CA4K™

iLock For Continental App

User Guide

Revision: Rev L

Date: 2/9/2022

DISCLAIMER

Continental Instruments LLC makes no representations or warranties with respect to the contents hereof and specifically disclaim any implied warranties of merchantability or fitness for any particular purpose. Further, Continental Instruments LLC reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of Continental Instruments LLC to notify any person of such revision or changes.

This document contains proprietary information of NAPCO Security Technologies. Unauthorized reproduction of any portion of this manual without the written authorization of NAPCO Security Technologies is prohibited. The information in this manual is for informational purposes only. It is subject to change without notice. Companies, names and data used in examples herein are fictitious unless otherwise noted. NAPCO Security Technologies assumes no responsibility for incorrect information this manual may contain.

A NAPCO SECURITY TECHNOLOGIES COMPANY
Publicly traded on NASDAQ   Symbol: NSSC

Visit our websites:
http://www.cicaccess.com/
http://www.napcosecurity.com/
http://www.alarmlock.com/

Table of Contents

Must Read before you begin installation

- Prior to programming the CA4K™, verify you have an Android (Jellybean 4.0 or later) or iOS mobile device with an internet connection to download the CA4K™ iLock for Continental app.

- Verify you have a wireless lock model that contains Bluetooth LE technology or a continental panel that includes one or more Bluetooth Reader

- Bluetooth credentials that reside within the iLock for Continental App works essentially as any other type of proximity credential; simply launch the iLock for Continental app and tap the Unlock button to allow entry.

- The Mobile credential can be sent to the mobile device via SMS, Email, upload a file to cloud or "On the Screen QR code". This document will only cover the "On the Screen QR code" method.

Overview

This document provides an overview of downloading and installing the CA4K™ iLock for Continental app on an Android or iOS mobile device. Once downloaded and installed, the CA4K software can create and send a Bluetooth credential to the iOS or Android Mobile device. The credential can be sent via Email, SMS, a scanned QR code or a file on the cloud. This document will only cover one of these available methods. The method discussed will be the scanning of a QR code. Once the credential is on the mobile device, it can be imported, thus making that mobile device a valid "User" of the lock/Panel. Only wireless locks or Continental panels containing Bluetooth LE technology is supported with the iLock for Continental app.

Prerequisites

- A functional CA4K System with version 1.1.5x or later.

- An Android (Jellybean 4.0) or iOS (V9.0 or later) mobile device with Bluetooth connectivity.

- A Continental panel reader / lock model that contains Bluetooth LE technology.

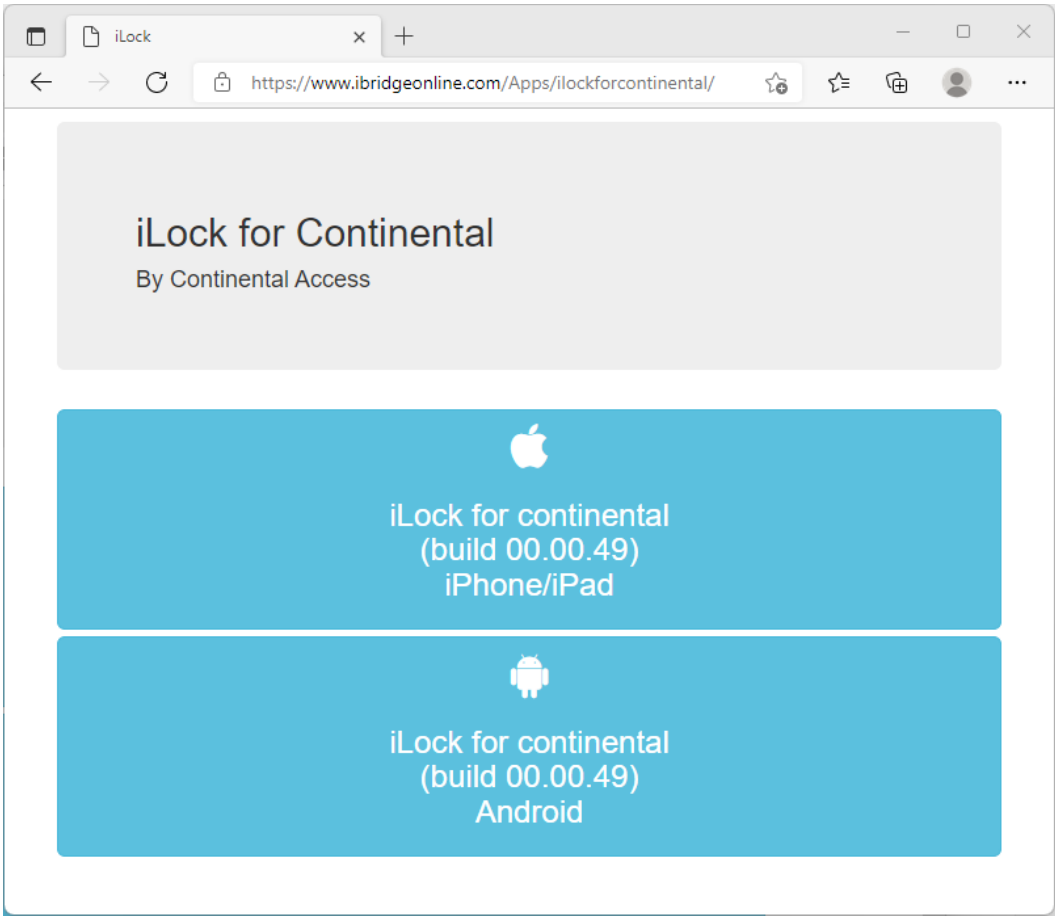
Downloading the iLock for Continental App

- Download the iLock for Continental Android or iOS app from the app store (Google Play Store / Apple App Store).

- If the App is still in testing, the user can download it from the following link. https://www.ibridgeonline.com/apps/iLockForContinental/

- Upon accessing the link, a menu will display with two options. The first option is iOS (iPhone/iPad), and the second option is for Android.

- Download the app that is compatible with the user's mobile device.



iLock for Continental

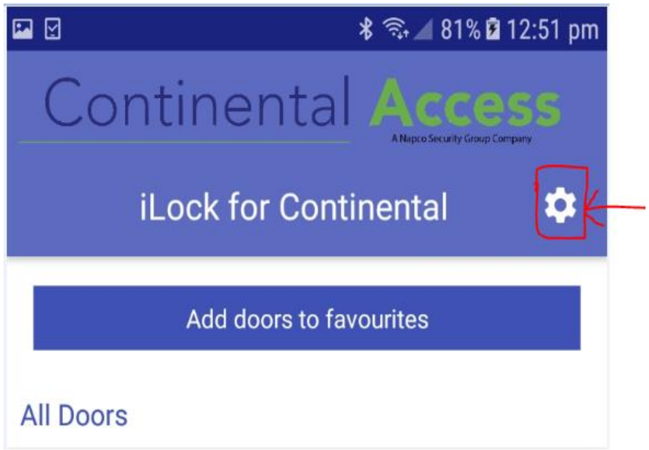
By Continental Access

Installing the iLock for Continental App

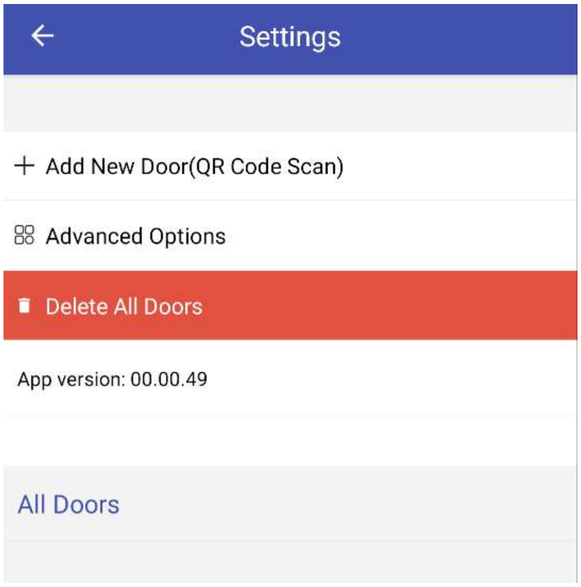
- Upon downloading the iLock for Continental app onto the user’s Android or IOS mobile device, install the iLock for Continental App on the IOS or Android device.

  Note: Due to the iLock for Continental app being downloaded from a website, the user might have to modify the security settings in the Mobile device to allow an unknown app to install. The user might be prompted for this setting automatically, or the user might have to go into Settings>Security on the mobile device.

- After the installation is done, click the Settings button (Marked in the Picture).



- Upon clicking the Settings button, the below screen will appear with options: **Add New Door (QR Code Scan), Advanced Options**, and **Delete All Locks**.



- **Add New Door** (QR Code Scan) menu could be the frequently used menu to import doors and mobile credentials.

- Advanced Options can add Admin Door (**Add New Admin door**) and Manual Credential (**Add Manual Credential**). These options are used for administrative purposes only.

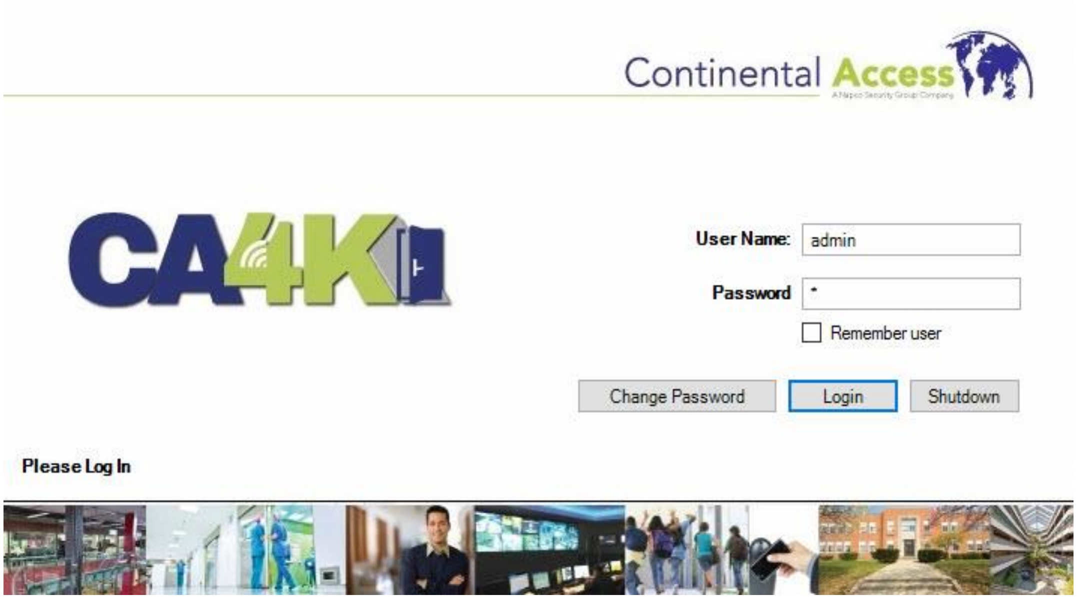
Configuring the CA4K™ Software for iLock for Continental App

- To Launch the CA4K™ software, Click the CardAccess 4K icon on the desktop.

