

CA4K™ “Mobile App”

Installation Guide

Revision: Rev D

Date: 2/24/2020



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.

Copyright © 2019 by Continental Instruments LLC. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, or stored in a retrieval system, without the prior written permission of Continental Instruments LLC, 355 Bayview Avenue, Amityville, NY 11701. Telephone: 631-842-9400 • FAX: 631-842-9135

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

| | |
|--|----|
| <i>DISCLAIMER</i> | 2 |
| <i>MUST READ - VERY IMPORTANT NOTES</i> | 4 |
| <i>Overview</i> | 5 |
| <i>System Requirements</i> | 5 |
| <i>Verify Full Administrator Permissions</i> | 5 |
| <i>Related Documents</i> | 6 |
| <i>Prerequisites</i> | 6 |
| <i>Install IIS (Internet Information Services)</i> | 7 |
| <i>Install CA4K Mobile App from V1.1.x DVD</i> | 10 |
| <i>CA4K Programming requirements</i> | 13 |
| <i>Purchase and Download the CA4K Mobile App for your device</i> | 14 |
| <i>Install CA4K Mobile App on the IOS or Android device</i> | 15 |
| <i>Launch CA4K Mobile App</i> | 15 |
| <i>Configure CA4K Mobile App</i> | 18 |

MUST READ - VERY IMPORTANT NOTES

1. Prior to installing IIS and the CA4K™ Mobile App, you must make certain you have **Full Administrator** privileges without any restrictions. This includes lowering the UAC settings to "Never Notify" and verifying there are no domain restrictions.
2. The CA4K Mobile App is supported on CA4K V1.1.x and later.
3. Internet Information Systems (IIS) is a Windows feature and is a Web Server that is used to run Web Applications. IIS is installed from Windows.
4. Prior to installing the CA4K Mobile App from the CA4K DVD, it is required to have Internet Information Systems (IIS) pre-installed. The default port installed for the CA4K Mobile App is 8080. This can be changed in the IIS settings.
5. The CA4K Mobile App is supported on an Android and IOS mobile device. It is required to have an internet connection to purchase and download the CA4K™ Mobile application. The CA4K™ Mobile App must be purchased and downloaded from the Apple App Store or Google Play Stores.
6. The CA4K software must have specific programming regarding Operators, Operator Privileges, Badges (Personnel) and Access Groups for the CA4K Mobile App to function properly.
7. In the CA4K, every user of the Mobile App must have an Operator created for them under Administration>Operators and also an associated badge configured for them in Personnel.
8. When creating the Operators as per note 7, you should use the Administrator Privilege Role for administrators and create a new basic Privilege role for Mobile App users.
9. If the same Operator is logged into two phones, you must still configure the settings on both phones. The settings are local to the device. This includes the settings under MY DOORS.
10. Upon launching the CA4K Mobile App the first time, you will be prompted to enter one or more names and URL's to connect to. If you wish to return to the URL screen while in the App, you must **SHAKE** the mobile device.

Overview

This document provides a step by step procedure for installing the CA4K™ Mobile App. Prior to starting the installation, you must verify the computer meets the recommended computer specifications and you have full Administrator rights. In addition to the computer specifications and permissions, you must also have the CA4K™ Version 1.1.x DVD and a V1.1.x software license.

Very Important: You must create a CA4K Operator for each user of the CA4K Mobile App. In addition to the Operator, you must create a badge in personnel for each Operator you create. For each badge, the first and last name must be identical to the first and last name of the Operator. This will be discussed in detail later in the document.

System Requirements

Ensure Recommended Server Requirements are met. Verify that the computer meets the specifications that are documented in the "CA4K™ System Requirements" document.

Verify Full Administrator Permissions

The installation of CA4K™ requires Full Administrator permissions. Failure to provide these permissions will result in installation failures.

Related Documents

CA4K™ Complete Server Installation Guide - A step by step guide on installing a "Complete Server" installation.

CA4K™ Database Only Installation Guide - A step by step guide on installing a "Database Server" installation.

CA4K™ Hardware Communication Server (HCS) Installation Guide - A step by step guide on installing an HCS Installation.

CA4K™ Report Station Installation Guide - A step by step guide on installing a "Report Station" installation.

CA4K™ Server Only Installation Guide - A step by step guide on installing a "Server Only" installation.

CA4K™ Workstation Installation Guide - A step by step guide on installing a "Workstation" installation.

CA4K™ Data Migration Guide - A step by step guide on migrating a CardAccess 3000 database to a CA4K™ database.

CA4K™ Quick Start Programming Guide - A step by step guide on programming a basic CA4K™ system.

CA4K™ TCP/IP Ports Reference Guide – TCP/IP Ports document.

CA4K™ System Requirements – V1.1.x Computer Specifications.

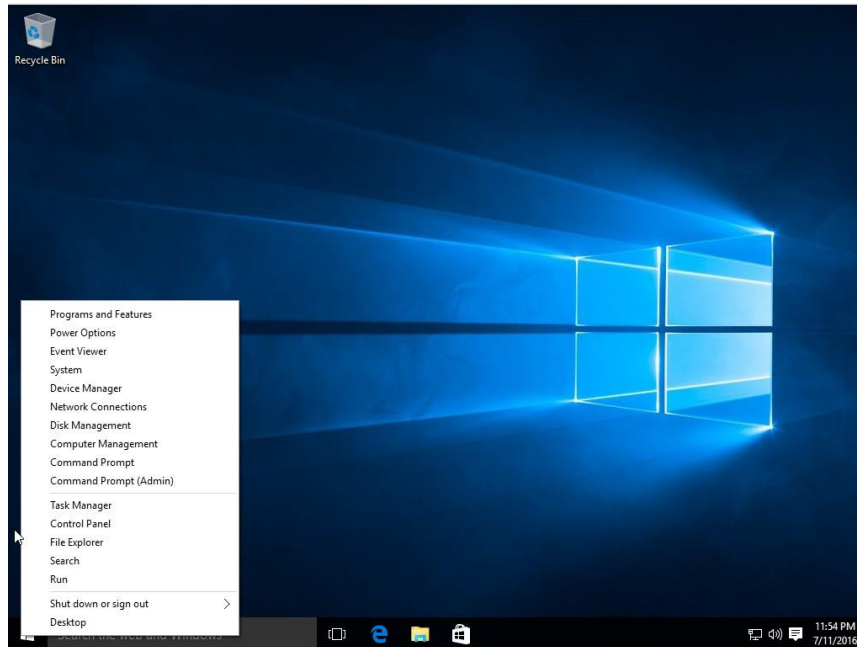
Prerequisites

- A functional CA4K™ Version 1.1.x Complete Server
- A functional IIS installation.
- An Android or IOS device

