

# CV-603 MProxBLE Controller / CV-603PS-K1 MProxBLE Controller Cabinet Kit

## INSTALLATION INSTRUCTIONS



CV-603-BLE



CV-603PS-K1

### 1. DESCRIPTION

The CV-603PS-K1 is a cabinet designed to mount all the central components for the MProxBLE controller including an optional 4AH battery for back-up. The CV-603 MProxBLE is a stand alone controller housed in a plastic enclosure that can be DIN mounted. To configure the controller, the CV-603 application is available on the Appstore for iPhone® users and on the Google Play for Android® users.

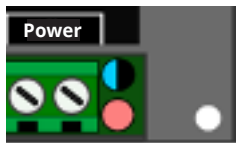
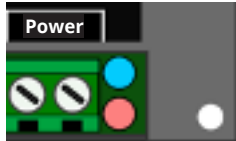
### 2. SPECIFICATIONS



<b>Power supply</b>	12VDC
<b>Average consumption</b>	< 100 mA
<b>Receiver Frequency</b>	433Mhz
<b>Number of users</b>	2000
<b>Number of events</b>	3000
<b>Number of reader inputs</b>	2
<b>Types of reader input</b>	Wiegand 26, 30, 34, 37 bit
<b>Number of relay outputs</b>	2
<b>Types of relay outputs</b>	Timed 1-180 seconds Momentary, bi-stable/latch
<b>Contact rating</b>	1A @ 12V
<b>Operating Temperature</b>	-4°F to 131°F (-20°C to +55°C)
<b>DIN rail mount</b>	Yes
<b>IP ratings</b>	IP 20
<b>Weight</b>	7 oz. (200 g)
<b>Size of controller housing.</b> (For metal cabinet, refer to last page.)	4-1/2" H x 3-1/2" W x 1-3/4" D (115mm x 90mm x 44mm)

### 3. PROGRAMMING

The MProxBLE application is available on iPhone® (Appstore) and Android® (Google Play).

### 4. VISUAL INDICATOR LED ON MPROXBLE CONTROLLER

	STATE	LED 1: BLUE
Smartphone connection	Waiting for smartphone connection	 1 Flash every 5s
	Smartphone connected	 ON

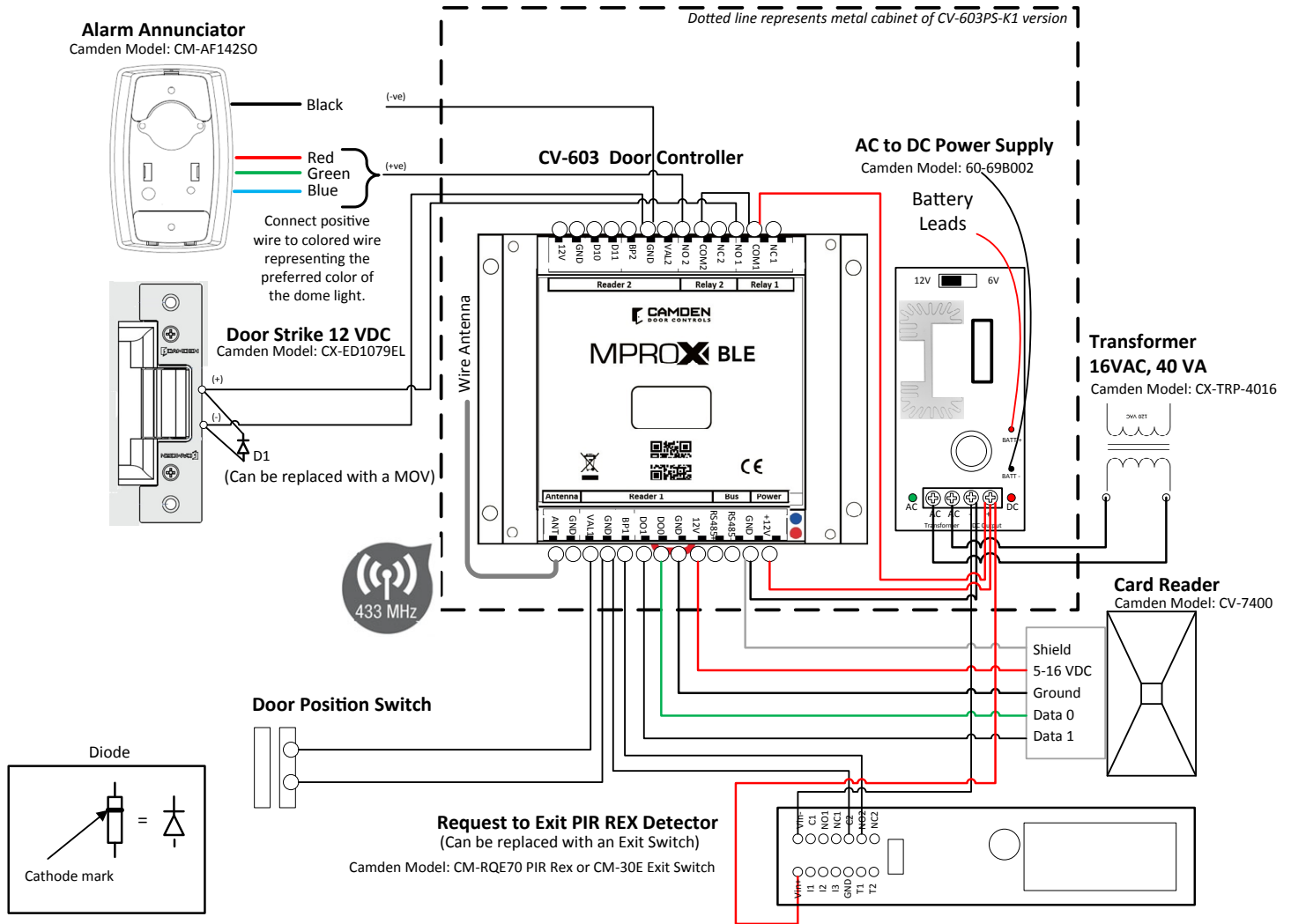
	STATE	LED 2: RED
ID reading	Denied ID	 2 Flashes
	Authorized ID	 On 1s

**CV-603 MPROXBLE CONTROLLER / CV-603PS-K1 MPROXBLE CONTROLLER CABINET KIT**

INSTALLATION INSTRUCTIONS

**5. WIRING**

**SINGLE DOOR With ALARM ANNUNCIATOR**



**CV-603 MPROXBLE CONTROLLER / CV-603PS-K1 MPROXBLE CONTROLLER CABINET KIT****INSTALLATION INSTRUCTIONS****Bill of material:**

Item	Description	Quantity	Camden Model#	
			CV-603PS-K1	CV-603
1	Controller	1	CV-603 provided in kit	CV-603
2	DC Power Supply	1	60-69B002 - provided in kit	PS-13
3	Transformer	1	CX-TRP-4016 provided in kit	CX-TRP-4016
4	Alarm Annunciator	1	CM-AF142SO	CM-AF142SO
5	Door Strike, 12 VDC	1	CX-ED1079	CX-ED1079
6	Door Position Switch, a door latch monitor switch can be used, add suffix "L" to CX-ED1079	1	CX-MDA surface or CX-MDH recessed.	CX-MDA surface or CX-MDH recessed.
7	Proximity Card Reader, 125 KHz. Not required if transmitters are used.	1	CV-7400	CV-7400
8	Request to Exit Device	1	CM-RQE70 PIR sensor or CM-30E Push button.	CM-RQE70 PIR sensor or CM-30E Push button.