- The CA4K™ **Log In** screen will display.

Log In to CA4K™

- Type the default **User name** (admin) and **password** (admin@4k) or valid credentials given by the access control administrator. Click **Login**. The CA4K™ event grid will display.



User Name: admin

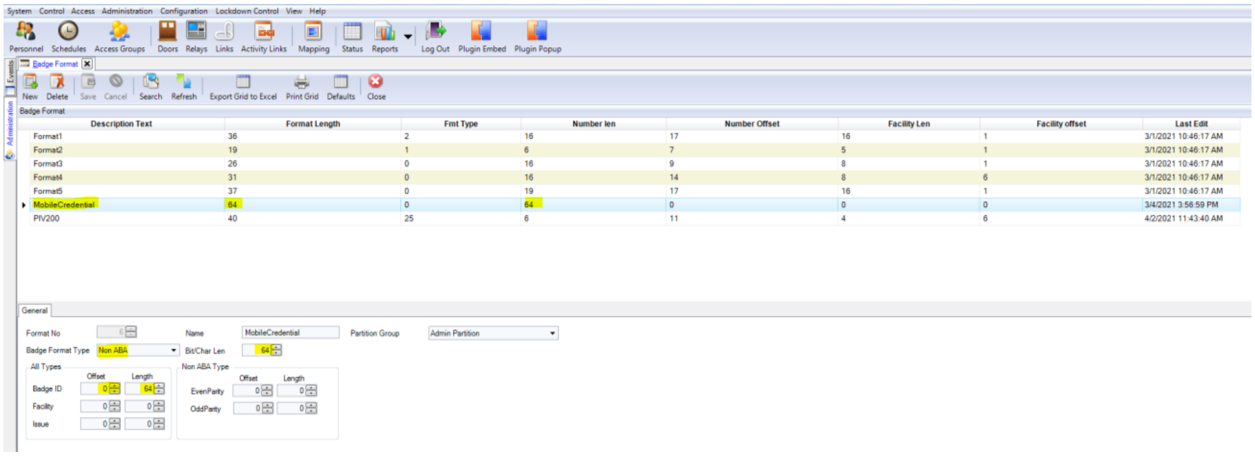
Password: *

□ Remember user

Please Log In

Configure a 64-bit Badge Format

- Mobile credentials require a 64-bit custom badge format.
- Click **Administration/Badge Formats** from the main menu. The **Badge Format** screen will display.
- Click **New**.
- Configure a 64-bit badge format precisely as per the screen below.
- Click **Save** and **Close**.



Badge Format

Description Text	Format Length	Fmt Type	Number len	Number Offset	Facility Len	Facility offset	Last Edit
Format1	36	2	16	17	16	1	3/1/2021 10:46:17 AM
Format2	19	1	6	7	5	1	3/1/2021 10:46:17 AM
Format3	26	0	16	9	8	1	3/1/2021 10:46:17 AM
Format4	31	0	16	14	8	6	3/1/2021 10:46:17 AM
Format5	37	0	19	17	16	1	3/1/2021 10:46:17 AM
MobileCredential	64	0	64	0	0	0	3/4/2021 3:56:59 PM
PIV200	40	25	6	11	4	6	4/2/2021 11:43:40 AM

Format No: 6
Name: MobileCredential
Partition Group: Admin Partition
Badge Format Type: Non ABA
Bit/Char Len: 64

All Types

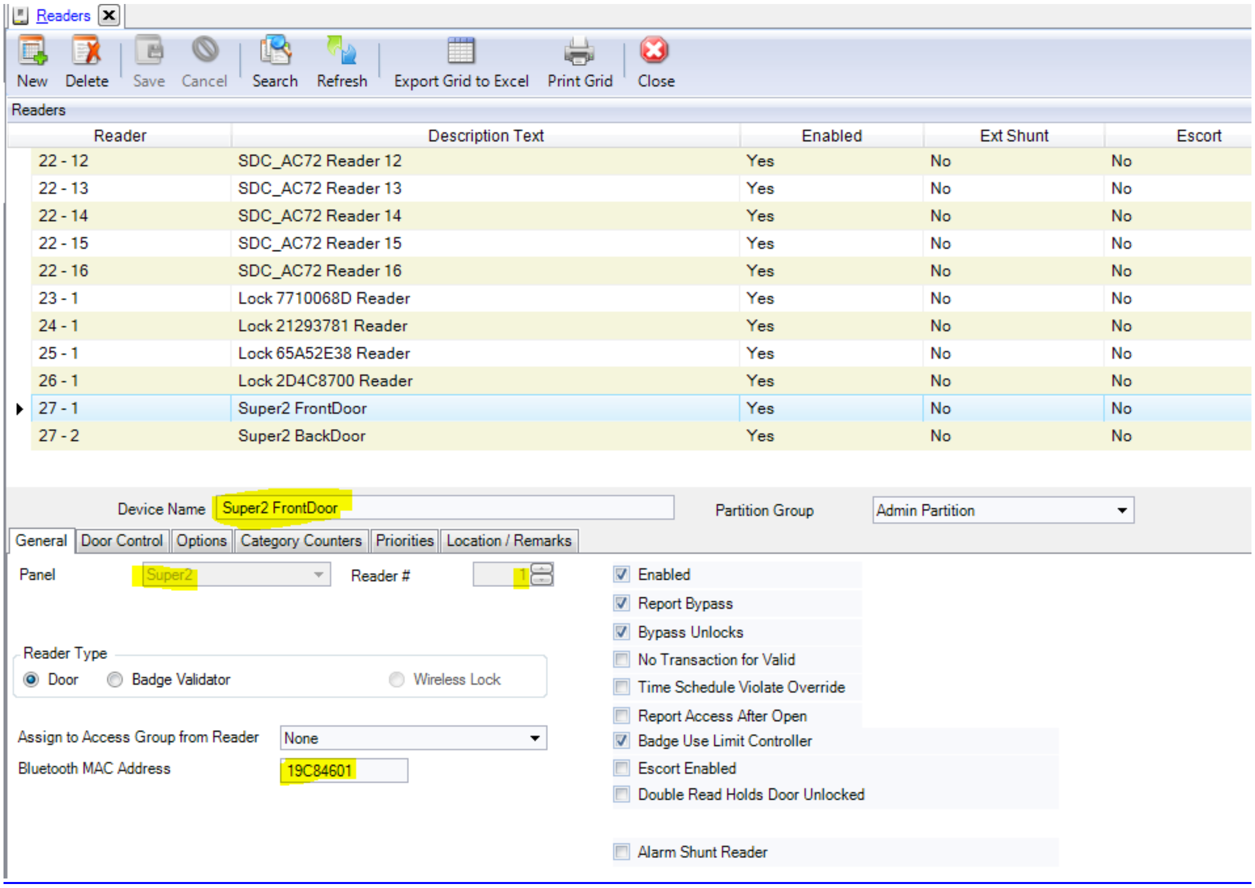
	Offset	Length
Badge ID	0	64
Facility	0	0
Issue	0	0

Non ABA Type

	Offset	Length
EvenParity	0	0
OddParity	0	0

Reader configuration for Locks and Panels

- Enter the **last eight characters** of the Bluetooth readers MAC address, in the **Bluetooth MAC Address** field in the reader screen (MAC address will be printed as text or barcode on the back of the Reader).



Readers

Reader	Description Text	Enabled	Ext Shunt	Escort
22 - 12	SDC_AC72 Reader 12	Yes	No	No
22 - 13	SDC_AC72 Reader 13	Yes	No	No
22 - 14	SDC_AC72 Reader 14	Yes	No	No
22 - 15	SDC_AC72 Reader 15	Yes	No	No
22 - 16	SDC_AC72 Reader 16	Yes	No	No
23 - 1	Lock 7710068D Reader	Yes	No	No
24 - 1	Lock 21293781 Reader	Yes	No	No
25 - 1	Lock 65A52E38 Reader	Yes	No	No
26 - 1	Lock 2D4C8700 Reader	Yes	No	No
27 - 1	Super2 FrontDoor	Yes	No	No
27 - 2	Super2 BackDoor	Yes	No	No

Device Name: Super2 FrontDoor
Partition Group: Admin Partition

Panel: Super2
Reader #: 1

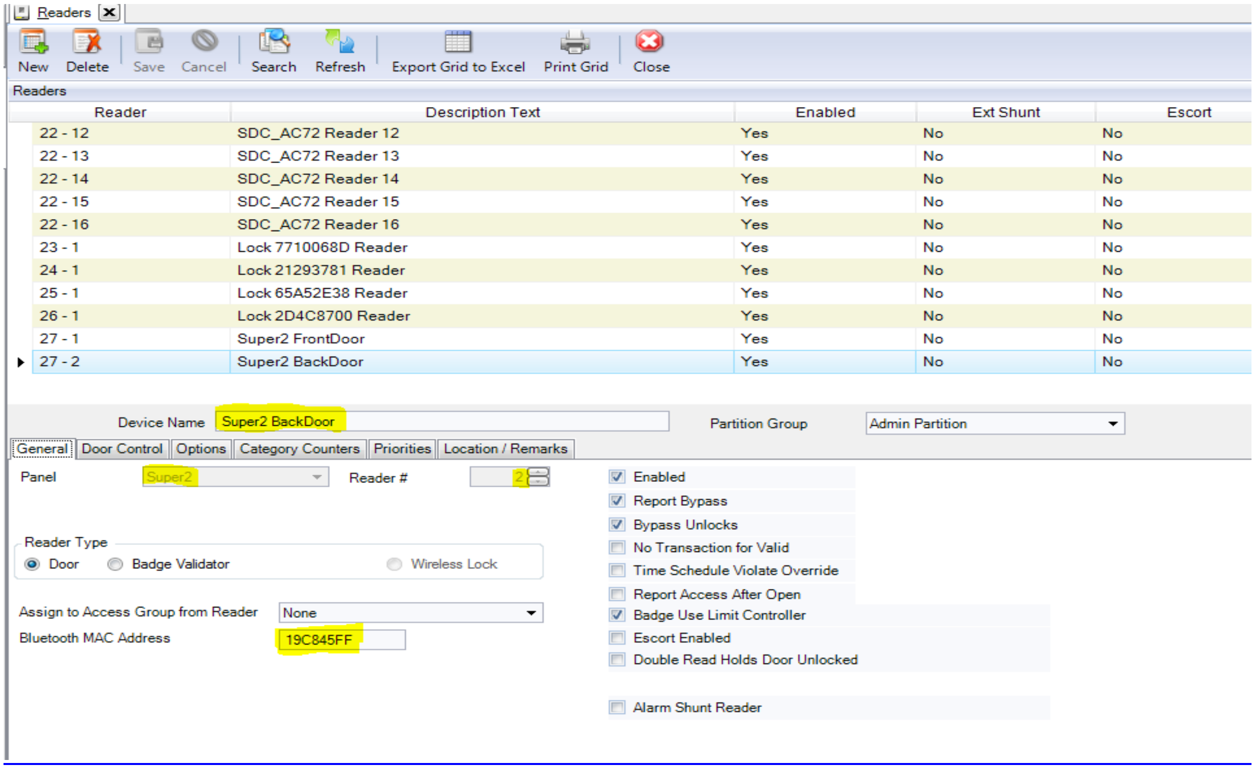
Reader Type
● Door ○ Badge Validator ○ Wireless Lock

Assign to Access Group from Reader: None
Bluetooth MAC Address: 19C84601

☑ Enabled
☑ Report Bypass
☑ Bypass Unlocks
☐ No Transaction for Valid
☐ Time Schedule Violate Override
☐ Report Access After Open
☑ Badge Use Limit Controller
☐ Escort Enabled
☐ Double Read Holds Door Unlocked

☐ Alarm Shunt Reader

- Similarly, the user can configure other available readers (if required) for the Locks and Panels.