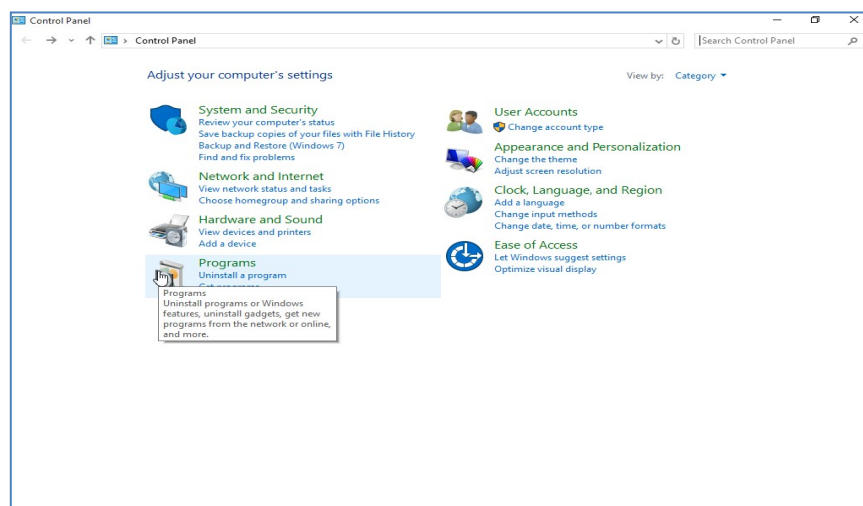
Install IIS (Internet Information Services)

Note: Installing IIS must be performed prior to installing the CA4K Mobile App from the V1.1.x DVD. The following screens may vary between different operating systems.

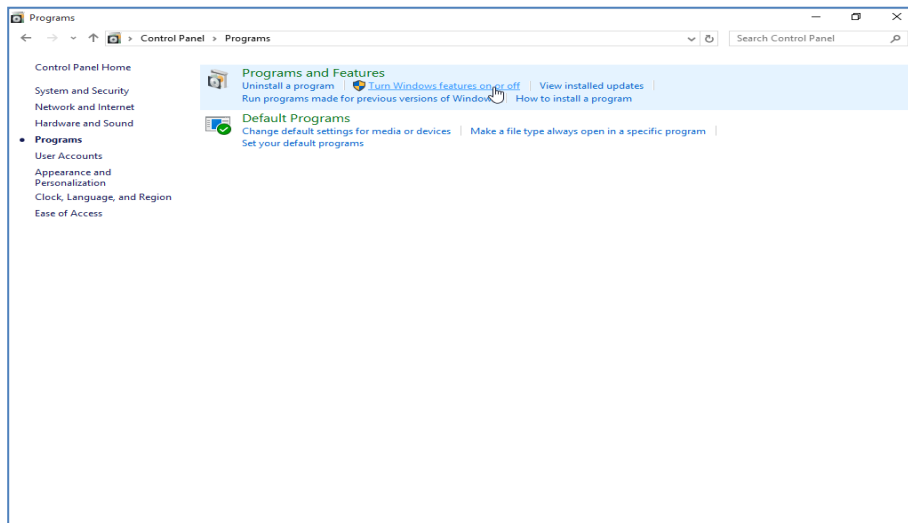
1. Open **Control Panel** from the Start Menu.