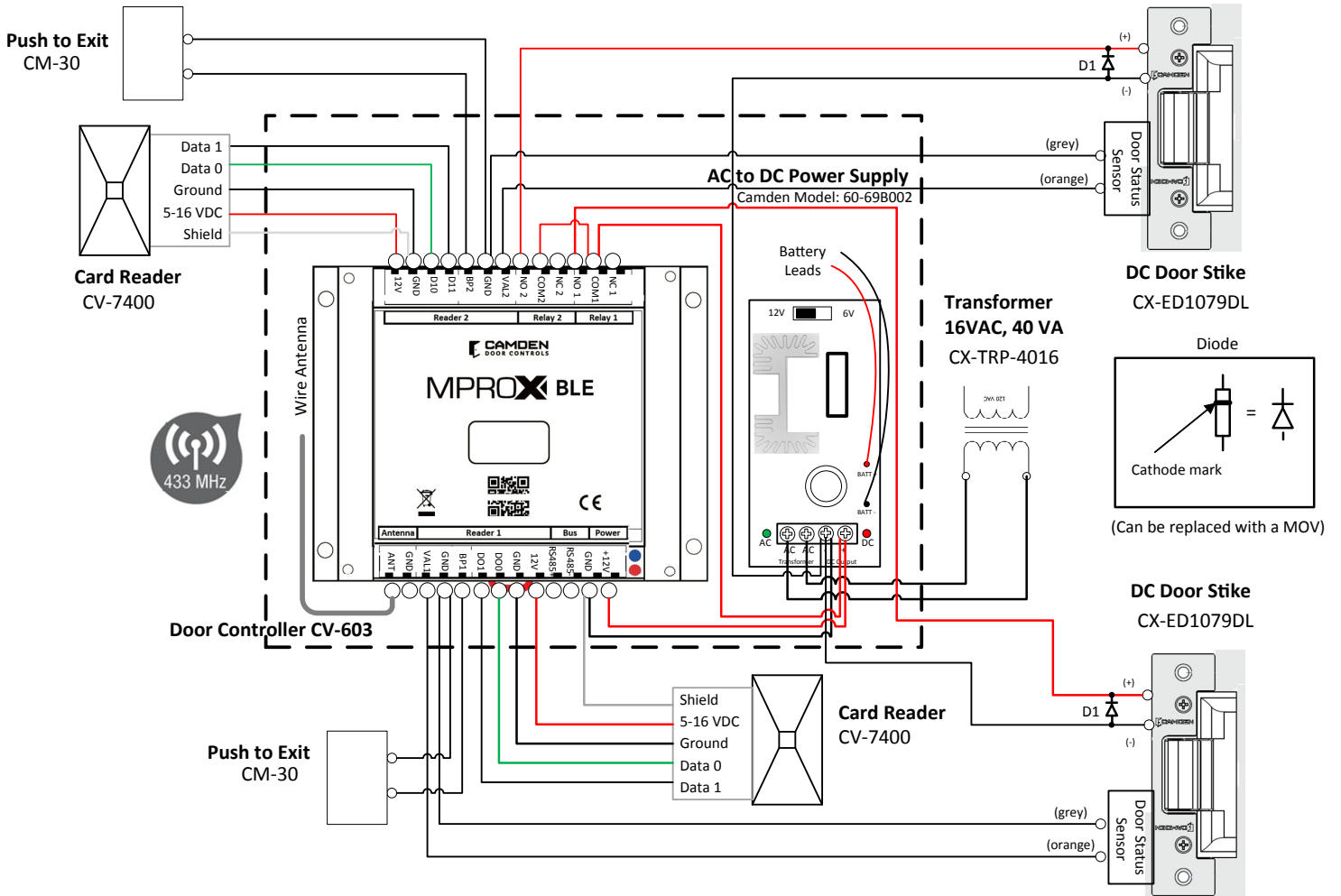
**System Operation:**

- a) The door is normally locked and closed. The door position switch confirms when the door is closed.
- b) A user presents a card credential in front of the card reader. The card reader's red LED indicates it is powered. When the credential is within 2 inches, the reader will beep, and the controller red LED will pulse on 1 second to confirm the credential data was received. If the controller red LED blinks twice, the credential is being denied by the controller.
- c) If the credential is approved by the controller, the door strike will energize for the pre-set period duration. The door strike will energize for the full duration of the period until the door is opened and the door position changes state. As soon as the door is opened, the door strike shall turn off securing the door as soon as it closes.
- d) Users exiting the door, must be detected by the request to exit device; manually by a push switch or automatically using a PIR detector. Opening the door without a request to exit switch shall cause the controller to generate a door forced open alarm.
- e) An alarm annunciator shall be triggered for the following selected alarm conditions. Relay 2 must be configured for ALARM and Relay 1 configuration must have door contact ON to activate these alarm conditions.
  - a. Intrusion
  - b. Door not opened after an approved credential read.
  - c. Door not closed after access. Alerts managers when the door is being left open.
  - d. Anti-passback
  - e. Access denied by location – Attempts made by credentials not approved by either reader 1, channel 1, reader 2 or channel 2.
  - f. Access denied by schedule.
  - g. Unknown user – a credential not enrolled into the controller user data base.
- f) Administrators shall use the app to control and configure the CV-603 controller using wireless Bluetooth. A steady on blue LED on the controller will confirm the connection.

**CV-603 MPROXBLE CONTROLLER / CV-603PS-K1 MPROXBLE CONTROLLER CABINET KIT**

**INSTALLATION INSTRUCTIONS**

**TWO DOORS: No Alarm Annunciator**



**CV-603 MPROXBLE CONTROLLER / CV-603PS-K1 MPROXBLE CONTROLLER CABINET KIT**  
**INSTALLATION INSTRUCTIONS**

**Bill of material:**

Item	Description	Quantity	Camden Model#	
			CV-603PS-K1	CV-603
1	Controller	1	CV-603 provided in kit	CV-603
2	DC Power Supply	1	60-69B002 - provided in kit	PS-13
3	Transformer	1	CX-TRP-4016 provided in kit	CX-TRP-4016
4	Door Strike, 12 VDC	2	CX-ED1079	CX-ED1079
5	Door Position Switch, a door latch monitor switch can be used, add suffix "L" to CX-ED1079	2	CX-MDA surface or CX-MDH recessed.	CX-MDA surface or CX-MDH recessed.
6	Proximity Card Reader, 125 KHz. Not required if transmitters are used.	2	CV-7400	CV-7400
7	Request to Exit Device	1	CM-RQE70 PIR sensor or CM-30E Push button.	CM-RQE70 PIR sensor or CM-30E Push button.