Reader	Description Text	Enabled	Ext Shunt	Escort
22 - 12	SDC_AC72 Reader 12	Yes	No	No
22 - 13	SDC_AC72 Reader 13	Yes	No	No
22 - 14	SDC_AC72 Reader 14	Yes	No	No
22 - 15	SDC_AC72 Reader 15	Yes	No	No
22 - 16	SDC_AC72 Reader 16	Yes	No	No
23 - 1	Lock 7710068D Reader	Yes	No	No
24 - 1	Lock 21293781 Reader	Yes	No	No
25 - 1	Lock 65A52E38 Reader	Yes	No	No
26 - 1	Lock 2D4C8700 Reader	Yes	No	No
27 - 1	Super2 FrontDoor	Yes	No	No
27 - 2	Super2 BackDoor	Yes	No	No

Device Name: Super2 BackDoor

Partition Group: Admin Partition

Panel: Super2

Reader #: 2

Reader Type: ● Door ○ Badge Validator ○ Wireless Lock

Assign to Access Group from Reader: None

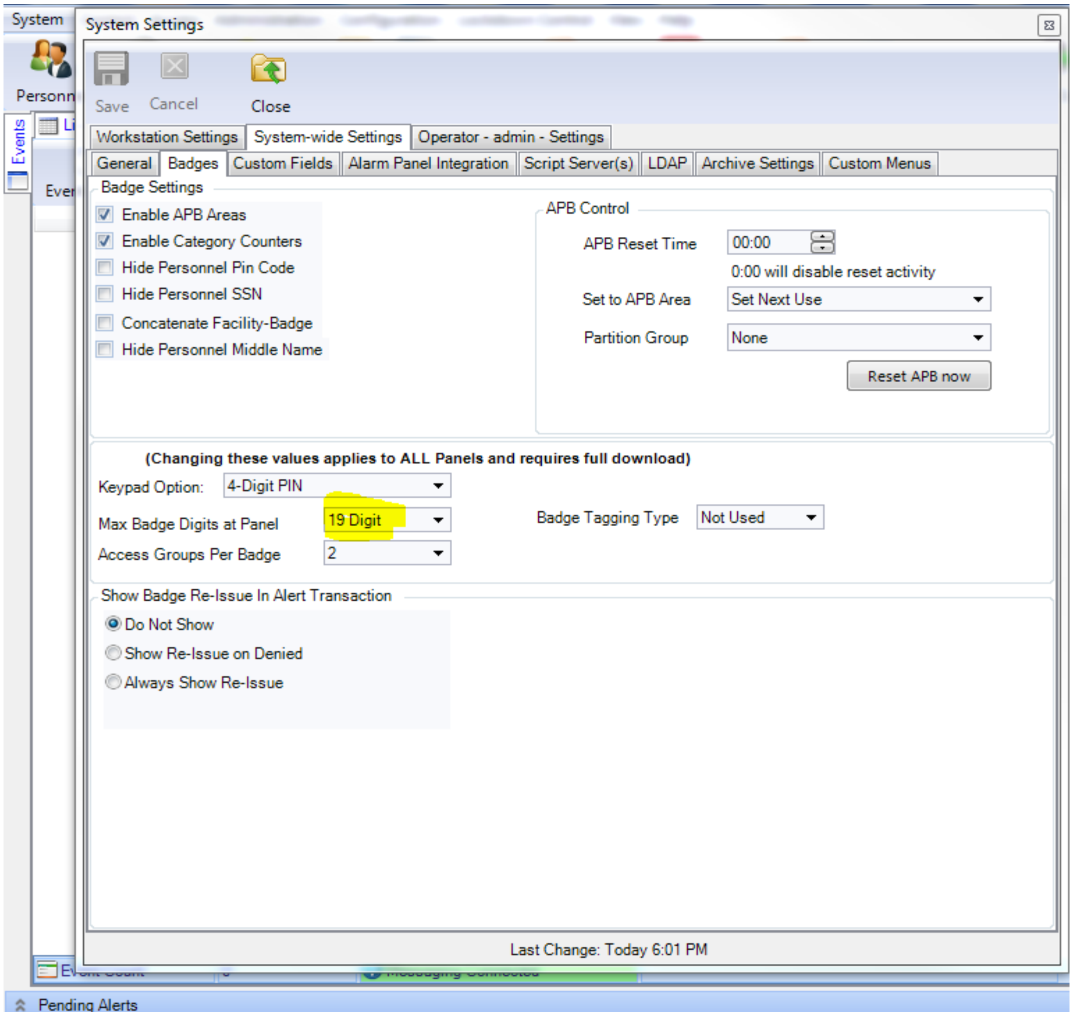
Bluetooth MAC Address: 19C845FF

☑ Enabled
☑ Report Bypass
☑ Bypass Unlocks
☐ No Transaction for Valid
☐ Time Schedule Violate Override
☐ Report Access After Open
☑ Badge Use Limit Controller
☐ Escort Enabled
☐ Double Read Holds Door Unlocked

☐ Alarm Shunt Reader

Add a Bluetooth Credential

- From System Settings, update the Max Badge Digits at Panel to 19 Digits. **System-> System Settings -> System-wide-Settings->Badges->Max Badge Digits at Panel-> 19 Digits**



System Settings

Badge Settings

☑ Enable APB Areas
☑ Enable Category Counters
☐ Hide Personnel Pin Code
☐ Hide Personnel SSN
☐ Concatenate Facility-Badge
☐ Hide Personnel Middle Name

APB Control

APB Reset Time: 00:00
0:00 will disable reset activity
Set to APB Area: Set Next Use
Partition Group: None

(Changing these values applies to ALL Panels and requires full download)

Keypad Option: 4-Digit PIN
Max Badge Digits at Panel: 19 Digit
Access Groups Per Badge: 2
Badge Tagging Type: Not Used

Show Badge Re-Issue In Alert Transaction

● Do Not Show
○ Show Re-Issue on Denied
○ Always Show Re-Issue

Last Change: Today 6:01 PM

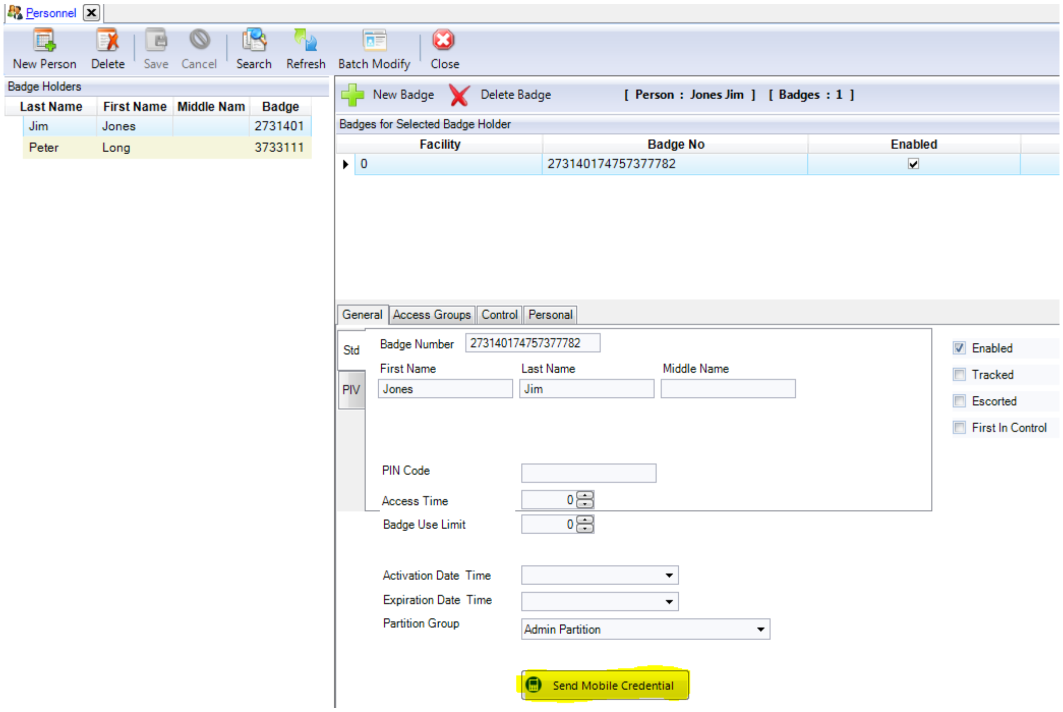
- Perform Full Data Download
- Click **Personnel** on the main toolbar. The **Personnel** screen will display.
- Click **New Person.**
- Click the **Generate Mobile Credential** button. Upon clicking the button, a random badge number will be generated for the Badge Number.

  Very Important: The user must have the 64-Bit Badge format configured for the **Generate Mobile Credential** button to be enabled.

- Type in the First and Last Name of the Badge holder.
- Click the **Mobile Credential** tab on the badge record. Enter the following information for each badge record.
- **Email Address** (optional- only required to send mobile credential by email)
- **Mobile Phone number** (optional-only required to send mobile credential by SMS)
- **SMSDomain** (optional-only required to send mobile credential by SMS)

  Note: Refer Page 21, 25, 26 and 27 for detail

- Click **Send Mobile Credential** button. Upon clicking this button, the **Reader Lookup** screen will display.