2. In the Control Panel, click Programs.

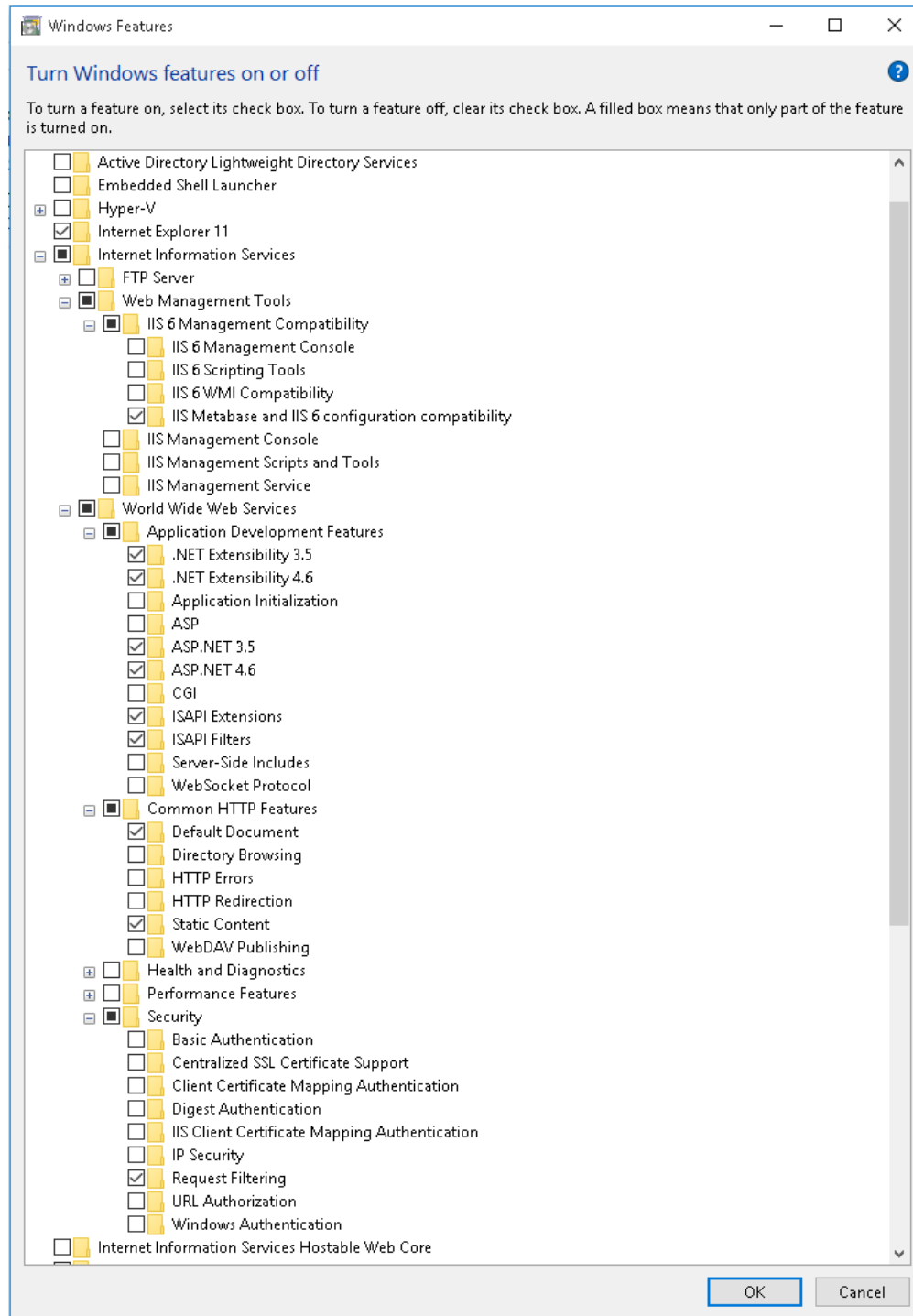


3. In the Programs and Features section, select Turn Windows features on or off link.

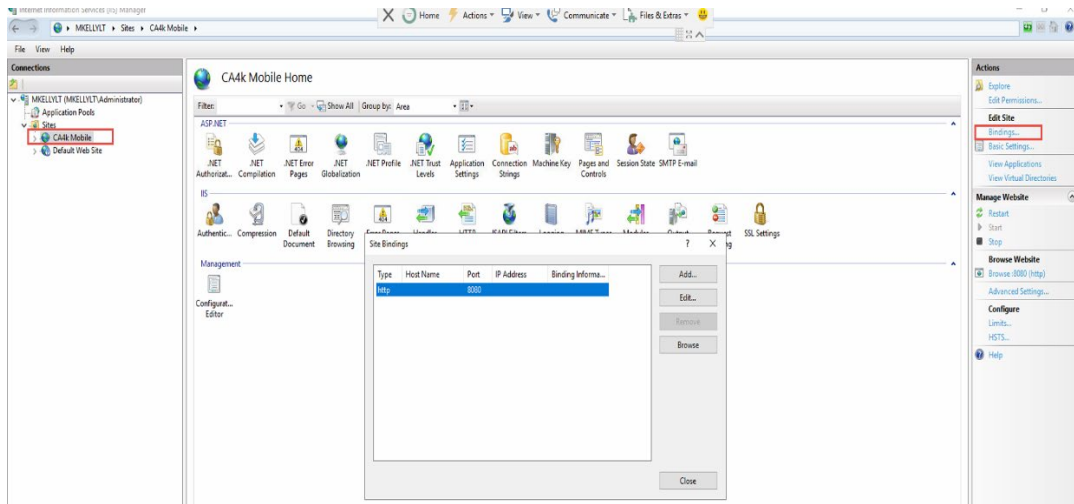


- Now, click on the features that are checked on the screen below and then click the **OK** button. The IIS settings for the CA4K Mobile App are very similar to the settings for the CA4K Web Client.

Note: It is recommended to install the **IIS Management Console under Web Management Tools**

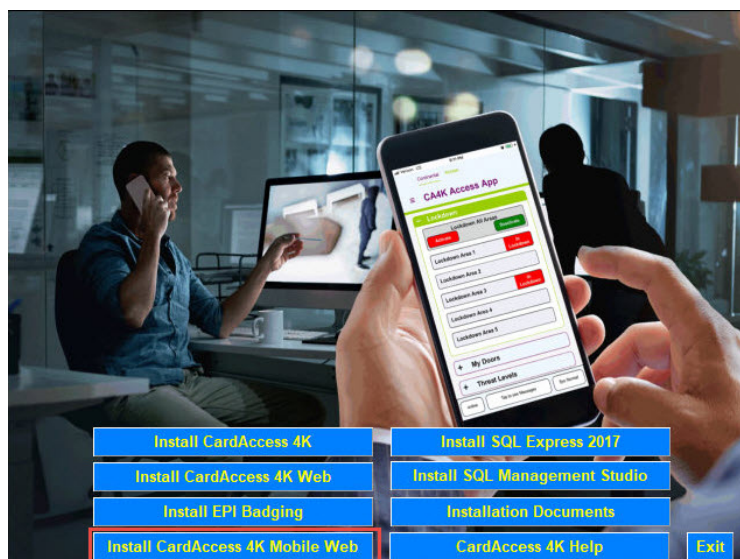


5. Changing Port Information in IIS (Optional) - By default, App website will be installed on port 8080. This port can be changed as needed. Open IIS->Click CA4K Mobile web site ->Bindings to edit port.