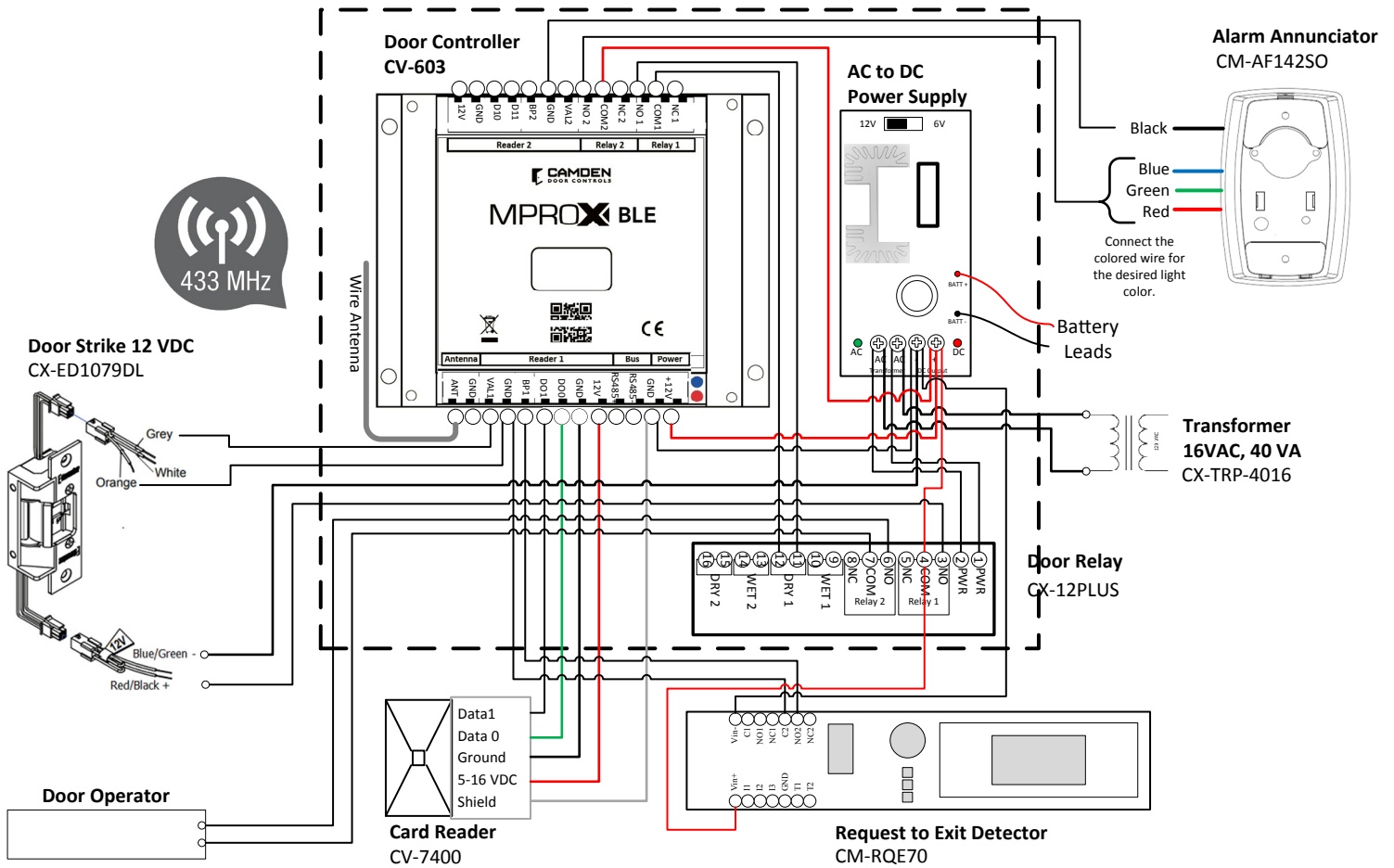
**System Operation:**

- a) The doors are normally locked and closed. The door position switch confirms when the doors are closed.
- b) A user presents a card credential in front of the card reader. The card reader's red LED indicates it is powered. When the credential is within 2 inches, the reader will beep, and the controller red LED will pulse on 1 second to confirm the credential data was received. If the controller red LED blinks twice, the credential is being denied by the controller.
- c) If the credential is approved by the controller, the door strike will energize for the pre-set period duration. The door strike will energize for the full duration of the period until the door is opened and the door position changes state. As soon as the door is opened, the door strike shall turn off securing the door as soon as it closes.
- d) Users exiting the door, must be detected by the request to exit device; manually by a push switch or automatically using a PIR detector. Opening the door without a request to exit switch shall cause the controller to generate a door forced open alarm.
- e) Administrators shall use the app to control and configure the CV-603 controller using wireless Bluetooth. A steady on blue LED on the controller will confirm the connection.