[Person : Jones Jim] [Badges : 1]

Badge Holders

Last Name	First Name	Middle Nam	Badge
Jim	Jones		2731401
Peter	Long		3733111

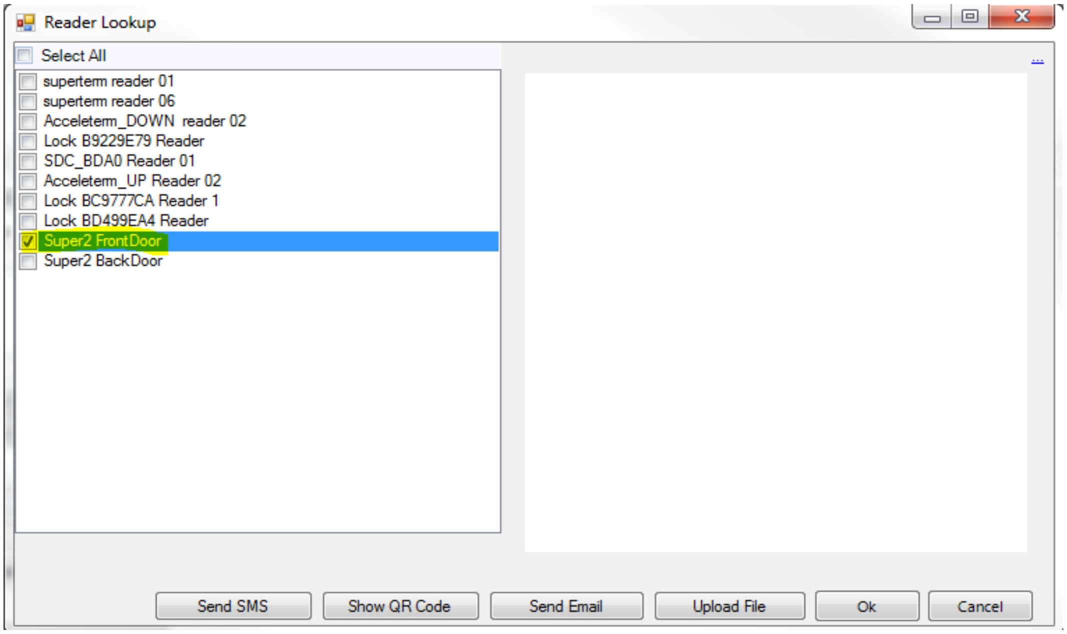
Badges for Selected Badge Holder

Facility	Badge No	Enabled
0	273140174757377782	☑

Badge Number	273140174757377782
First Name	Jones
Last Name	Jim
Middle Name	
PIN Code	
Access Time	0
Badge Use Limit	0
Activation Date Time	
Expiration Date Time	
Partition Group	Admin Partition

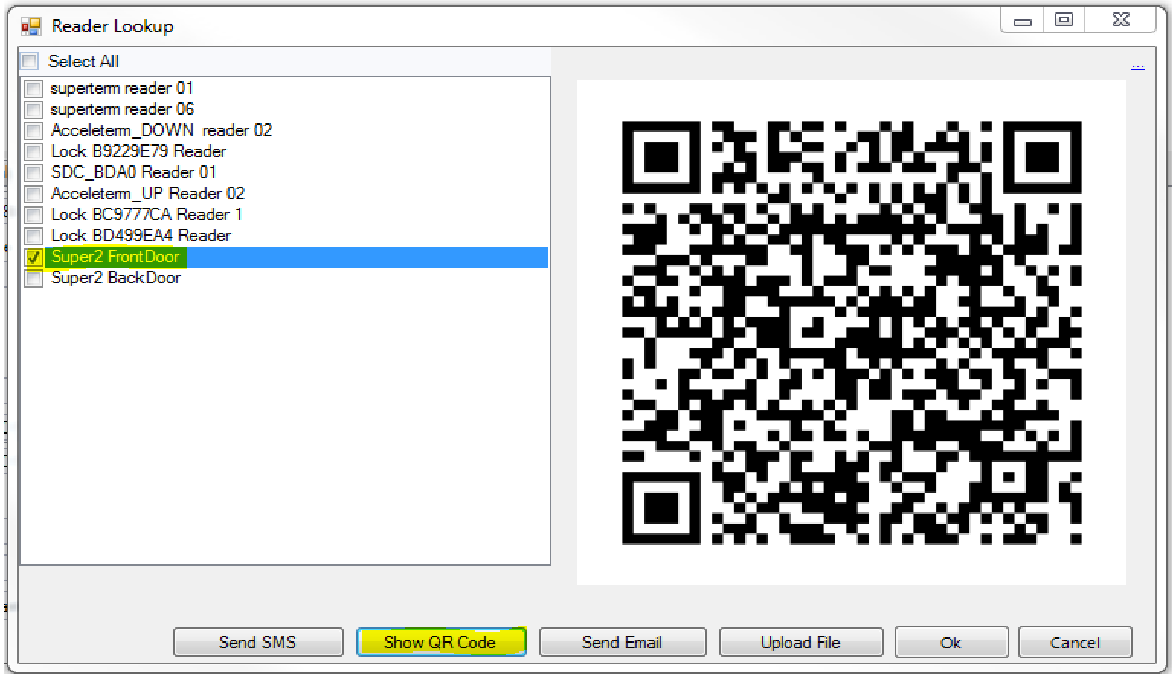
☑ Enabled
☐ Tracked
☐ Escorted
☐ First In Control

- Select the Reader(s) to send the credential. Upon selecting the Reader(s), the **Send SMS**, **Show QR Code**, **Send Email**, **Upload File** Tabs will enable. For our demonstration in this document, we will only perform the **On-Screen QR Code**.



☐ Select All
☐ superterm reader 01
☐ superterm reader 06
☐ Acceletem_DOWN reader 02
☐ Lock B9229E79 Reader
☐ SDC_BDA0 Reader 01
☐ Acceletem_UP Reader 02
☐ Lock BC9777CA Reader 1
☐ Lock BD499EA4 Reader
☑ Super2 FrontDoor
☐ Super2 BackDoor

- Click the **Show QR Code** Tab. Upon clicking **Show QR Code**, the QR code will display on the right side of the screen.



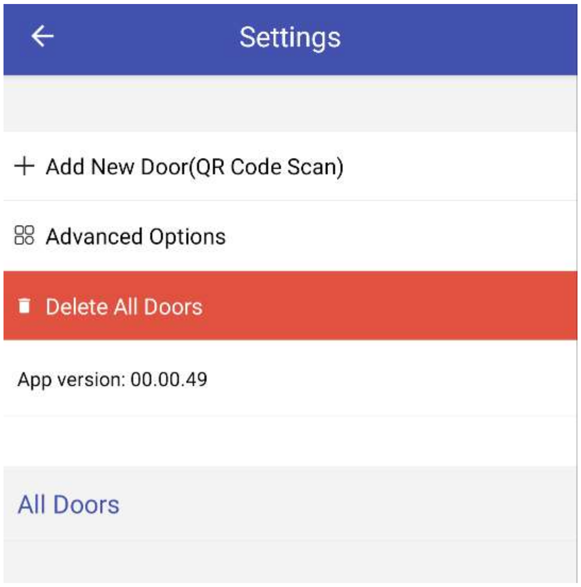
Reader Lookup

□ Select All

□ superterm reader 01
□ superterm reader 06
□ Acceleterm_DOWN reader 02
□ Lock B9229E79 Reader
□ SDC_BDA0 Reader 01
□ Acceleterm_UP Reader 02
□ Lock BC9777CA Reader 1
□ Lock BD499EA4 Reader
☑ Super2 FrontDoor
□ Super2 BackDoor

- Follow the same steps to add Bluetooth credentials with Panels' other available readers (if required).

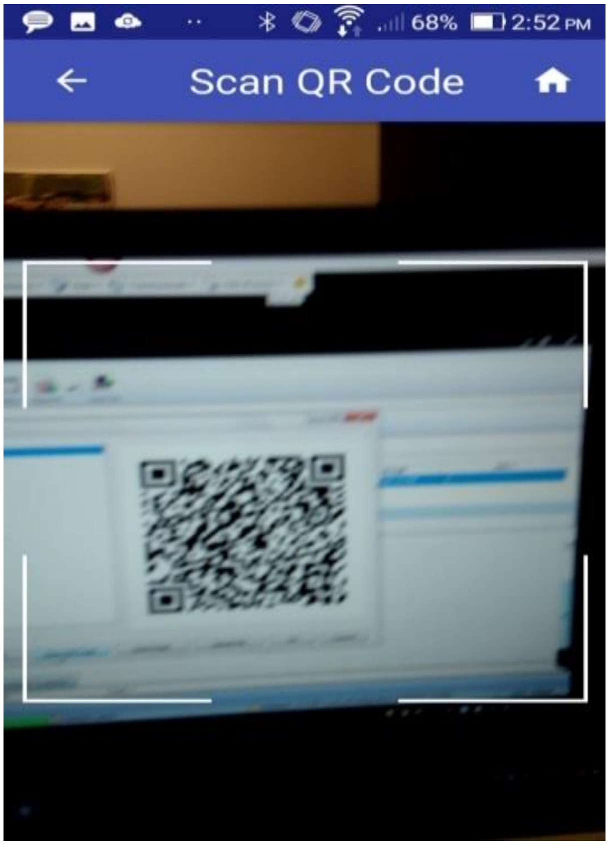
Add New Door (QR Code Scan)

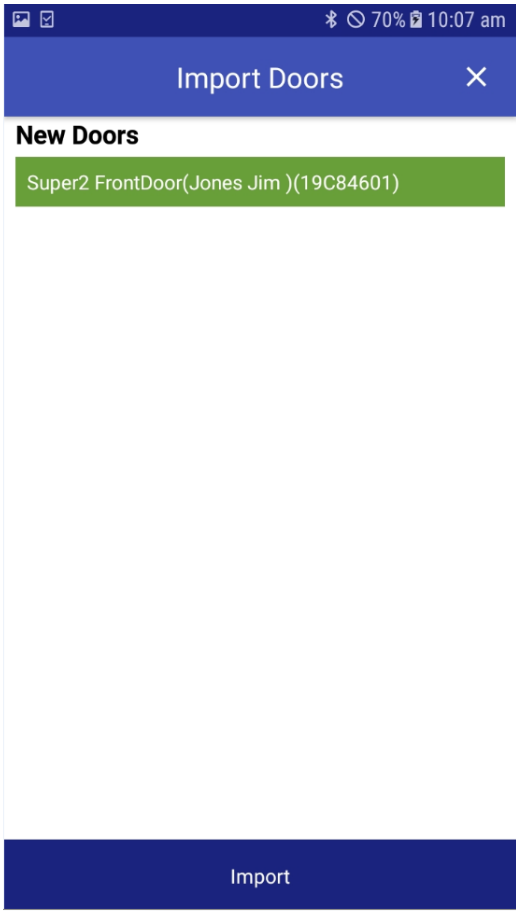


App version: 00.00.49

- On the Settings screen, click the **+ Add New Door (QR Code Scan)** button.
- Align the camera with the QR Code within the guidelines.
- On the iLock for Continental app, click the **Scan QR Code** button.
- Upon clicking the **scan QR code**, the door information will display on the **Import Doors** screen. Click Import to import the doors.

Import Door





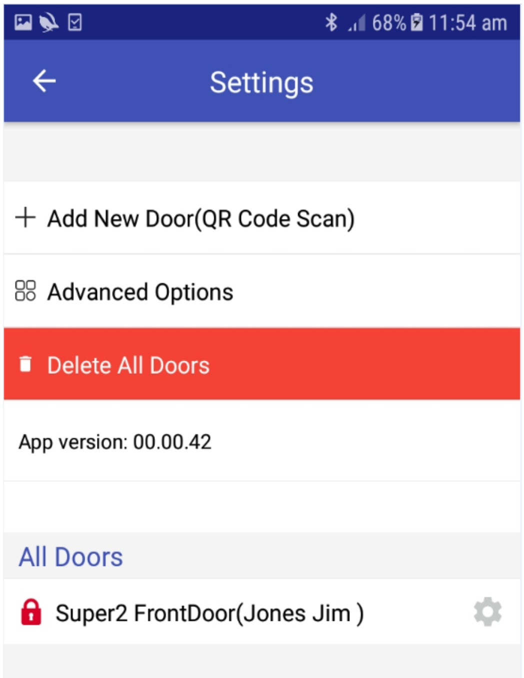
70% 10:07 am

Import Doors

New Doors

Super2 FrontDoor(Jones Jim)(19C84601)

- Upon the Doors being imported, the imported door will display under **All Doors** with a Lock icon. Refer to the screen below.