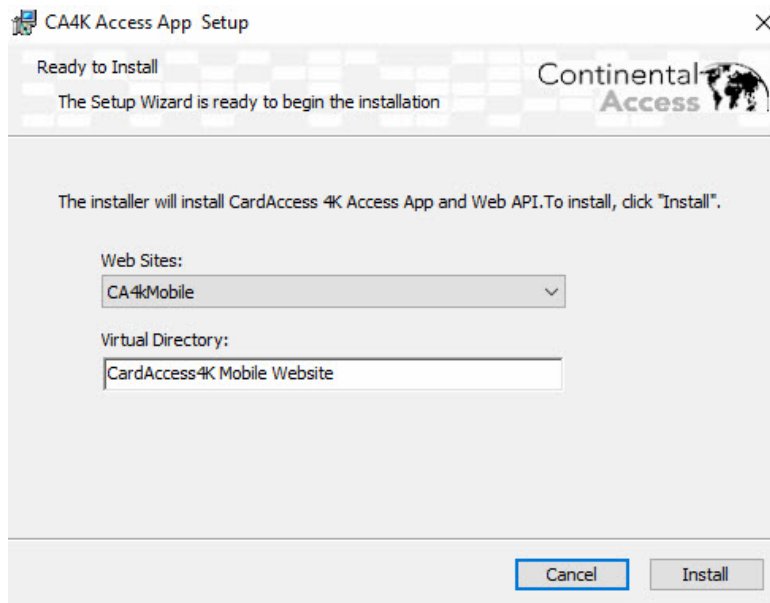


Install CA4K Mobile App from V1.1.x DVD

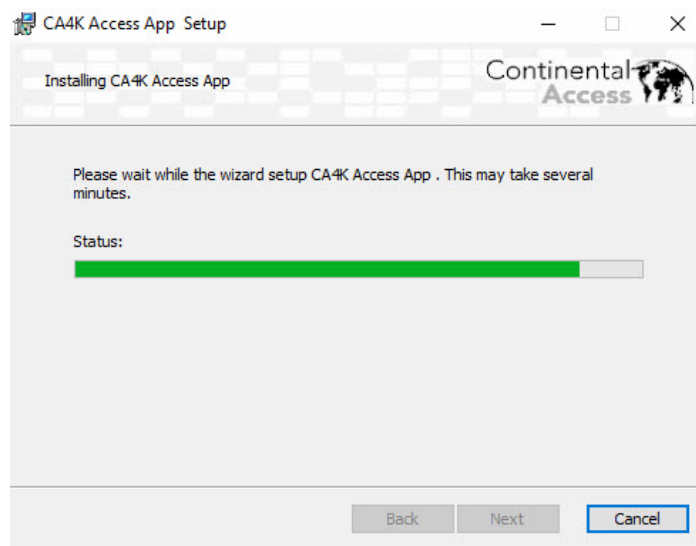
1. Open **Launch.exe** (Run as administrator) from installer, and click **Install CardAccess 4K Mobile Web** option.



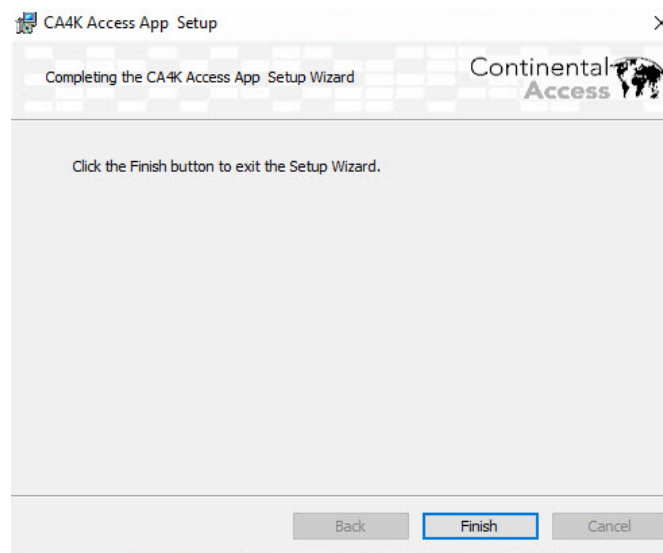
2. At the **CA4K Access App Setup** screen, select the Web Site name and the virtual directory. It is recommended to leave these settings at the default settings. Click **Install** button.



3. Upon clicking **Install**, a progress bar will display while installing the CA4K Web Access App.



4. After the installation completes, click **Finish** to finish the CA4K Mobile App Installation process.



CA4K Programming requirements

Very Important– As per the following steps, every user of the CA4K Mobile App must be configured as a CA4K Operator and also must have a badge assigned in Personnel that corresponds to the Operator.

1. In the CA4K software, you must configure an **Operator** for each Mobile App user. This is done under Administrator>Operators. Next, for each Operator, you must assign a **Privilege Role** to the Operator. It is recommended to use the Administrator Privilege Role for Administrators and create a new Privilege Role with basic permissions for all basic Mobile App users.
2. Next, in the CA4K software, you must assign a **Badge** in **Personnel** for each Mobile App user. There must be a corresponding badge created for each Operator created. In Personnel, the Badgeholders first and last name must match exactly, the first and last name of the Operator. The first and last name of the Operator is under the Operators Personal tab.
3. Next, in Personnel, you must assign one or more access groups to each badge. The Access Groups assigned to the badge will determine what doors the Mobile App user will see under MY DOORS on the configuration screen and main menu.

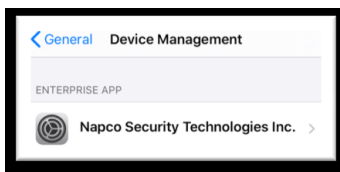
Purchase and Download the CA4K Mobile App for your device

1. The next step is to Purchase and download the CA4K Mobile App that is compatible with your mobile device from the Apple App Store or Google Play store. While in the App stores, search for Napco or CA4K.



VERY IMPORTANT: Upon downloading the App and installing it on an IOS device, you might be required to VERIFY the App under Settings>General>Device Management. Refer to the following screenshots. If you are using an Android device, you can skip this process.

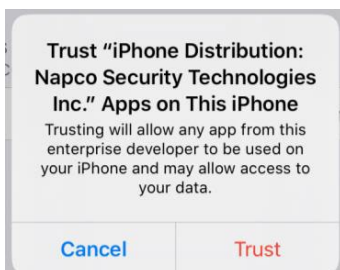
2. In Device Management, click Napco Security Technologies Inc.



3. Click Trust Napco Security Technologies Inc.

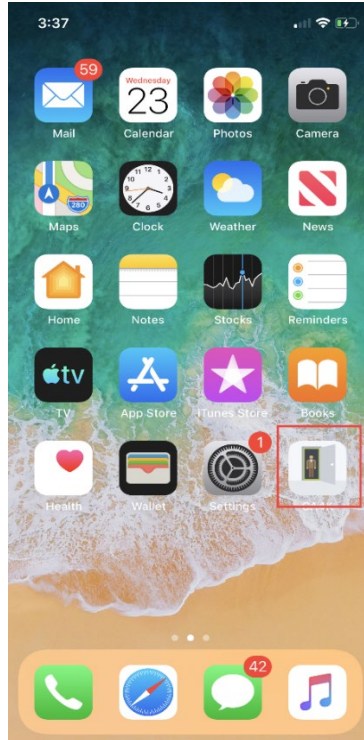


4. Click **Trust**.



Install CA4K Mobile App on the IOS or Android device

1. Install the CA4K Mobile App on the IOS or Android mobile device.
2. Upon installing the CA4K Mobile App, a CA4K Icon will display on the mobile device.



Launch CA4K Mobile App

1. Launch the CA4K Mobile App by clicking the CA4K icon.

The first time you launch the App, you will be prompted for one or more Names and URL's to connect to. Upon entering one or more Names and URL, you must click Save.

Note: Below is an example of two URL's entered with the first one enabled. Please verify you type in the port 8080 as per the following example. The port number can be changed in IIS as mentioned above.