**CV-603 MPROXBLE CONTROLLER / CV-603PS-K1 MPROXBLE CONTROLLER CABINET KIT**

**INSTALLATION INSTRUCTIONS**

**SINGLE DOOR Frictionless Access Control Solution**



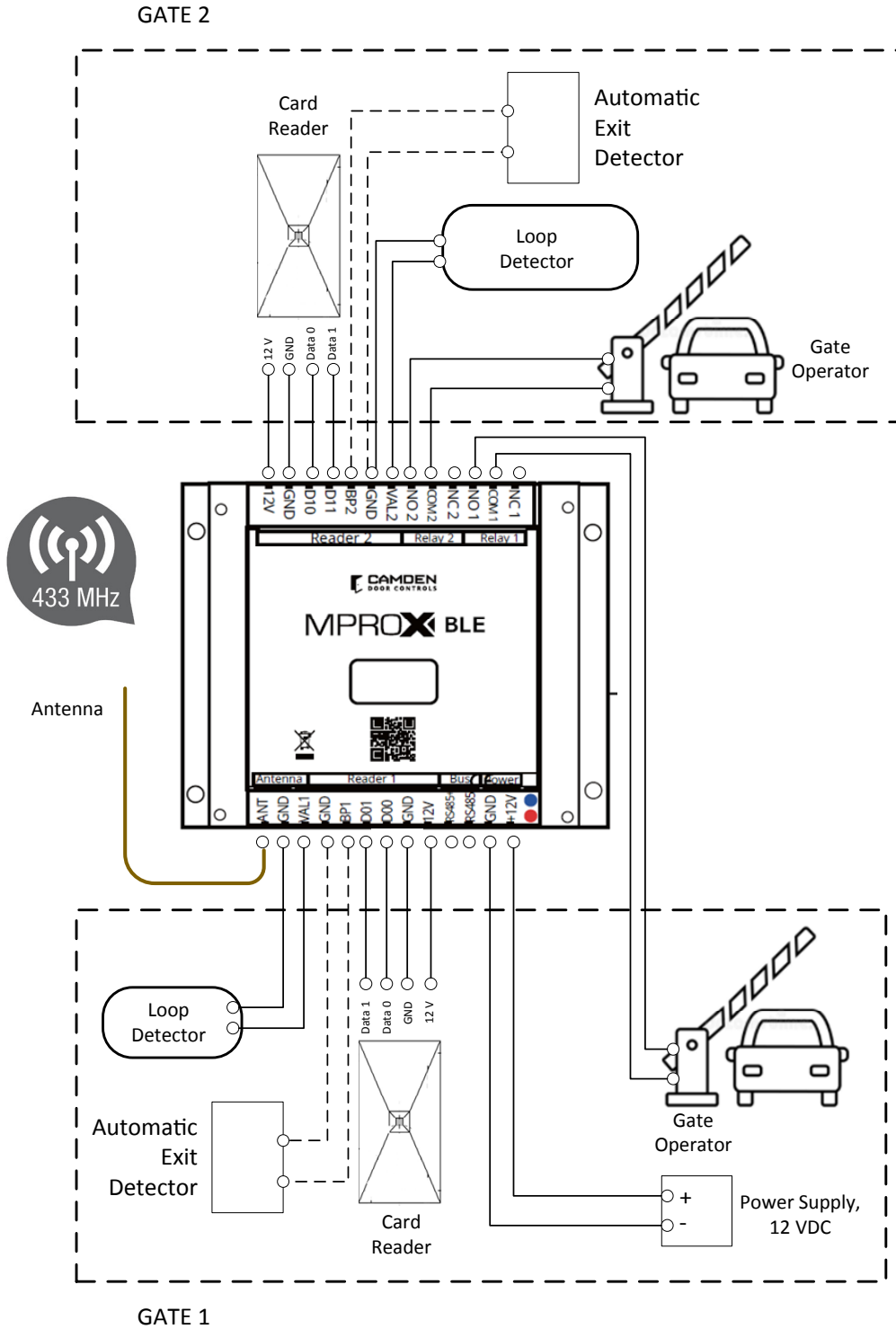
**Bill of material:**

Item	Description	Quantity	Camden Model#	
			CV-603PS-K1	CV-603
1	Controller	1	CV-603 provided in kit	CV-603
2	DC Power Supply	1	60-69B002 - provided in kit	PS-13
3	Transformer	1	CX-TRP-4016 provided in kit	CX-TRP-4016
4	Door Strike, 12 VDC	1	CX-ED1079	CX-ED1079
5	Door Relay	1	CX-12PLUS	CX-12PLUS
6	Door Position Switch, a door latch monitor switch can be used, add suffix "L" to CX-ED1079	1	CX-MDA surface or CX-MDH recessed.	CX-MDA surface or CX-MDH recessed.
7	Proximity Card Reader, 125 KHz. Not required if transmitters are used.	1	CV-7400	CV-7400
8	Request to Exit Device	1	CM-RQE70 PIR sensor or CM-30E Push button.	CM-RQE70 PIR sensor or CM-30E Push button.
9	Alarm Annunciator	1	CM-AF142SO	CM-AF142SO

**System Operation:**

- a) The system operation is identical to the single door operation (a) and (b).
- b) If the credential is approved by the controller, the door strike will energize for the pre-set period duration on the Cx-12 PLUS module. The door operator will trigger to operate after the door strike has been energized. Once the pre-set periods have expired, the door operator and strike shall de-energize from the Cx-12PLUS module.
- c) Users exiting the door, must be detected by the request to exit device; manually by a push switch or automatically using a PIR detector. Opening the door without a request to exit switch shall cause the controller to generate a door forced open alarm
- d) An alarm annunciator shall be triggered for the following selected alarm conditions. Relay 2 must be configured for ALARM and Relay 1 configuration must have door contact ON to activate these alarm conditions.
  - a. Intrusion
  - b. Door not opened after an approved credential read.
  - c. Door not closed after access. Alerts managers when the door is being left open.
  - d. Anti-passback
  - e. Access denied by location – Attempts made by credentials not approved by either reader 1, channel 1, reader 2 or channel 2.
  - f. Access denied by schedule.
  - g. Unknown user – a credential not enrolled into the controller user data base.
- e) Administrators shall use the app to control and configure the CV-603 controller using wireless Bluetooth. A steady on blue LED on the CV-603 controller will confirm the connection.

## TWO VEHICLE GATES: ANTI-PASSBACK



**CV-603 MPROXBLE CONTROLLER / CV-603PS-K1 MPROXBLE CONTROLLER CABINET KIT**  
INSTALLATION INSTRUCTIONS

---

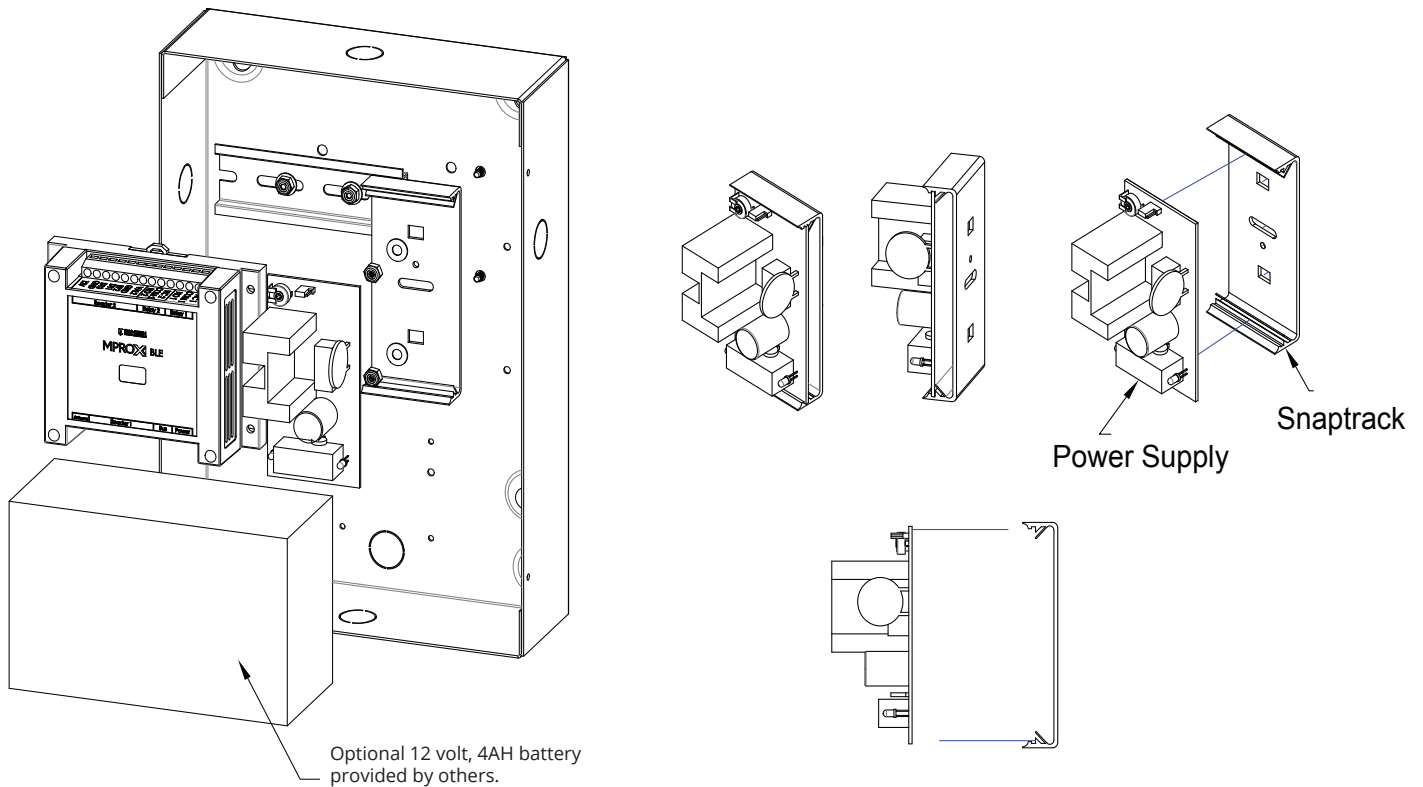
**Bill of material:**

Item	Description	Quantity	Camden Model #
1	MproxBLE Controller	1	CV-603
2	12 VDC Power supply, usually accessible from gate controller.	1	
3	Gate Operator	2	
4	Loop or beam detector	2	
5	Automatic exit switch or sensor	2	
6	Proximity Card Reader, 125 KHz	2	CV-7400
7	Request to Exit device	2	