68% 11:54 am

Settings

App version: 00.00.42

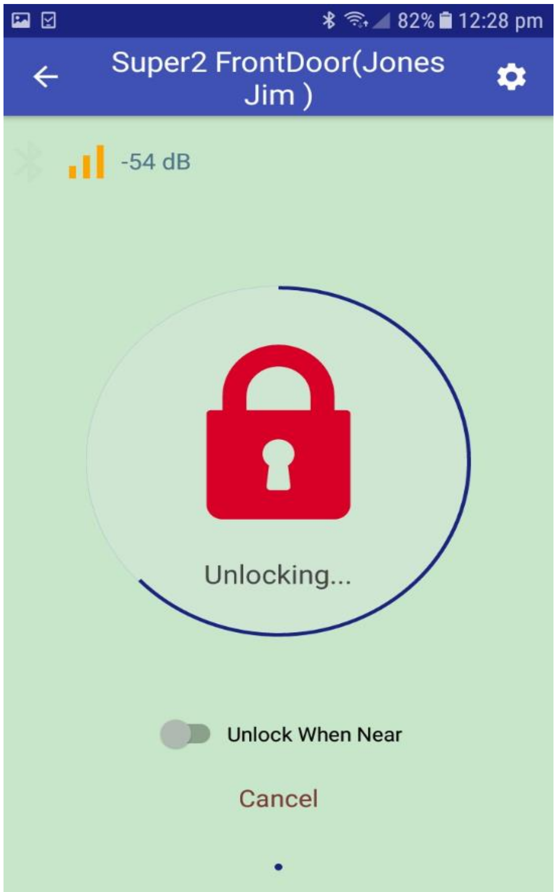
All Doors

🔒 Super2 FrontDoor(Jones Jim)

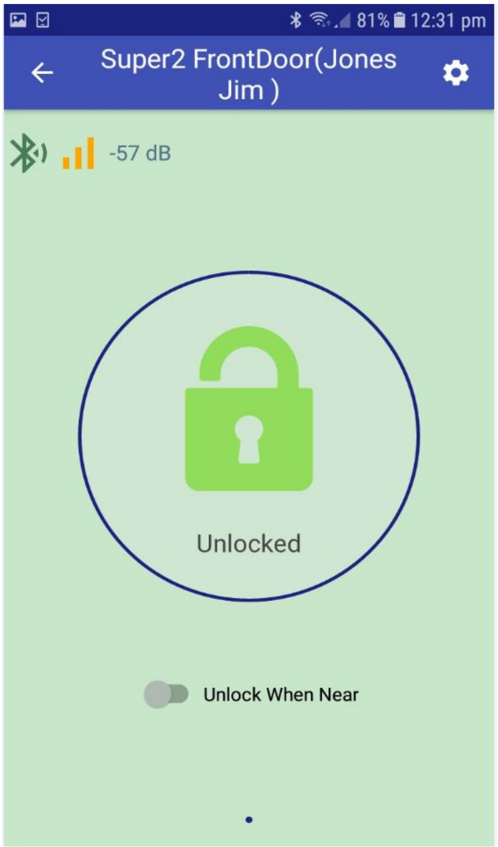
- Once doors are imported, can add selected doors to “Favorite Doors”. Click the menu “Add doors to favorite” to select and add.

Unlock Selected Door

- To unlock the Door, Tap the Lock icon on the Door Screen. While opening, an **Unlocking** icon (Red Lock icon) and Bluetooth signal strength will continue to display on the Door Screen. If the Door Unlocked executes successfully, an **Unlocked** icon **(**Green Lock icon**)** icon will display.



(Unlocking is in Progress)



81% 12:31 pm

Super2 FrontDoor(Jones Jim)

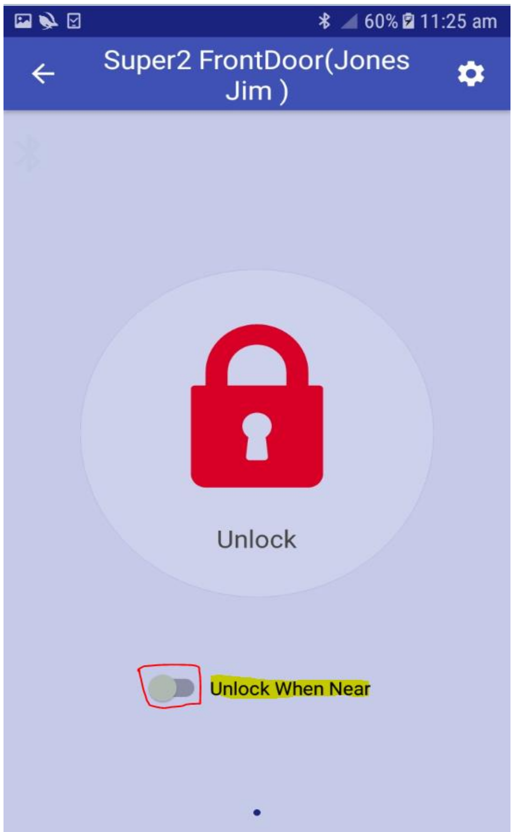
-57 dB

Unlocked

Unlock When Near

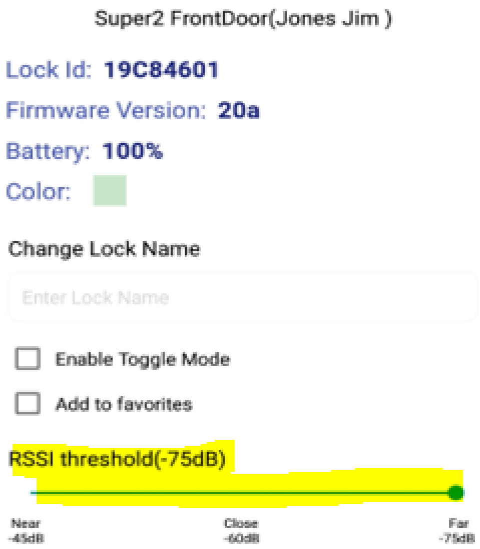
(Unlocking Complete)

- **Unlock When Near** in the door status screen option can restrict the distance to execute the door open operation. By default, **Unlock When Near is** turned off.



(Unlock When Near is **Disabled**)

- Suppose the user enables **Unlock When Near** option, then he/she needs to come in reasonable proximity to the reader to execute the door open operation. Distance is based on the RSSI threshold level set at settings for each door.



Super2 FrontDoor(Jones Jim)

Lock Id: **19C84601**

Firmware Version: **20a**

Battery: **100%**

Color: 🟩

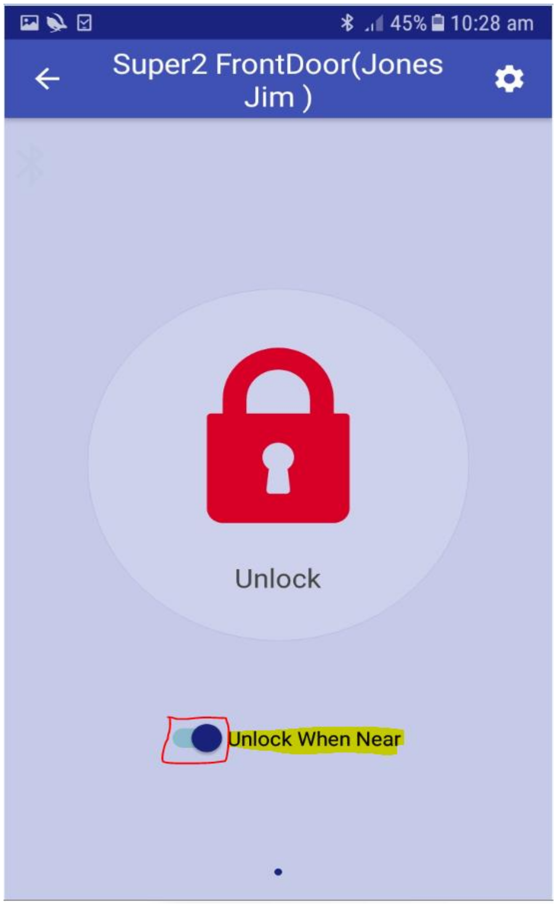
Change Lock Name

Enter Lock Name

□ Enable Toggle Mode

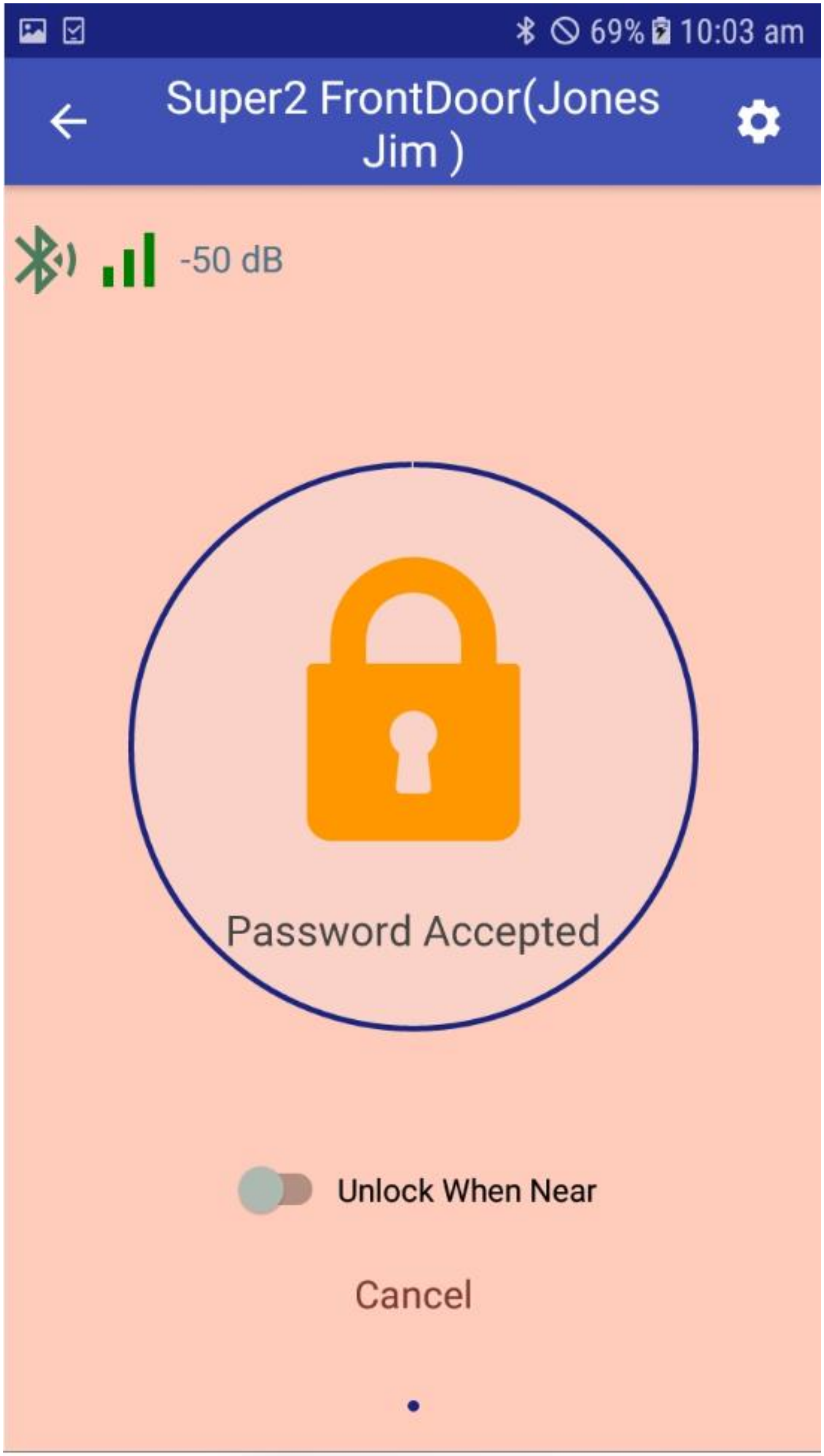
□ Add to favorites

RSSI threshold(-75dB)



(Unlock When Near is **Enabled**)

- The User receives a **Password Accepted** message if he/she tries to execute a door unlock operation, but for some reason, did not receive a feedback signal from the panel.