<http://192.168.1.111:8080/CA4KMobile/>

Very Important: The version of the CA4K Mobile App will display on the bottom of the Name/URL screen along with a Save button. In the screenshot below, the phone App is V1.0.6.

3:52 ⋮ 📶 🔋

☒ Office

☐ Mk

☐ Enter Name

☐ Enter Name

+ v.1.0.6 Save

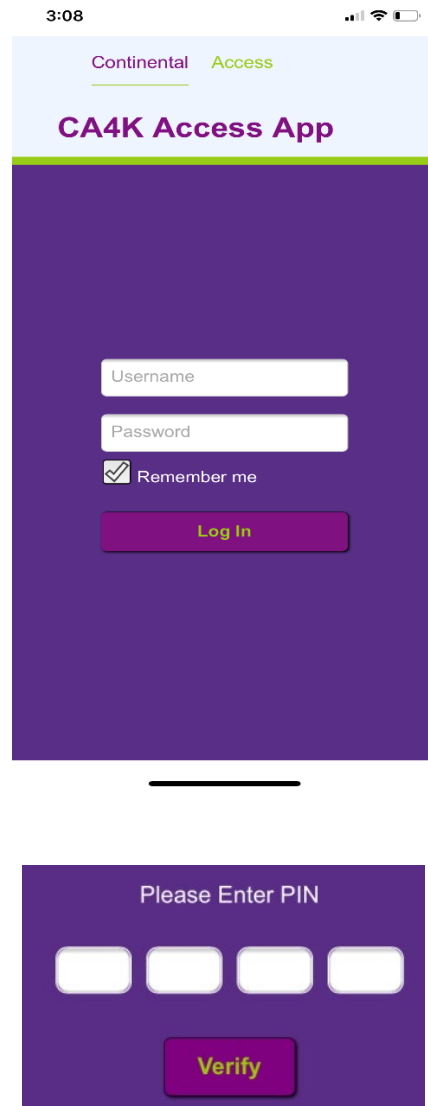
2. If you wish to return to the URL screen while in the App, you must SHAKE the mobile device to the left and right. Upon shaking the device, the following dialog box will display. Click Yes if you wish to reopen the URL screen.

Info!

Are you sure, you want to open the url settings

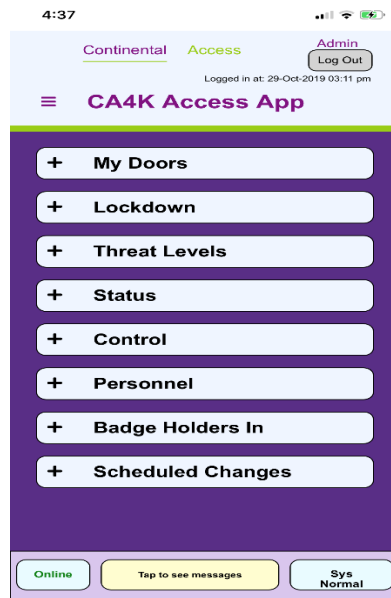
Yes No

3. Upon launching, a CA4K Mobile App login screen will display. Login with your CA4K credentials. Login with the operator you created for the Mobile user. Type in the Operator Username and Password. If you selected to use an App Pin Entry in the configuration settings, you must also enter the Pin number.



The image shows two screenshots of the CA4K Access App. The top screenshot is the login screen, which has a light blue header with 'Continental' and 'Access' in green. Below the header is a purple bar with 'CA4K Access App' in white. The main area is purple and contains a white login form with fields for 'Username' and 'Password', a 'Remember me' checkbox, and a 'Log In' button. The bottom screenshot is the PIN entry screen, which is purple and contains the text 'Please Enter PIN' above four white input boxes and a 'Verify' button.

4. Upon a successful login, the CA4K Access App main menu will display.



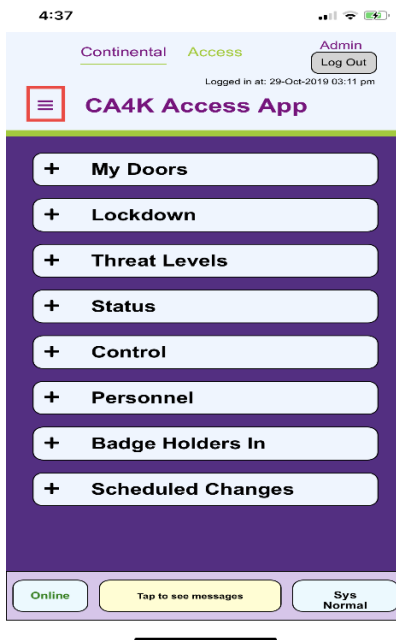
App Messages / Status:

- First section shows connection status with the server Online/Offline.
- Middle Section shows the general messages.
- And the last section shows activate status for Lockdown and Threat Level.

Configure CA4K Mobile App

MORE button (Configuration Settings)

1. At the main menu of the CA4K Mobile App, click the MORE button (3 horizontal bars) for the App configuration settings. These settings are unique to the mobile device and must be configured on each mobile device being used.



APP VERSION – This is the version of the Web App on the IIS Web Server.

BASE URL - The Base URL displays the URL of the IIS Web Server, Port number and web application folder name.

GENERAL SETTINGS - The General Settings contain:

Login Session Timeout: This setting determines how long the app will stay logged in after user's last interaction with the App. Time can be set to 5 min to 60 min.



App PIN Entry: When this is check box is selected, the user is required to enter a valid 4-digit Pin Code. Upon entering the 4-digit pin code, you must click Done. Upon doing so, you will be required to enter the pin code during the App log in process.

BADGE HOLDERS LINK - The Badge Holder's Link displays the badge number, Facility, First Name and Last Name associated with the Operator who is logged into the CA4K App. If there is not a badge configured for the Operator in CA4K, this box will be blank and you will not have access to any doors.

The screenshot shows the CA4K App Config screen. At the top, there's a status bar with the time 3:45 and signal indicators. Below that, a header bar contains 'Continental', 'Access', and 'Admin' with a 'Log Out' button. The main title is 'CA4K App Config' with a subtitle 'Logged in 13-Jan 04:12 PM'. Below the title are 'Save' and 'Cancel' buttons. The settings are organized into sections: 'App Version' (1.0.12 (137)), 'Base URL' (http://192.168.1.120:8080/ca4kmobile/), 'General' (Login Session Timeout: 10 mins, App PIN Entry: [checkbox]), and 'View Selections'. The 'View Selections' section contains a 'Badge Holder's Link' box with fields for 'Badge' (2000), 'Facility' (0), 'First Name' (admin), and 'Last Name' (admin). At the bottom, there are three buttons: 'Online' (green), 'Tap to see messages' (yellow), and 'TL/LD Active' (red).