**System Operation:**

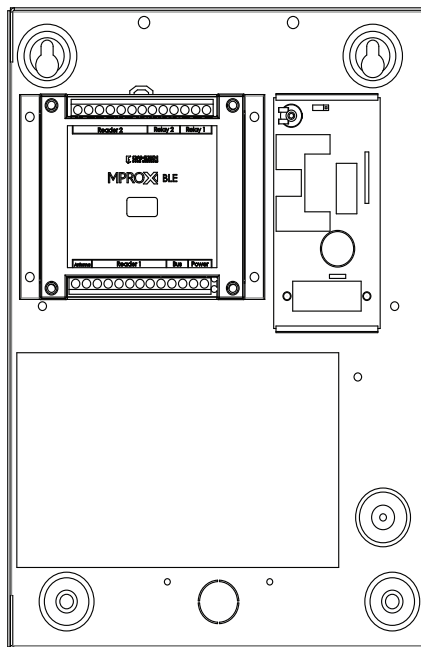
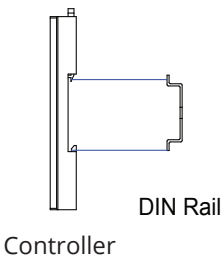
- a) The gates are normally closed.
- b) A vehicle approaches and stops in front of gate. A sensor or loop detector will validate the position of the vehicle and enable both the card reader and receiver. If the device wired to the VAL1 or VAL2 terminals do not detect the proper position of the vehicle, the reader and receiver will prevent the user to trigger the gate to open.
- c) Identical system operation for single door application (b).
- d) If an automatic exit sensor is connected to the controller, vehicles exiting will be detected by the exit device triggering the gate to open.
- e) Administrators shall use the app to control and configure the CV-603 controller using wireless Bluetooth. A steady on blue LED on the CV-603 controller will confirm the connection.

**6. CV-603PS-K1 CABINET ASSEMBLY**



**MProxBLE ASSEMBLY AND DINRAIL ASSEMBLY**

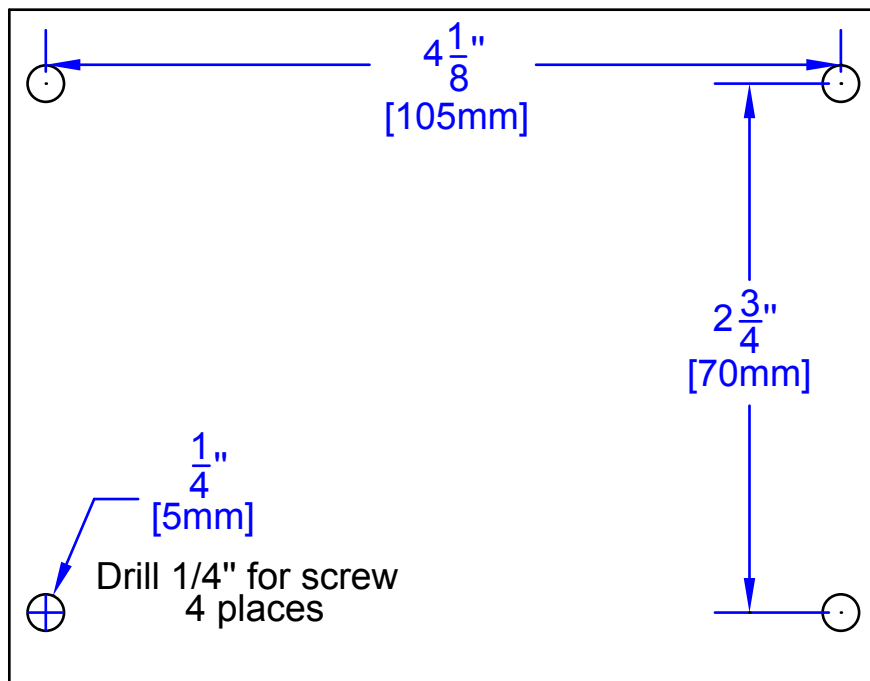
1. Take the top of the MProxBLE base and hook it onto the top of the DIN rail. Then take the bottom part with the red clip and push it onto the rail until it snaps into place.
2. Slide the component along the rail to desired location/spacing from component A.



**Power Supply ASSEMBLY**

1. Take the Snap track, align the 2 square holes with the mounting holes on the cabinet base.
2. Take the 2 screws and place them through the holes from the back of the cabinet. Place the washer over the snaptrack and over the screws. Screw the nuts onto the screw, securing the snaptrack is in place.
3. Push the power supply onto the top of the snaptrack, into the grooves allowing the snaptrack to hook onto the power supply.

6. CV-603 BLE TEMPLATE





## 7. SAFETY WARNINGS

These warnings are an integral and essential part of the product, and must be delivered to the user. Read them carefully: they provide important installation, operating, and maintenance instructions. Keep this form and give it to any persons who may use the system in the future. Incorrect installation or improper use of the product may cause serious danger.

## 8. INSTALLATION INSTRUCTIONS

- Installation must be performed by a qualified professional and must observe all local, state, national and European regulations.
- Before starting installation, make sure that the product is in perfect condition.
- Laying, electrical connections, and adjustments must be done to "Industry Standards". The product must be installed in a box not accessible to the operator.
- Do not install the product in an explosive environment or in an area disturbed by electromagnetic fields.
- The presence of gas or inflammable fumes is a serious safety hazard.
- Provide an overvoltage protection, mains/knife switch and/or differential on the power network that is suitable for the product and conforming to current standards. The manufacturer declines any and all liability if any incompatible devices and/or components are installed that compromise the integrity, safety, and operation of the product.
- Only original spares must be used for repair or replacement of parts. The installer must supply all information regarding the operation, maintenance, and use of individual components and of the system as a whole

## 9. MAINTENANCE

To guarantee the efficiency of the product, it is essential that qualified professionals perform maintenance at the times and intervals required by the installer, by the manufacturer, and by current law. All installation, maintenance, repair and cleaning operations must be documented. The user must store all such documentation and make it available to competent personnel.

**FCC:** This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Changes or modifications made to this equipment not expressly approved by Camden Door Control could void the user's authority to operate the equipment.

### TERMS AND LIMITS OF WARRANTY

Refer to Camden's warranty online for details.

[https://www.camdencontrols.com/about/product\\_warranty](https://www.camdencontrols.com/about/product_warranty)

# CV-603 Quick Start up Guide for User App

User friendly Bluetooth app provides quick and easy set-up and management for property and security managers.