Super2 FrontDoor(Jones Jim)

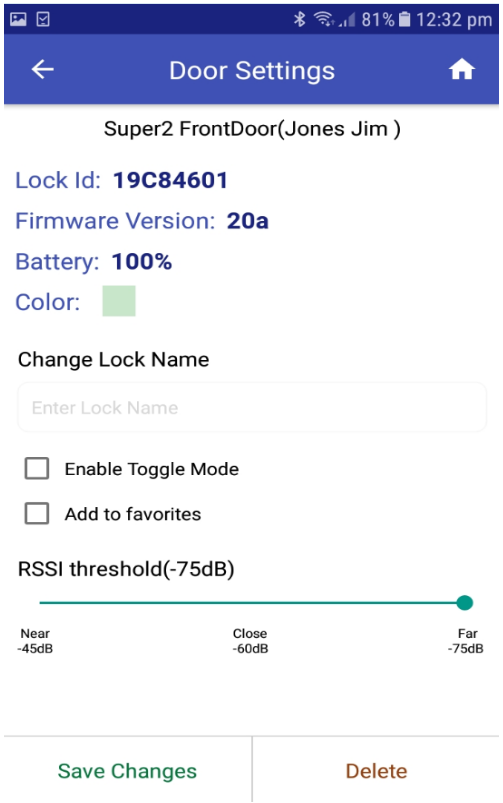
-50 dB

Password Accepted

Unlock When Near

Editing Door Information

- To edit the door information, select the door and click the **Settings** button on the right top corner.
- Edit the door information.
- Click **Save Changes**.



Super2 FrontDoor(Jones Jim)

Lock Id: **19C84601**

Firmware Version: **20a**

Battery: **100%**

Color: 🟩

Change Lock Name

Enter Lock Name

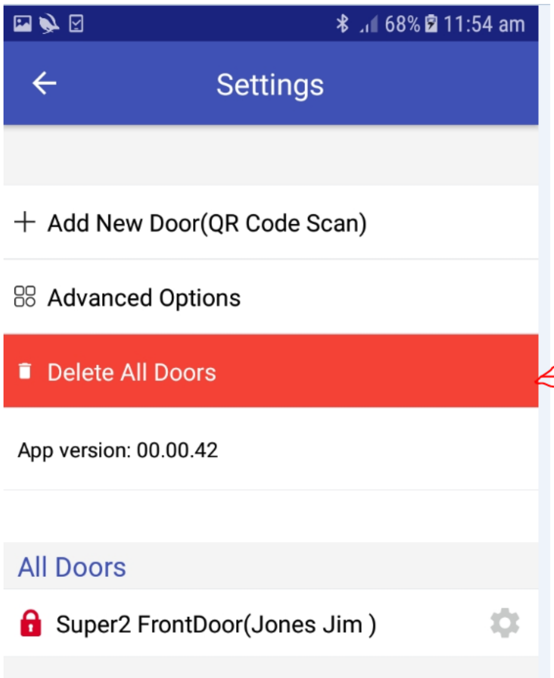
□ Enable Toggle Mode

□ Add to favorites

RSSI threshold(-75dB)

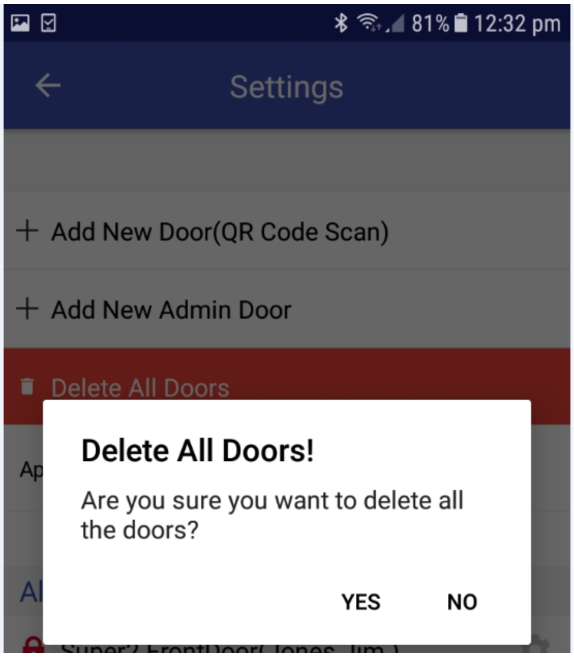
Delete All Doors

- To delete all the Doors, click **Delete All Doors**.



App version: 00.00.42

- Upon clicking **Delete All Doors**, a confirmation message will display as per the screen below.
- Click **Yes**.



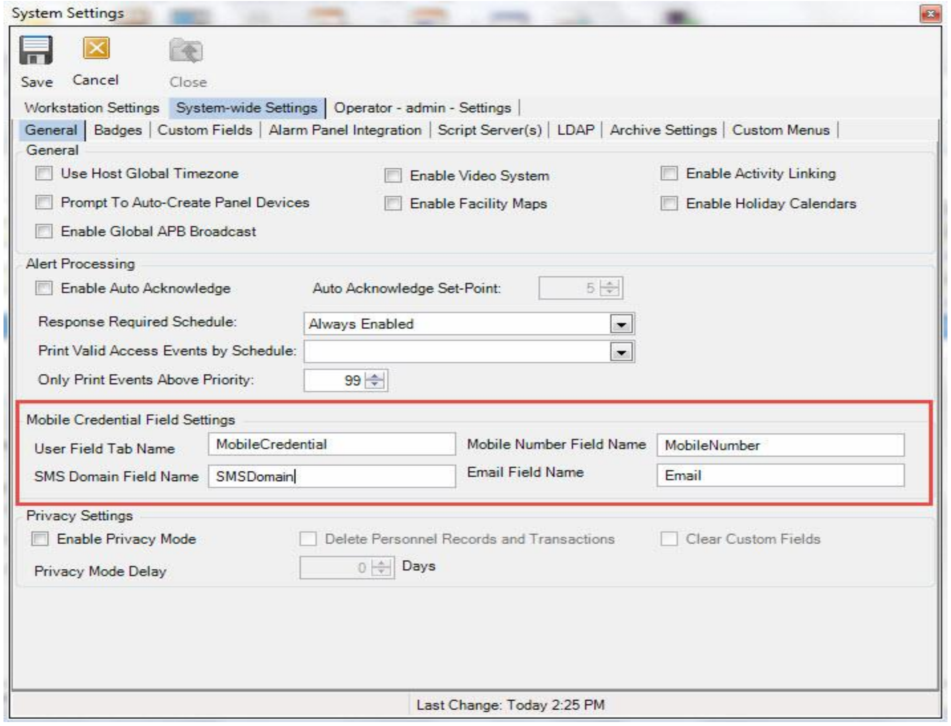
Delete All Doors!

Are you sure you want to delete all the doors?

Send mobile credentials via Email or SMS

Configure Mobile Credential Field Settings in System Settings

- Click **System/System Settings/System-wide Settings.** The System Settings screen will display.
- On the General tab, configure the **Mobile Credential Field Settings** as per the screen below.
- Click **Save.**



General

□ Use Host Global Timezone
□ Enable Video System
□ Enable Activity Linking
□ Prompt To Auto-Create Panel Devices
□ Enable Facility Maps
□ Enable Holiday Calendars
□ Enable Global APB Broadcast

Alert Processing

□ Enable Auto Acknowledge
Auto Acknowledge Set-Point: 5
Response Required Schedule: Always Enabled
Print Valid Access Events by Schedule:
Only Print Events Above Priority: 99

Mobile Credential Field Settings

User Field Tab Name: MobileCredential
Mobile Number Field Name: MobileNumber
SMS Domain Field Name: SMSDomain
Email Field Name: Email

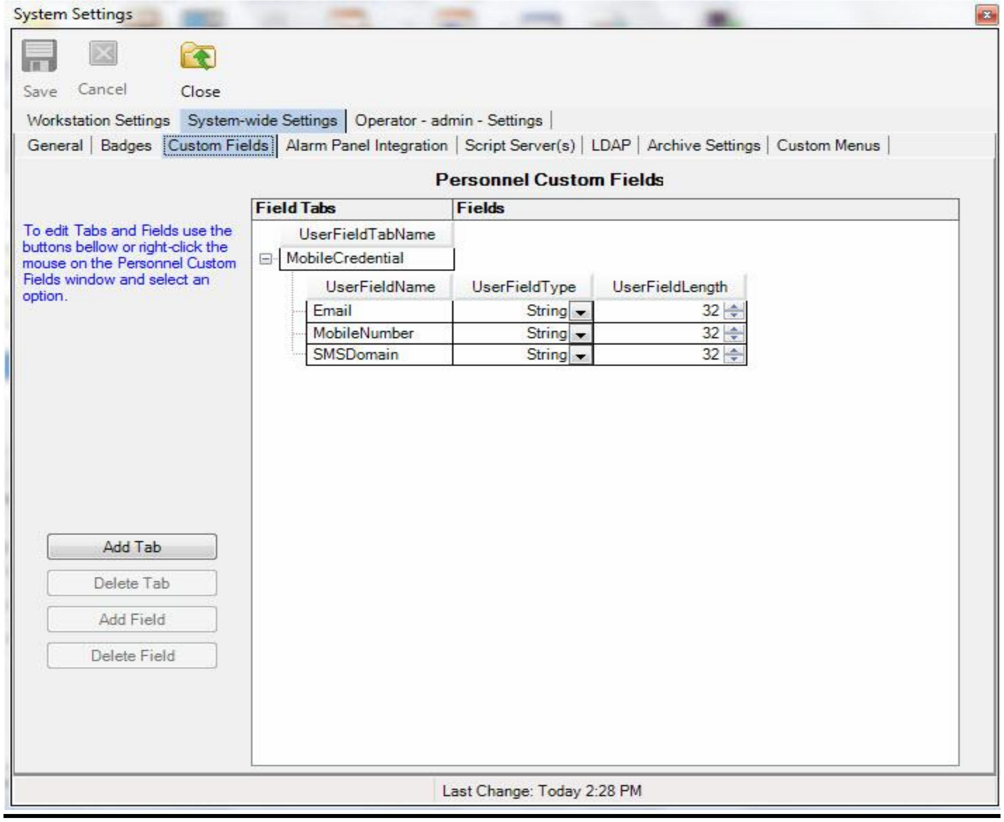
Privacy Settings

□ Enable Privacy Mode
□ Delete Personnel Records and Transactions
□ Clear Custom Fields
Privacy Mode Delay: 0 Days

Last Change: Today 2:25 PM

Configure Personnel Custom Fields in System Settings

- Upon configuring the previous screen, the Personnel Custom Fields will be automatically configured as per the screen below. Please verify that they have been preconfigured. If they have not been preconfigured, they must be manually configured.



