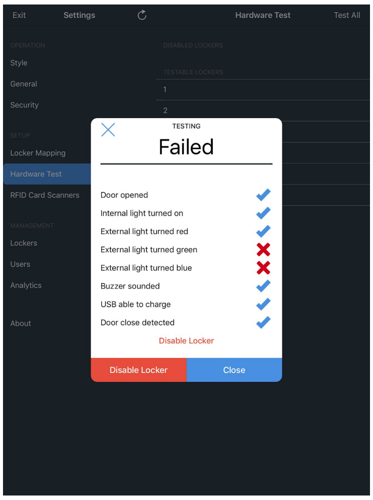


Door opened ✓
Internal light turned on ✓
External light turned red ✓
Is the external light green?

Progress through the tests by answering each question.



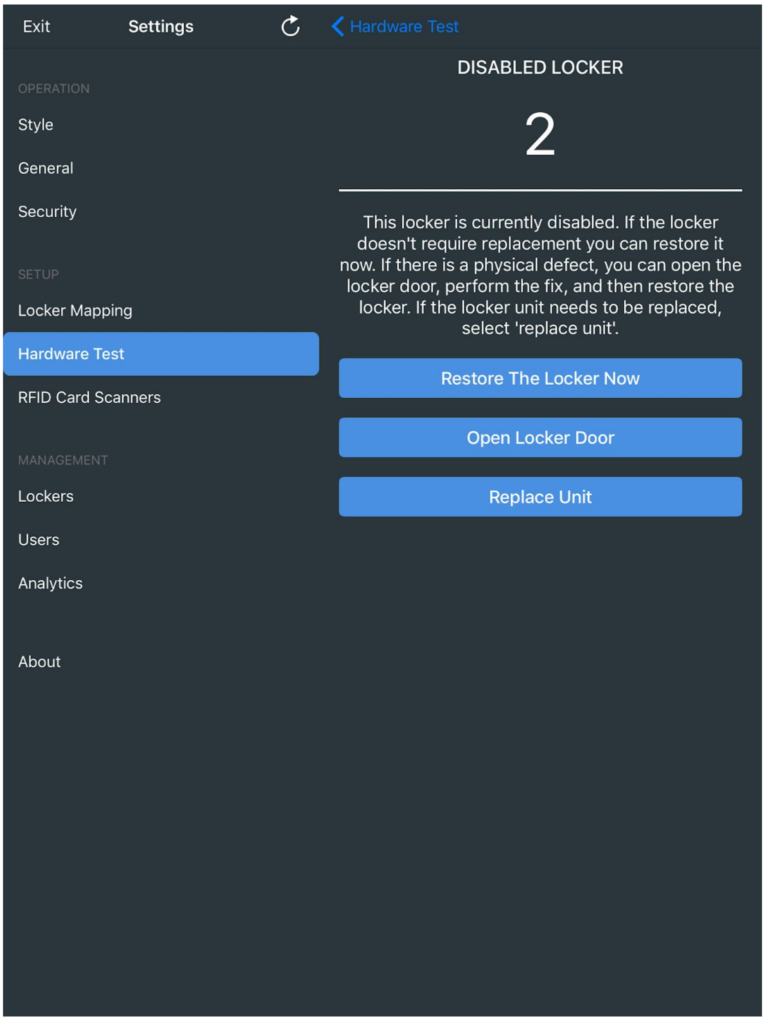
Door opened ✓
Internal light turned on ✓
External light turned red ✓
External light turned green ✓
External light turned blue ✓
Buzzer sounded ✓
USB able to charge ✓
Door close detected ✓



Door opened ✓
Internal light turned on ✓
External light turned red ✓
External light turned green ✗
External light turned blue ✗
Buzzer sounded ✓
USB able to charge ✓
Door close detected ✓

If all tests pass, then the locker passes. If any of the tests fail then the locker will fail the test.

If the locker fails the test then the user is given option to disable the locker. A disabled locker cannot be assigned to any user via fixed or adhoc reservation until it is replaced or otherwise returned to service

 Exit Settings Hardware Test OPERATION Style General Security SETUP Locker Mapping Hardware Test RFID Card Scanners MANAGEMENT Lockers Users Analytics About Restore The Locker Now Open Locker Door Replace Unit DISABLED LOCKER 2 This locker is currently disabled. If the locker doesn't require replacement you can restore it now. If there is a physical defect, you can open the locker door, perform the fix, and then restore the locker. If the locker unit needs to be replaced, select 'replace unit'.	To return the failed locker to service without replacing it - for example where the fault is not important, tap “Restore the Locker Now”. To replace the locker if a replacement is available then use the Replace Unit button which will walk through the removal of the locker from the bank and the mapping of the replacement into the old lockers ID.

4.2 Access to Slave / Standalone Web Administration

Each standalone or slave controller has a web interface used to perform low level tasks. Access to this interface is restricted to Smartalock technicians.
The Kiosk Admin interface is protected by a default PIN number - set to 5555, or to a different code that is set during the commissioning of the system as agreed with the customer. To change this PIN code requires access to the IP interface of the Smartalock slave or standalone controllers Web Interface, so as such will require a Smartalock Technician to perform.

4.3 Automatic Database Backups

The Smartalock Master server runs a database backup to the Smartalock cloud service once per day. These database records are encrypted and stored by Smartalock in case the Smartalock master hardware fails and needs to be replaced. It is therefore important that the

Smartalock master continues to have access to the Internet in order to perform these automatic backups.

The Database backups can also be used by the customers Administrator in case of inadvertent deletion of many user accounts / reservations