**MPROX BLE**



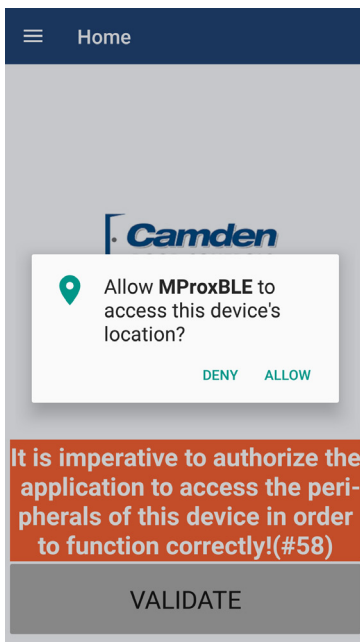
## 1. REQUIREMENTS:

1. CV-603 Controller
2. Smartphone with Bluetooth 5
3. The CV-603 app. (Supports both iOS and Android 5.0 and later).
4. Credentials; a proximity card, a key tag or 2 button transmitter, either or both.
5. Card Reader optional if no transmitters are used

## 11 STEPS TO GET THE MPROXBLE CONTROLLER CONFIGURED.

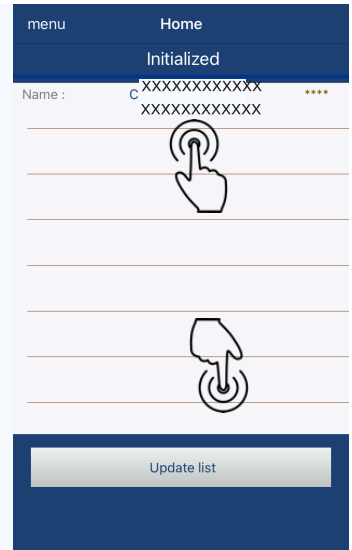
### 1. Download and install the app from Google Play or the App Store.

- a. Allow the app to access your internal storage.
- b. Bluetooth must be enabled on your phone and you must be within range of the MProxBLE controller for the app to respond. (under 60 feet, (20 m) is recommended.)



### 2. Open the app and click on UPDATE LIST icon.

- a. A default name for your controller will appear. The title will state uninitialized.



### 3. Tap on the default name and the home page will appear.

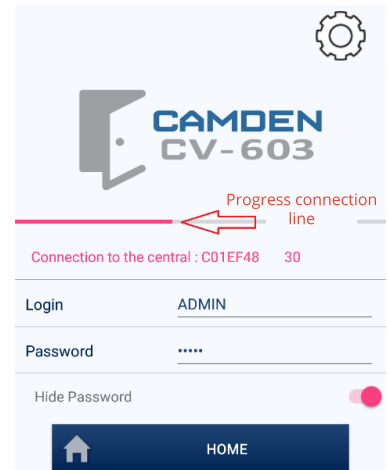
- a. Confirm you are connected to the controller by the 'connection to the central: (name)' message.
- b. The default login and password will appear (ADMIN).

### 4. Click on the CONNECT icon to connect to the controller.

- a. A progress line will scroll from left to right of the screen during this process.

**NOTE:** If the process line stops at the beginning, close the app and re-open the app to update list before attempting to connect again.

- b. The General Configuration screen will appear after connecting.
- c. It is recommended to replace the default equipment name that will be relatable to you. Example: 260 Main Street, Utility closet B2, etc.



**5. Adjust the 5 slide switches for the requirements of your site.**

Default recommendations have been selected to expedite the process.

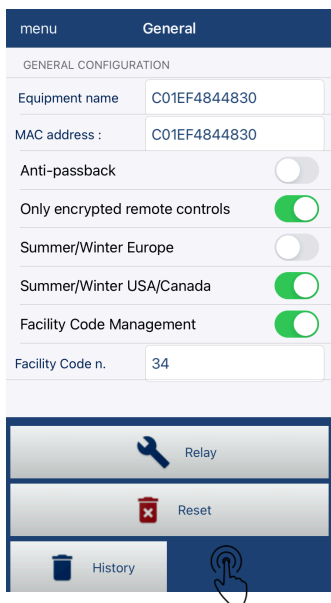
**a. Anti-passback:** Leave off if you do not intend to restrict users from sharing their card credentials with other people to gain entry.

**b. Only encrypted remote controls:** Turn on to get the best performance of 2 button transmitters, if used.

**c. Summer/Winter Europe or Summer/Winter USA/Canada:** Turn on only if your area is using daylight savings time.

**d. Facility code Management:** Turn on if you will be monitoring regularly the event reports.

**i.** If you turn on this feature, you must enter a value for the facility code that is being used on your card credentials. (1 to 255 if using 26-bit Wiegand cards.)



**6. Scheduling:**

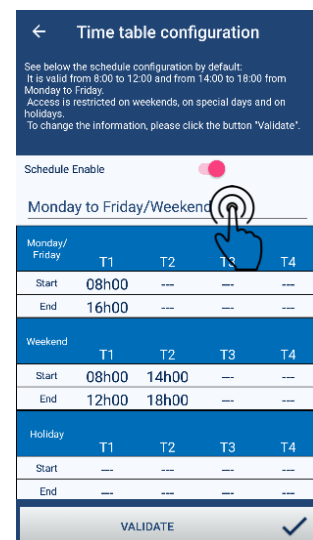
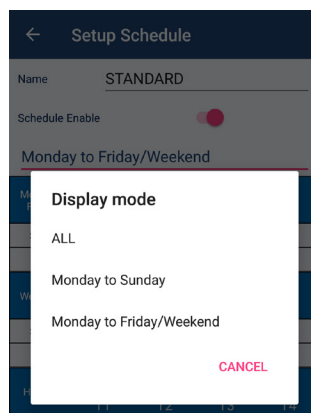
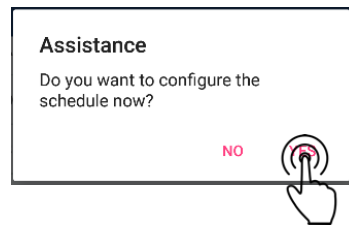
A pop up message will appear, "Do you want to configure a schedule now?" Click Yes to proceed to the Time table

**a.** You can rename the default name 'STANDARD' to M-F as an example or something relatable to your facility configuration.

**b.** Click on the ALL label underlined in red to select one of the three views; ALL, Monday to Sunday or Monday to Friday/Weekend.

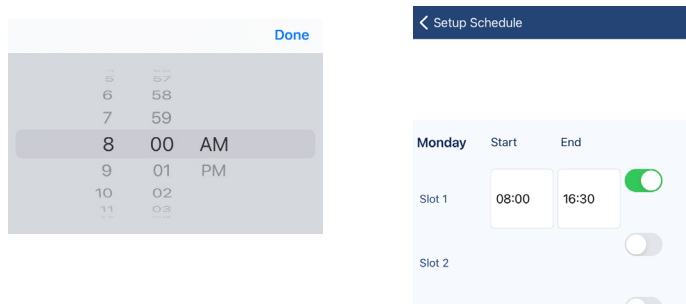
**c.** Click on the time to alter the time slots T1 to T4 per period.

**d.** To save your settings, click on VALIDATE icon at the bottom. (Android app). Click on DONE icon (iOS app).



**On iOS Devices**

Tap the time you wish to adjust and the time will appear on the bottom of the screen. Scroll the hours and minutes for the time preferred. To save the new values, tap on the DONE icon.



**7. Relay Configuration:**

There are three standard modes for the relays;

- (i) Momentary, 2 seconds on then off
- (ii) Timed, a period defined in hours, minutes, and seconds.
- (iii) Bistable or latched, the relay toggles on or off. Depending on the type of mode, secondary selections will appear.