VIEW SELECTIONS – By default, the main menu items will be selected by default. If you wish not to display a main menu item, you must un-select it. Under MY DOORS, all the doors you have permissions to will display. These are NOT checked by default. You MUST select the doors you wish to display and Unlock.

4:38

● View Selections

Badge Holder's Link

Badge 2000

Facility 0

First Name admin

Last Name admin

- My Doors ☒

- Science Building Rdr 1 ☒

- Science Building Rdr 2 ☒

- Science Building Rdr 3 ☒

- Science Building Rdr 4 ☒

- Math Building Rdr 1 ☒

- Math Building Rdr 2 ☒

- Math Building Rdr 3 ☒

- Math Building Rdr 4 ☒

- Lockdown ☒

- Threat Levels ☒

Online Tap to see messages Sys Normal

View Options

My Doors Expanded: When selected, MY DOORS will be expanded by default on the main screen of the App.

Request Wireless Lock Status: This allow app to request status for wireless locks when perform My Door, Manual Control operation and Status screen. There is no way app will request Wireless Locks status automatically with a time interval because of battery. In order to get actual status for any wireless locks this option must be checked. However, it is recommended to use this feature only if required for longer battery life.

In-List Refresh: The interval the Badge Holder's In data will refresh. The time interval is in Seconds.

Message Options

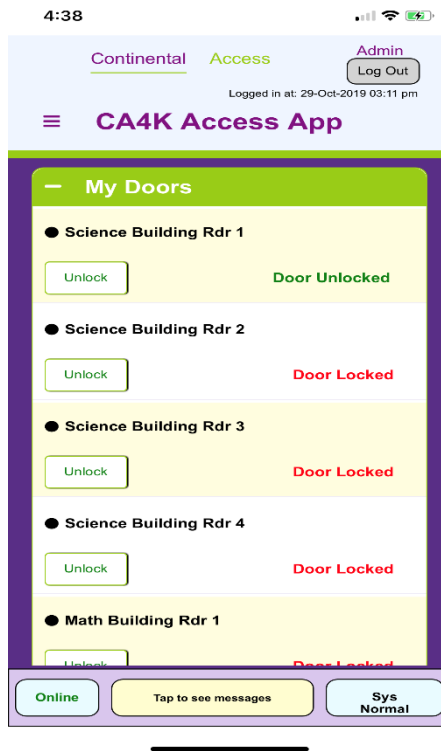
Display Message Time - This setting determines how and when general messages will be cleared from the message section of the status bar. The time interval is in Seconds.

MY DOORS - Upon selecting MY Doors on the main menu, the MY DOORS screen will display the Readers that the Mobile App Operator has permissions to in CA4K. In the CA4K, the permissions are determined by the Operators Privilege and the Access Groups assigned to the corresponding Badge number. Under MY DOORS, you will have the option to Unlock the doors you have permissions to. Click Unlock on a door. The status will change from **Door Locked** to **Door being Unlocked**, then **Door Unlocked** and then back to **Door Locked**.

NOTE: If badge is disabled from CA4K which is currently linked to Badge Holder's Link Badge, in the next iteration of auto refresh data (within 1 / 2 second depending on network latency) the Badge from Badge Holder's Link will be removed. If the logged in user has multiple badges, then the first available badge will be selected and My Door list will refresh accordingly. It is important to know that if any mutual door is found which was checked for the previous badge, will show as checked.

Functional notes:

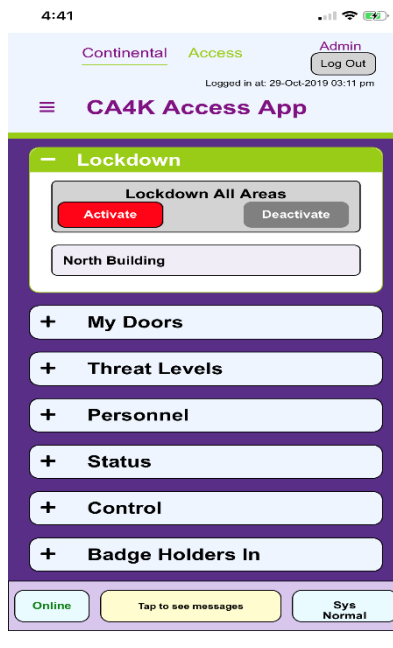
- To unlock a door, tap Unlock and the status will display, Door Being Unlocked.
- PIN or Common code may need to be entered depending on reader and badge configuration. A small window will appear to get the PIN or Code.
- Door status displays on right side depending on current state. If door is disabled or status is not found then displays UNKNOWN.
- Door Locked will display for the following Door Status: "Door is Secure", "Manual Locked" and "Door Secure".
- Door Unlocked will display for the following Door Status: "Forced Door", "Free Access", "Manual Unlocked", "Bypass Active", "DOOR is Open", "Free Access Open", "Disabled and Open" and "Door Unlocked", any other status will display unknown.
- Unlocking the door allows access to the door and generates a Valid Badge Type event and unlock door event. If this fails, then a Violate Type event is generated.
- If any operations fail, the messages will display in the general message section. This will hold up to the last 5 messages and can be seen by tapping and hold on the section for 5 seconds.



LOCKDOWN – Upon selecting LOCKDOWN from the main menu, the LOCKDOWN screen will display the status of Lockdowns. You will also have the option to Activate and Deactivate a Lockdown.

Functional notes:

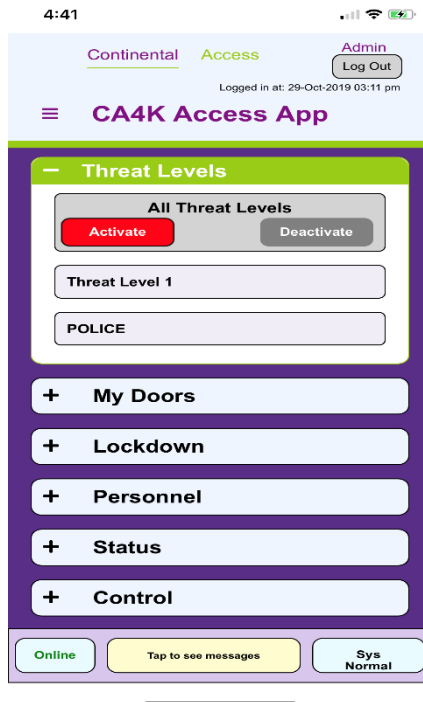
- All lockdown areas are displayed here for logged in operator considering partition.
- A Tap on a Lockdown Description, the user can Activate or Deactivate a single Lockdown Area.
 - A tap on a **Activate** button, the user can activate all lockdown areas which are listed at a time
- A Tap on **Deactivate** button, the user can deactivate all lockdown areas which are listed.