Personnel Custom Fields

To edit Tabs and Fields use the buttons bellow or right-click the mouse on the Personnel Custom Fields window and select an option.

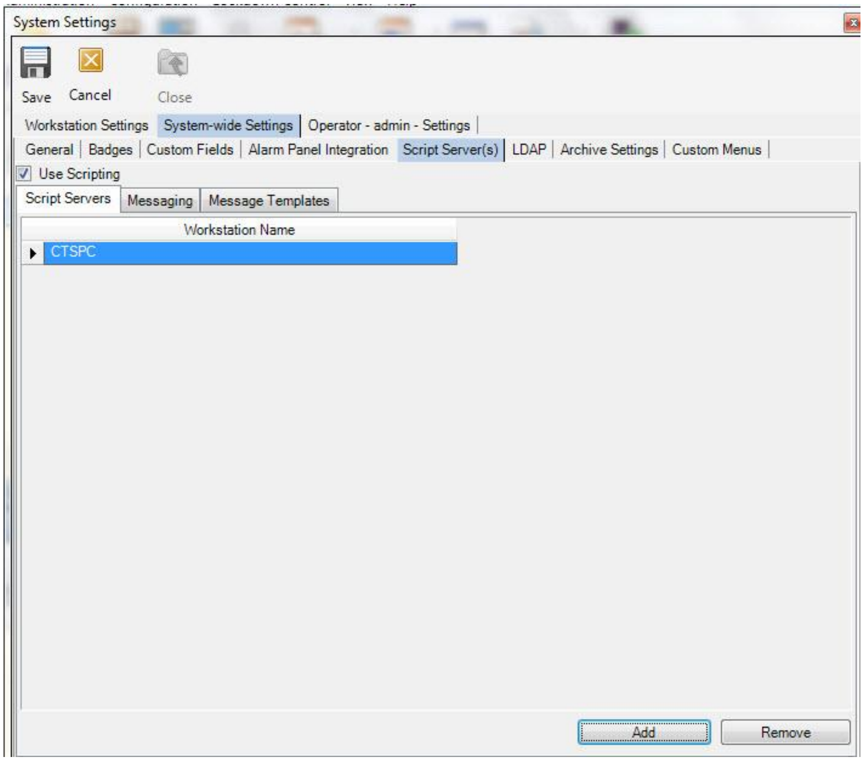
Field Tabs
UserFieldTabName
MobileCredential

UserFieldName	UserFieldType	UserFieldLength
Email	String	32
MobileNumber	String	32
SMSDomain	String	32

Last Change: Today 2:28 PM

Enable Scripting in System Settings

- Enable Scripting in System Settings.



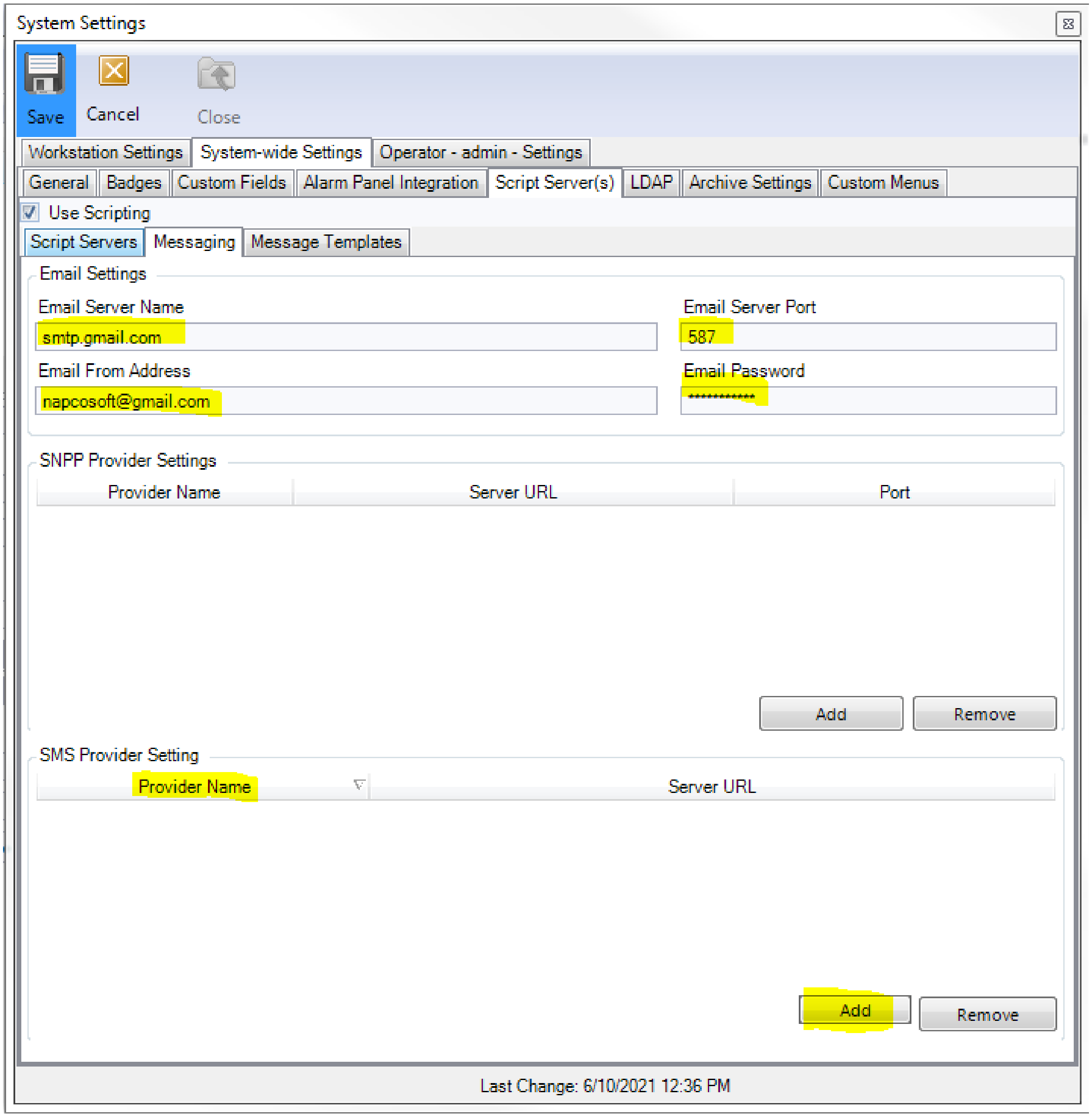
☑ Use Scripting

Workstation Name
CTSPC

Configure Messaging in System Settings

- Click the **Messaging** tab.
- Configure the Messaging tab (Email and SMS) as per the screens below.
- Click **Save**.

Note: Refer to the CA4K online help file for details on configuring the Email and SMS settings screens as per below.



☑ Use Scripting

Email Settings

Email Server Name: smtp.gmail.com

Email Server Port: 587

Email From Address: napcosoft@gmail.com

Email Password: ************

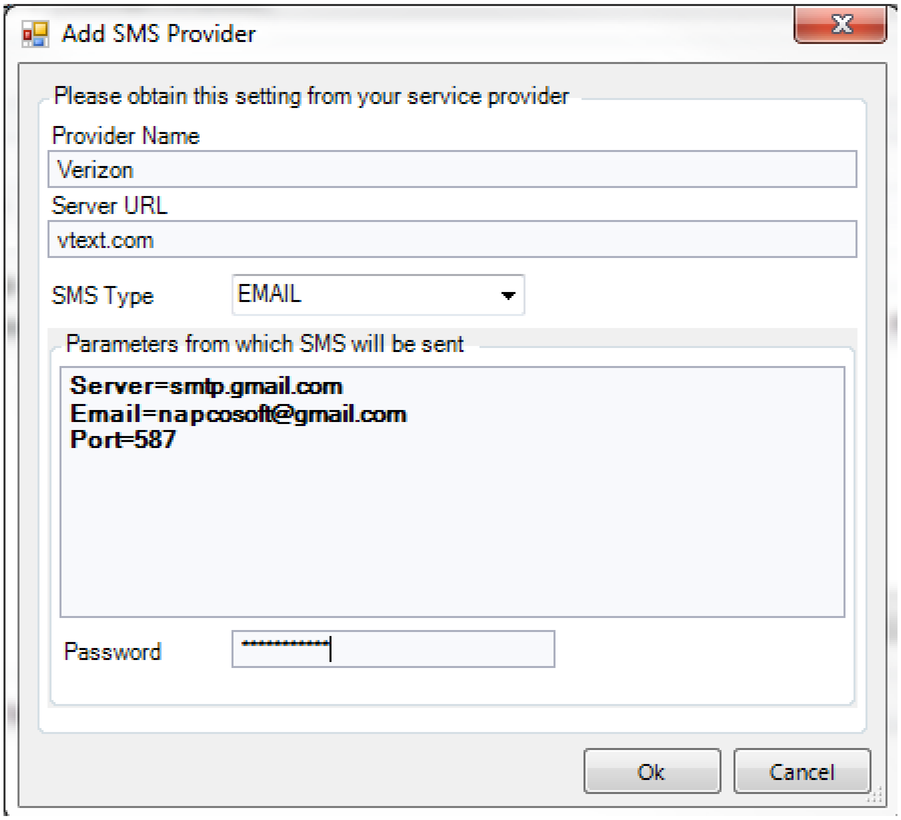
SNPP Provider Settings

Provider Name	Server URL	Port

SMS Provider Setting

Provider Name	Server URL

Last Change: 6/10/2021 12:36 PM



Please obtain this setting from your service provider

Provider Name: Verizon

Server URL: vtext.com

SMS Type: EMAIL

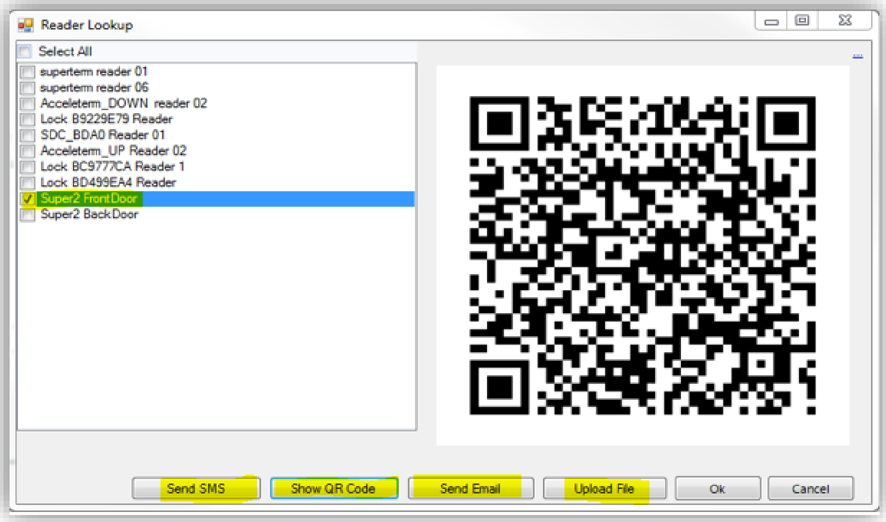
Parameters from which SMS will be sent

```
Server=smtp.gmail.com
Email=napcosoft@gmail.com
Port=587
```

Password: ************

- Once customer fields are created and messaging and scripting are configured, the user needs to enter the phone number and email address in the personal screen for a badge holder to receive mobile credentials by email or SMS.