**FEATURE RESTRICTIONS AND LIMITATIONS**

	<b>Momentary</b>	<b>Timed</b>	<b>Bistable or latching</b>	<b>Alarm ONLY Available for Relay 2</b>	<b>Description</b>
<b>Conditional Input</b>	ON or OFF	ON or OFF	Not Available	Not Available	This selection will prevent the respective relay to activate unless the controller validation terminals VAL1 or VAL2 are normally closed while a credential is being presented. To prevent vehicle tailgating this feature is turned on.
<b>Door Contact</b>	ON or OFF	ON or OFF {If ALARM features including intrusion, door not opened or door ajar are to be activated, this must be on.}	Not Available	Not Available	This will monitor the validation terminals VAL1 and VAL2 wired to a normally closed, door position switch. When active, the relay energized period will immediately turn off as soon as the door is opened to immediately relock the door as soon as it closes. Use this feature to prevent unauthorized entry by individuals reopening the door during the door release period.
<b>Schedule reading ID</b>	Select one of the predefined schedules.	Select one of the predefined schedules.	Select one of the predefined schedules.	Not Available	Select the schedule you wish for the selected mode to function. The default schedules; NEVER and ALWAYS will be available. If you added more schedules, you can select the schedule previously defined.
<b>Schedule forced opening</b>	Select one of the predefined schedules.	Select one of the predefined schedules.	Select one of the predefined schedules.	Not Available	The relay will automatically activate to the schedule selected.
<b>First Person In Delay</b>	ON or OFF	ON or OFF	ON or OFF	Not Available	The relay will not automatically activate (open) until an authorized credential is used. This is to prevent a relay to be energized unless an employee has entered the facility. Schedule forced opening must not be set to NEVER for this to appear.
<b>Unlock Time</b>	Not Available	In 00h: 00m: 00s:	Not Available	Not Available	Enter the time in hours, minutes, and seconds.
<b>Door Ajar Limit</b>	Not Available	In 00h: 00m: 00s:	Not Available	In 00h: 00m: 00s:	This feature is ideal for limiting the time the door can remain open to prevent unauthorized entry. The field appears only when the Door Contact is switched on.
<b>Alarm Delay</b>	Not Available	Not Available	Not Available	In 00h: 00m: 00s:	Enter the maximum time in hours, minutes and seconds before the relay automatically de-energizes.

**On Relay 2 ONLY**

For applications requiring a common alarm annunciation, relay 2 can be wired to an audible-visual device to alert security personnel to an alarm condition.

Click on Relay 2 mode field, to pop open relay operating mode choices. You will notice 'Alarm' as an additional selection. Click on 'Alarm' to open alarm selections below.

ALARM Conditions	Requirements	Description
<b>Alarm, Intrusion</b>	Relay 1 Door Contact must be ON	If the door is opened without a valid credential, an alarm condition will occur.
<b>Alarm, door not open</b>	Relay 1 Door Contact must be ON	If the door is not opened after a valid credential, an alarm condition will occur.
<b>Alarm, door not closed</b>	Relay 1 Door Contact must be ON	If the door is left open past the relay unlock time, an alarm condition will occur.
<b>Alarm, user anti-pass back</b>	ON or OFF	If a user violates the anti-pass back condition, an alarm condition will occur.
<b>Alarm, access denied by location</b>	ON or OFF	If a credential is used on unapproved reader, an alarm condition will occur.
<b>Alarm, access denied by time schedule</b>	ON or OFF	If a credential is used outside the time period selected, an alarm condition will occur.
<b>Alarm, access denied by date schedule</b>	ON or OFF	If a credential is used outside the dates selected, an alarm condition will occur.
<b>Alarm, Unknown User</b>	ON or OFF	If an unknown credential is used, an alarm condition will occur.

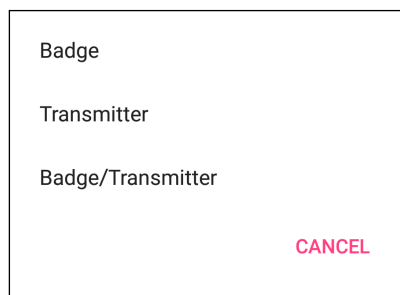
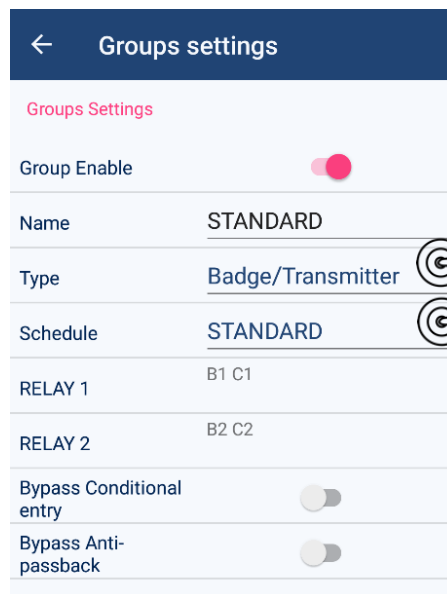
Once you have made the selections, click on the VALIDATE icon. A pop-up alert message will appear to confirm your settings have been saved. Click ok to close.

Alarm Output: RELAY2 is used for common alarm notifications when selected. RELAY 1 must be set to 'TIMED' mode.

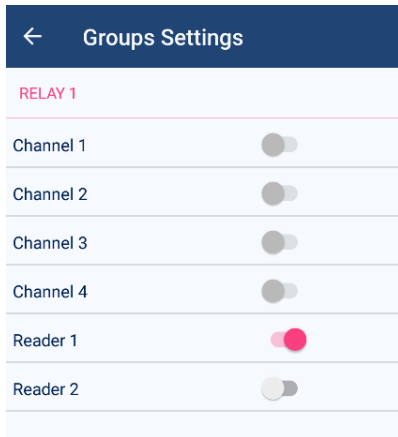
### 9. Group Configuration:

Every user must be assigned to a group. You can select to turn any group on or off from this screen.

- a. [Name] You can change the default group STANDARD or add a new name up to 17 characters.
- b. [Type] Tap on the default setting Badge/Transmitter and a pop-up selection will appear. Select the type of credential that will be accepted for this group.
  - i. Badge = Only cards or tags that are read inches away from a proximity card reader wired to the controller Reader 1 or Reader 2 terminals.
  - ii. Transmitter = Only battery powered, two button transmitters that can be read over 100 feet from the MProxBLE Controller.
  - iii. Badge/Transmitter = Both types of credentials will be accepted.
- c. [Schedule] Tap on the field right of the label to see one of the three default schedules for the group. Additional schedules can be added from the main menu selection under schedules.
  - i. Always – The group will always be active.
  - ii. Never – The group will never be active
  - iii. Standard – The active time and dates are defined in schedules.



d. [Relay 1 and Relay 2] Tap on the greyed out numbered letters B and/or C to open the list of actions that can trigger the relay.



i. C represents the channel; Channel 1 to 4 refers to a transmitter's button 1 to 4. Pressing the corresponding button for the active ON channel will trigger the relay. In most cases, only 2 buttons are used

ii. B represents the badge; Selecting Reader 1 and/or Reader 2 to determine which reader(s) can trigger the relay for the presented badge/card credential.

e. [Bypass Conditional entry] Turning on this feature by sliding the icon to the right will turn off the monitoring of the VAL terminals.