THREAT LEVELS - Upon selecting THREAT LEVELS from the main menu, the THREAT LEVELS screen will display the status of Threat Levels. You will also have the option to Activate and Deactivate a Threat Level.

Functional notes:

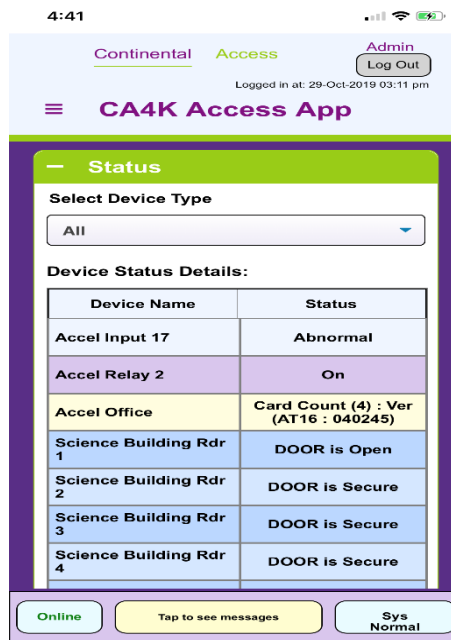
- All Threat Levels are displayed here for logged in operator considering partition.
- A tap on a Threat Level Description, the user can Activate or Deactivate a single Threat Level.
- A tap on **Activate** button, the user can activate all Threat Levels which are listed at a time.
- A Tap on **Deactivate** button, the user can deactivate all Threat Levels which are listed at the time.



STATUS - Upon selecting STATUS on the main menu, the Status screen will display. You will also have the option to select a device type and view the status of it. This function displays device status for device type **Panel, Door, Relay** and **Input**. A common type is defined as **All** which allow to see all those device statuses together without filtering. This is selected by default. User need to filter by type himself.

Functional notes:

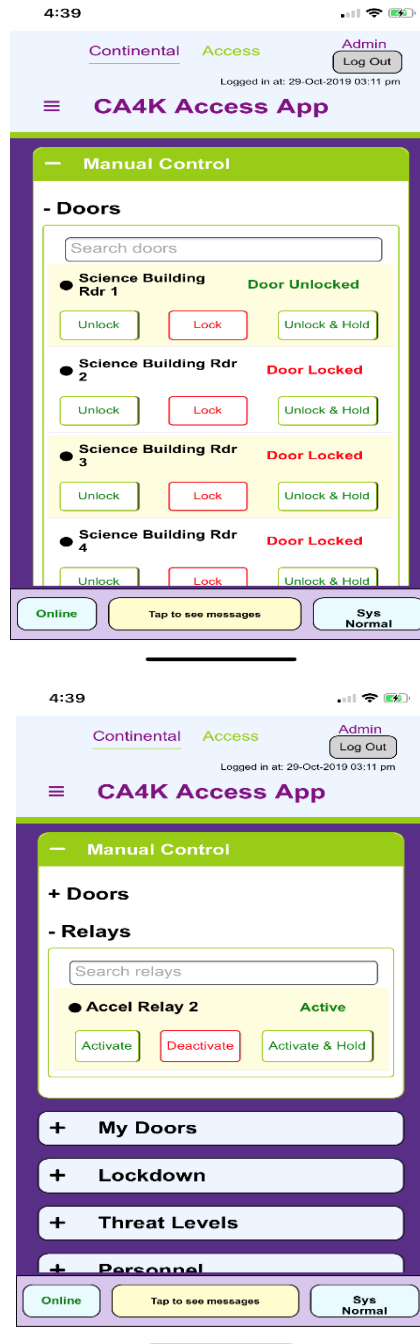
- **Panel Status:** Displays Panel/Lock description and its current status. The Panel status will show **Card Count** and **Firmware Version** if it is responding. If not, this will display **Not Responding**. For wireless lock it will not display Card Count as Wireless Lock does not support it.
- **Door Status:** This displays door's name and current status for example **Forced Door, Door is Secure, Not Configured** etc.
- **Relay Status:** Displays relay name and its current status for example **Off, On, Not Configured** etc.
- **Input Status:** Displays relay name and its current status for example **Normal, Abnormal, Not Configured** etc.



CONTROL – Upon selecting CONTROL on the main menu, the Manual Control screen will display for Doors and Relays. Under Doors, you will have the option to Unlock, Lock and Unlock & Hold the Doors you have permissions to control. Under Relays, you will have the option to Activate, Deactivate and Deactivate and Hold the Relays you have permissions to control.

Functional notes:

- The manual control of Doors and Relays work identical as manual control in the CA4K. After expanding each item, a search option will display in order to search any desired devices for door and relay.
- **Doors:** Expanding doors, all doors should display based on the operator partition. This allow user to manual control doors to Unlock, Lock and Unlock & Hold. Door current status is reflected depend on operation performed. Default strike time 5 second or which is set in reader screen will be followed as there is no way to override the strike time. If any door is disabled or status not found will be displayed as UNKNOWN on status. This will generate event followed by CardAccess4k. For Unlock and Unlock & Hold will generate Door Manual Unlocked; for Lock, Door Manual Lock event will generate.
- **Relays:** Expanding relays, all relays should display based on the operator partition. This allow user to manual control relays to Activate, Deactivate and Activate & Hold. Relays current status is reflected depend on operation performed. If any relay is disabled or status not found will be displayed as UNKNOWN on status. This will generate event followed by CardAccess4k. For Activate and Activate & Hold will generate Output On alert; for Deactivate, Output Off event will generate.