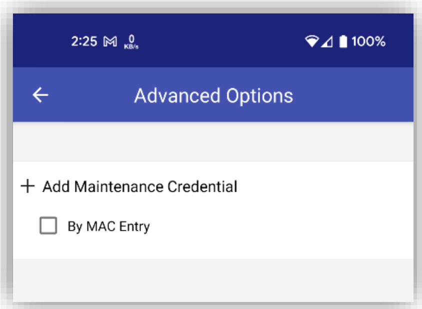
- Click the SMS or Email button in the Reader Lookup screen to receive credentials by email or SMS. Upon receiving, click the link to import doors/credentials to the mobile device.



☐ Select All

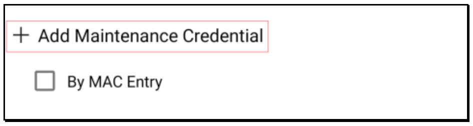
☐ superterm reader 01
☐ superterm reader 06
☐ Acceleterm_DOWN reader 02
☐ Lock B9229E79 Reader
☐ SDC_BDA0 Reader 01
☐ Acceleterm_UP Reader 02
☐ Lock BC9777CA Reader 1
☐ Lock BD499EA4 Reader
☑ Super2 FrontDoor
☐ Super2 BackDoor

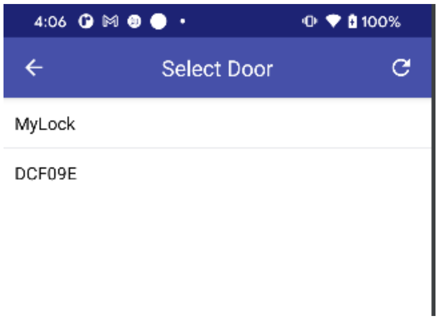
Advanced Administrative Options

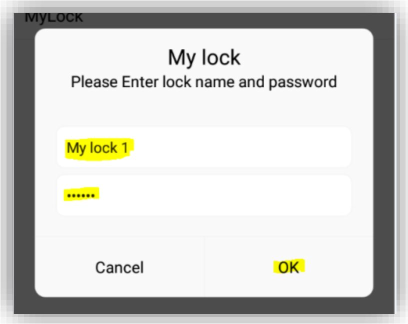


1. The administrator or installer can use some admin functions (Output operation mode select, adjusting Bluetooth advertising transmit strength, etc.) during construction or installation time.
2. To access admin functions, set the module into admin enroll mode by pressing the Module's Pushbutton once, and there will be three quick RED LED flashes with beeps followed by one GREEN LED flash and then a continuous beeping with green LED flashes.
3. While green LED flashes with continuous beeps, the user can configure the admin Door in two ways:

   a) By Clicking **Add Maintenance Credential** and selecting **MYLOCK** from the available Doors list.







My lock

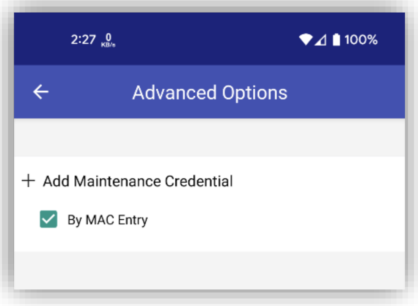
Please Enter lock name and password

My lock 1

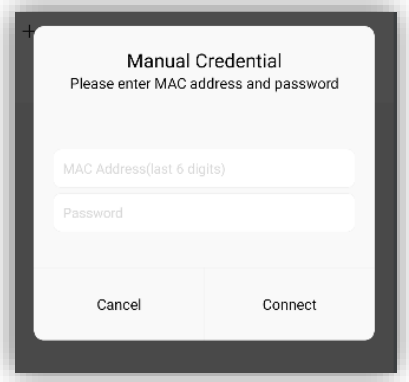
••••••

b) By **MAC Entry:**

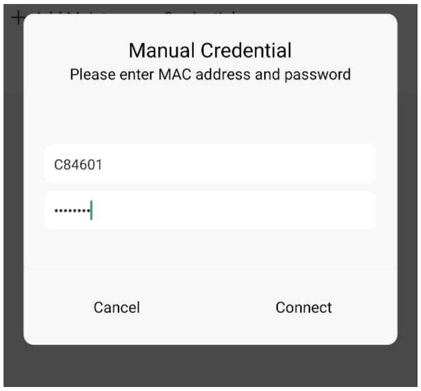
i) Check By MAC Entry and tap on + Add Maintenance Credential



ii) Enter the last Six digits of the MAC Address and the password when the Manual Credential window prompt, click Connect.


Manual Credential

Please enter MAC address and password

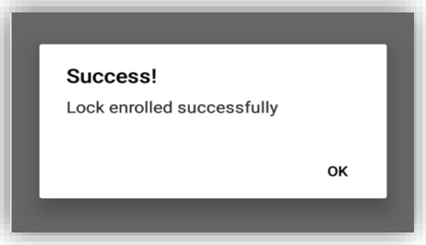

Manual Credential

Please enter MAC address and password

C84601

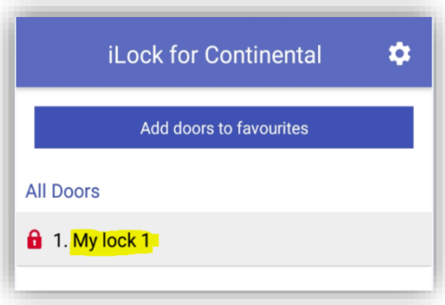
••••••••

A. **Enroll successful Message** displays when the Lock enrolled successfully**.**

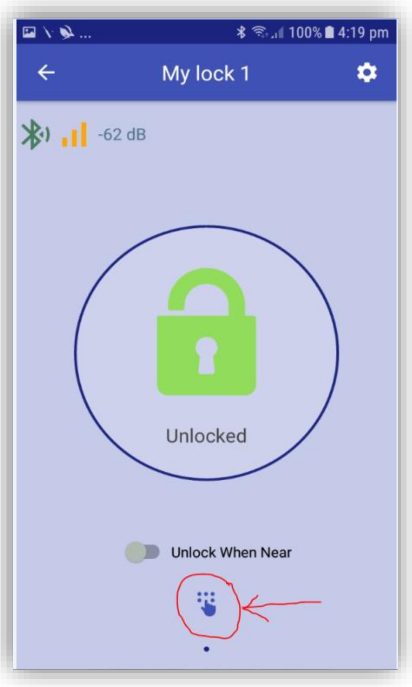

Success!

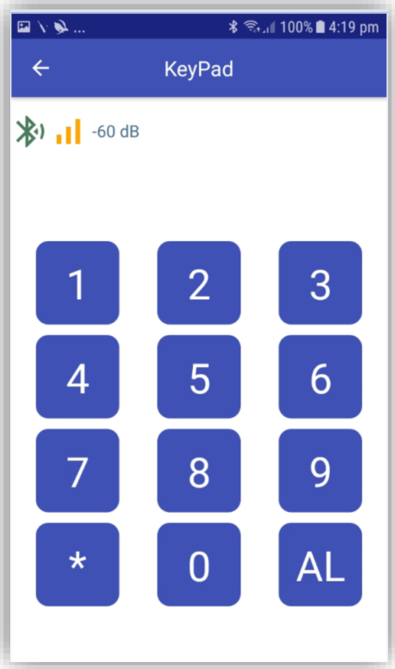
Lock enrolled successfully

B. Now the Admin mode door will be displayed under **All doors.**



C. Select the admin door and click unlock icon to connect to the door and enable admin mode. Once the connection is made, a new icon will appear for the keypad to perform various system configurations: (Output operation mode select, adjusting Bluetooth advertising transmit strength etc.).





4. Once the connection is made, a keypad will appear to perform admin functions.
5. The admin Users can perform the following functions using the keypad screen.
   a. Configure output operation modes
      Command: AL, 1, AL, Arg1, *
      Arg1 = Mode,
      0= Automatic (default), based on detected credential and serial port status.
      1= Serial Only
      2= Wiegand Only (64bit)
      3= Wiegand 160Bit Only

   b. Configure device address
      Command: AL, 2, AL, Arg1, *
      Arg1 = Address,
      5= Door 1(default)
      6= Door 2, for Networx panel second door

   c. Configure a sounder on Unlock event
      Command: AL, 5, AL, Arg1, *
      Arg1 = Sounder On/ Off,
      0 = No Sounder on Unlock Detect
      1= Sound Beep on Unlock Detect (Default)

   d. Configure Bluetooth Advertisement transmit strength
      Command: AL, 7, AL, Arg1, *
      Arg1 = indexing strength, 0 being the weakest and 7 being the strongest,
      0 = -19.1 dBm
      1 = -15.1 dBm
      2 = -10.9 dBm
      3 = -6.9 dBm
      4 = -2.5 dBm
      5 = 1.6 dBm

6 = 5.8 dBm
7 = 7.5 dBm (default)

e. Exiting Program mode
Command: AL, 8, *
(User can also exit program mode by holding down **AL** key)

f. Default and restart
Command: AL, 9, 9, AL, 0, 0, 0

Note: Defaulting can be performed in two ways

Default Method 1: Remove the power and wait for 10 seconds and power up the module and waits for three RED LED flashes with Beeps. After that, hold the Button for approximately three (3) seconds. The user will observe three GREEN LED flashes with Beeps followed by three quick RED LED flashes for two consecutive times with 1-second interval and a terminating GREEN LED flash with a beep.

Default Method 2: When the module is already powered up, press and hold the Button, and there will be periodic RED LED flashes with Beeps ended with a green led flash with beep followed by consecutive RED LED flashes for approximately 20 seconds. Release the Button once the four quick RED LED flashes with Beeps stop with a green LED flash. The module will be defaulted after three GREEN LED flashes with Beeps followed by three quick RED LED flashes for two consecutive times with a 1-second interval and a terminating GREEN LED flash with a beep.

THE END