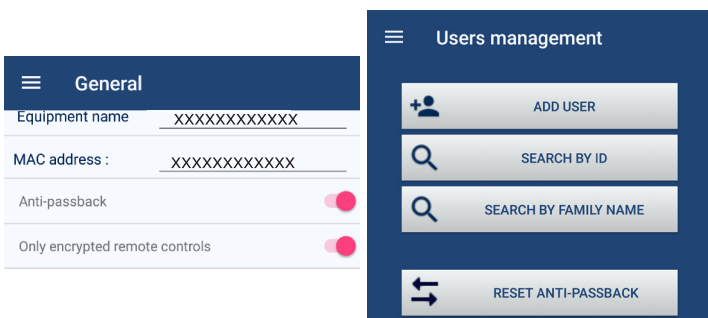
f. [Bypass Anti-pass back] Turning on this feature will ignore the pass back state of the user.

Once you have made the selections, click on the VALIDATE icon. A pop-up alert message will appear to confirm your settings have been saved. Click ok to close.

**10. User Management:**

This will bring you to the User Management screen where you can add, search, and reset the anti-pass back state.

**NOTE: The Reset Anti-pass back icon only appears if anti-pass back is selected on Central Settings from the main menu.**



All references to credentials could be either a two button transmitter or a proximity card/tag.

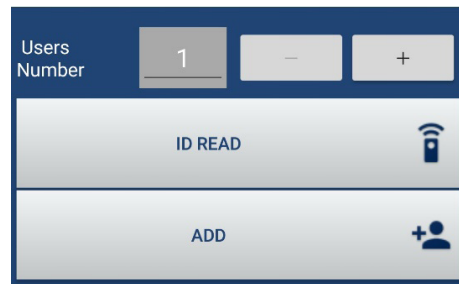
**Transmitter versus proximity credentials:**

**Two button transmitter** – The button #1 and #2 are preassigned to RELAY1 and RELAY2 for entry and exit.

**Proximity credentials** – You can use RELAY1 for access control and RELAY2 for alarm.

a. **ADD USER:** Click on ADD USER icon to open the screen to add user credentials. You can manually enter each Wiegand card number manually or auto-enroll the ID number using the ID READ icon.

**NOTE:** It is recommended that you use card credentials with the same facility code number you entered on Central Setting page. If you use cards that have a different facility code, you will be denied access due to a mismatch of facility codes. All credentials provided by Camden Controls will have identical facility codes to ensure ease of use.



i. **BULK ADD:** To bulk add a sequence of credentials, simply enter the start ID number into the User ID field.

ii. **Users Number:** Enter the number of credentials to be added or click on the + icon to increase the number of credentials to be added.

Click on ADD icon to complete. A confirmation pop up message will state "The user has been successfully added". Press OK to close.

b. **SEARCH BY ID:** To add the family and users name to the bulk credentials you added, click on the Search by ID, enter the first ID number you entered then click on the search icon. The User page for the assign ID will appear for you to complete the entry by adding the family and users name. When the name fields have been edited, click on the Validate icon to save it. Repeat this sequence for the remaining ID numbers that require the name fields to be filled.

i. To add only one card, simply enter the card ID number into the Users ID field or

ii. press ID READ icon to auto enroll the card ID by presenting the card in front of the card reader. Pressing the ID Read icon shall activate the unit to read the credential presented to the card reader to automatically place the credential code it read into the User ID field.

Simply enter the remaining data fields for family name, username, users group.

iii. Press ADD icon to add it to memory.

c. A confirmation pop up message 'The user has been successfully added' will appear. Press OK to close

**Adding Transmitters:**

Follow the same procedure above for adding one or many transmitters but press one of the push buttons to transmit the ID code to the controller.

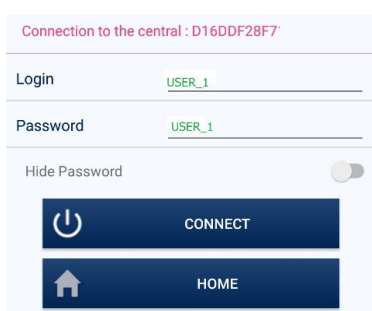
**11. Administrator Levels:**

Select Session Management from the main menu to define the 5 administrative levels. If you have numerous managers responsible for administrating this controller, you may wish to restrict specific capabilities to protect the original configuration or unclutter the screen to tasks the user is responsible for.

**NOTE: If you forget your password, you will need to do a factory reset deleting all previous settings and user IDs.**

**a. User:** You can change the default entry of USER\_1 by simply overwriting the field.

**b. Password:** You can change the default entry of USER\_1 by simply overwriting the field.

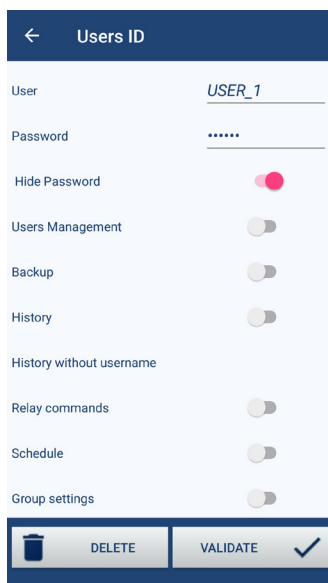


**c. User Management:** Enables the person to; add user IDs, search by ID, search by family name and reset the anti-pass back.

**d. Backup:** Enables the person to export or import data.

**e. History:** Enables the person to see past events by pressing the EVENTS icon.

**f. Relay Commands:** Enables the user to see the status of the validation inputs (VAL1/VAL2), the request to exit input (BP1/BP2) and Alarm status. They can manually activate Relay 1 and Relay



**g. Schedule:** The person can alter schedules, holidays and special days.

**h. User Group Settings:** The person can alter the group settings.

For site managers, they may only need the first three selections turned on; User management, Backup and History to perform their daily tasks.

To manually reset alarms, relay commands will need to be selected.

**ANTI-PASS BACK FEATURE:** MProxBLE uses hard anti-pass back. Users will be restricted from passing their credential, 'pass back', to another person to gain entry because once they have entered, the system knows that they are inside and won't let them re-enter unless they first exit. Hard anti-pass back maintains a high level of security but may inconvenience users who forget to use their card to enter or exit (by following someone else in). The system will have their status confused in the system if they do not badge in AND out, it will think that they are outside when they are inside, and so will not let them leave. Administrators can 'reset' the state of anti-pass back using the MProxBLE app.

Reader 1 is designated as 'entry' and Reader 2 is designated as 'exiting' under **User Management anti-pass** back field.

When you create a badge: its Anti-pass back status is «unknown» : it can be accepted indiscriminately the first time on an incoming or outgoing reader. As soon as it is accepted on a reader it loses its "unknown" state and enters the cycle of anti-pass back.

When the badge is accepted on an "entering" reader (reader 1), its state of Antipass-back is "exiting", means that it can only be accepted on an "exiting" reader

When the badge is accepted on an "exiting" reader (reader 2), its state Anti-passback is "entering" state means that it can only be accepted on an "entering" reader

When powering up the MProxBLE, all users systematically switch to an "unknown" state of anti-passback.

**Feature Table**

	Anti-Passback	Alarm	One Door	Two Doors	Request to Exit
Anti-Passback		Yes	Yes	Yes	Yes
Alarm	Yes		Yes	No	Yes
One Door	Yes	Yes		Not Applicable	Yes
Two Doors	Yes	No	Not Applicable		Yes
Request to Exit	Yes	Yes	Yes	Yes	

**CV-603 MPROXBLE CONTROLLER / CV-603PS-K1 MPROXBLE CONTROLLER CABINET KIT**  
INSTALLATION INSTRUCTIONS