PERSONNEL - Upon selecting PERSONNEL on the main menu, the Personnel screen will display the badges in your partition. You will also have the option to Add, Edit and Delete badges. The **Personnel** screen is used for creating badge holder records. Using this screen, it is possible to create a badge with a badge number and name including facility, set access groups, and PIN digits field to the badge. **CA4K App** also allows multiple badges create to add to assigned to a user (Person) like **CA4K**.

Functional notes:

- Only one Badge can be modified at a time. If a new badge is being added or modified that must be Saved or Canceled in order to move to another badge.
- Badge which is currently being used in Badge Holder's Link for My Door cannot be Deleted or Edit any value for that particular badge. However, user can still modify or delete any other badge which belongs to the same person.

- **Search:**

To search person/badge, tap on **Fields** from the combo and select items from the list **First Name**, **Last Name** or **Badge**, enter value on **Value** field to search person.

This allows the user to find out the specific person/badge quickly from a bunch of badges by selecting three fields like **First Name**, **Last Name** and **Badge** and entering person/badge's value considering **Field** selection.

- **Add Personnel:**

New personnel can be created by tapping on Add button. This will redirect to the add personnel screen where user can enter **First** and **Last** name, **PIN** code, set **Enabled** state, assign **Access Groups**. Number of Access Groups a badge can have depended on CA4K system settings.

In order to add Badge and Facility user need to tap **Add Badge+** button and enter values.

Once all required inputs are entered, the user can save the change by tapping on **Save** button to create or discard the changes by tapping on **Cancel** button on the top.

Access Groups:

CA4K allows a maximum of 16 access groups and displays as system settings configuration for per badge. **CA4K App** also have the same feature for access group per badge.

- Each **Access Group** combo load with all available access groups considering partition.
- Each combo starts with **NO ACCESS** on top.
- Assign or Un-assign an Access Group can be done by selecting a configured Access Group or selecting **No Access**.
- Duplicate access group for the same badge must not allow.

- Remove access group for the badge which is currently using for My Door operation will get reflected.
- Tap on any access group combo and select any one from the list to set access for person/badge. See two diagrams below.

Edit or Add Another badge to an existing Person:

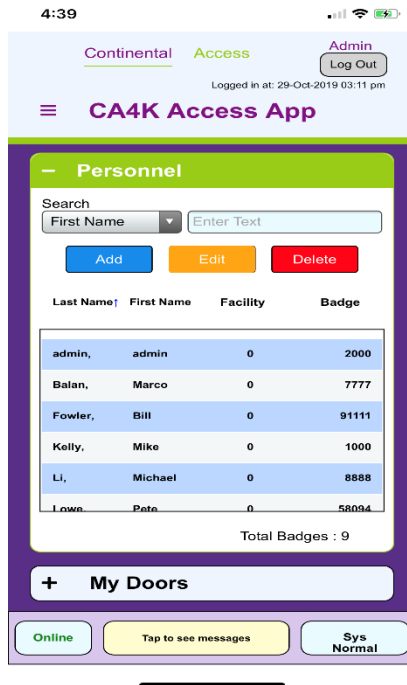
In order to edit an existing badge, the user needs to select the desired badge and tap on Edit button from the top.

- To edit the existing badge, users can simply change the values of it and tap on save. Note: badge and Facility cannot be changed from this App.
- To Add a new badge to an existing person, the user needs to tap on **Add Badge+** and enter **Badge No** and **Facility**. After adding badge, the newly created badge will be listed under the badge list and selected by default. Access Group and other values can be set at this point for this.
- Upon completion, save the changes.

Delete:

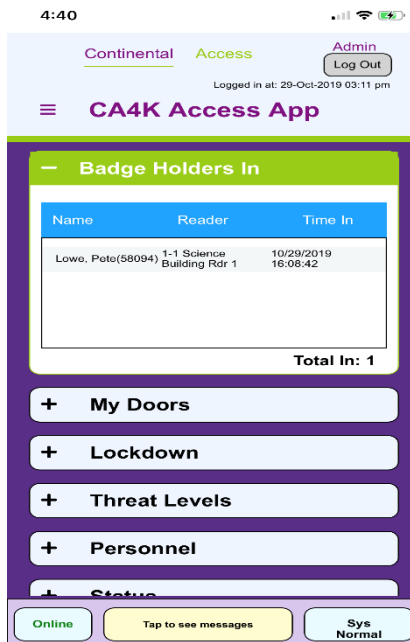
On **Delete**, the user needs to select any person/badge from grid and tap on it. **Delete** throws a pop-up to confirm about the deletion and delete the person/badge tap on **OK** as below diagram.

- Deleting a person/badge which currently assigned for logged in operator then reflect to **Badge Holder's Link** combo and **My Doors** section on **CA4K App Config** also on **My Doors** on app main screen.



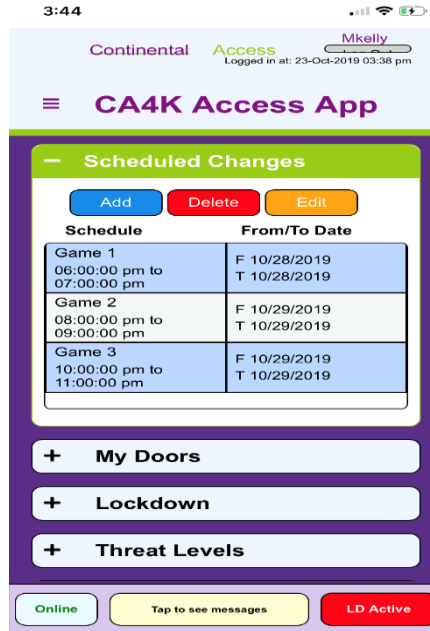
BADGEHOLDERS-IN - The purpose of the Badge Holders In function is to display a list, commonly called a 'muster list', of all badge holders that have entered a building. In the CA4K App, the user can only view entry badge holders displaying Name, Reader and Time with total count.

- The InList grid shows the entry badge holders list.



SCHEDULED CHANGES - Upon selecting SCHEDULED CHANGES on the main menu, the SCHEDULED CHANGES screen will display all the configured scheduled changes with their dates and times. The **Scheduled Changes** screen is a utility screen where you can create schedules that can temporarily override 'standard' schedules that were created using the 'Schedules' screen. Schedule changes on **App** also have same hardware items to apply changes to such as **Readers, Inputs, Relays** and **Links**.

The Scheduled Changes function allows the ability to **Add, Edit** and **Delete scheduled changes**. The **Cancel Active** feature provides the ability to cancel an active scheduled change.



The End.