

CVCC ProDataKey (PDK) Administrative Documentation

July 2024

Contents

Introduction	2
PDK Apps	2
Definitions	2
CVCC Policies	3
System Overview	4
Physical Configuration	4
System Administration.....	6
System Navigation	6
Home Screen	6
CVCC Admin Screen	7
Procedure Guide	8
Creating A New Person	8
Defining a Group	12
Unlocking a Door Remotely (Ad Hoc)	15
Unlock a Door for 10 seconds.....	15
Unlock a Door for up to 90 minutes	15
Open a Door indefinitely (Force Toggle).....	16
Auto Open and Blackout Rules	18
Defining an AutoOpen / Blackout Rule.....	18
Ordering Proximity Cards.....	19
Troubleshooting.....	20

Introduction

The church's four main entrance doors are secured with an electronic lock system provided by ProdataKey (PDK). This document will provide guidance to the administrators who issue electronic entrance permissions to individuals and groups. Note: PDK has many more features which we will not use at CVCC. This documentation will only cover the features which we will be using.

PDK Apps

The PDK system features two apps:

- **ProdataKey Smartphone App** (Previously known as the **PDK Touch** app). This is a smartphone app available from the Google Playstore or the Apple App store, and is used by all users to temporarily unlock the main front entrance door. It is also used by System Administrators to manage the system and to remotely unlock any door.
- **PDK IO Browser App**: This is a browser app that can be accessed by administrators at <https://pdk.io>.

Definitions

The following definitions apply:

- **People**. All administrators and users of the system are referred to as People or collectively as Persons. People are identified in the system by the e-mail address they use to access the system, and are associated with a Group that determines their access privileges. People are also assigned an access Credential which determines the type of technology they will use to unlock a door.
- **Groups**. Groups are a collection of People. Rules are associated with each Group, determining which doors can be accessed at what times.
- **Credentials**. Credentials determine the type of technology an individual will use to unlock a door. There are two types of Credentials: Card and Mobile. Most CVCC users will use their Mobile phone to unlock a door. A limited few may be issued a proximity Card.
- **Rules**. Rules determine which doors can be unlocked by a Person at what times. All Rules should be granted to People through their Group assignment.
- **AutoOpen**. AutoOpen are recurring or one-time periods where the building locks should be unlocked. For example, all doors should be unlocked during our Sunday

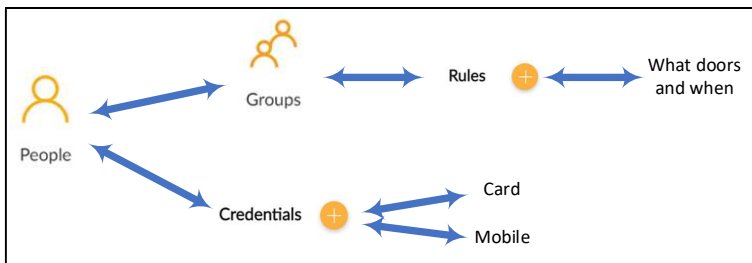
worship periods. Blackouts reverse the effect of a defined AutoOpen. Multiple AutoOpen and Blackout periods can be defined. Blackout periods override AutoOpen periods for the same time period.

CVCC Policies

This section documents policies that should drive how we use and configure the system.

- **Administrators.** System Administrators have the ability and primary responsibility to add and maintain users (People), Groups, Access Rules, and AutoOpen rules. Only two or three staff members trained in the administrative functions should be regarded as System Administrators. The church office has primary responsibility for all administrative functions within the PDK system.
- **Use of Groups.** All individuals (People) will be associated with a Group. Access privileges (Rules) will only be assigned to Groups.
- **Auto Open.** Auto Open is defined as every Sunday from 8AM to 12 Noon. All doors will automatically be unlocked during this period. Additional one-time or recurring Auto Open periods can be defined as needed.
- **Blackouts.** One-time Blackouts should be defined as needed to reverse the effect of a recurring Auto Open. An example of an appropriate Blackout period would be Cowboy Church, where we do not meet at the church building, and thus do not want the building to unlock. Blackouts override AutoOpen rules for the same time period.
- **Credentials.** Almost all users will be given Mobile credentials, allowing them to use their smartphone with the building's main front door reader. Users who struggle using smartphone technologies can be issued proximity cards.

The following shows the relationship between People, Groups, Access Rules, and Credentials.



System Overview

The PDK (<https://www.prodatakey.com/>) system provides a robust platform to control the issuance of electronic keys to unlock the four main entrance doors for the church. These doors are:

- Main entrance door
- Back entrance door (near the photocopier near the nursery)
- Right Paw entrance door
- Left Paw / Office entrance door

Each of these four doors are paired with a PDK Controller which facilitates communication and sends electrical pulses to door lock mechanisms (solenoid-activated crash bars). These door lock mechanisms are configured as normally locked (NC). It takes a manual push on the crash bar (from inside the building) or an electrical pulse from the PDK controller to open/unlock them. During power outages, the doors remain locked.

PDK controllers work with the church's Internet connection to reach PDK servers. PDK servers maintain a database of electronic key holders, door lock configurations, and transactions (including unlock authorizations). PDK's servers also provides a Web browser interface for the church's administration of the system.

The system provides redundancy should the church's Internet connection, provided by Frontier, fails. Two of the doors (Front and Back entrances) are configured with a physical key with very limited distribution should there be an electrical outage at the building

The church pays a recurring fee to PDK that covers support, software upgrades and warranty service.

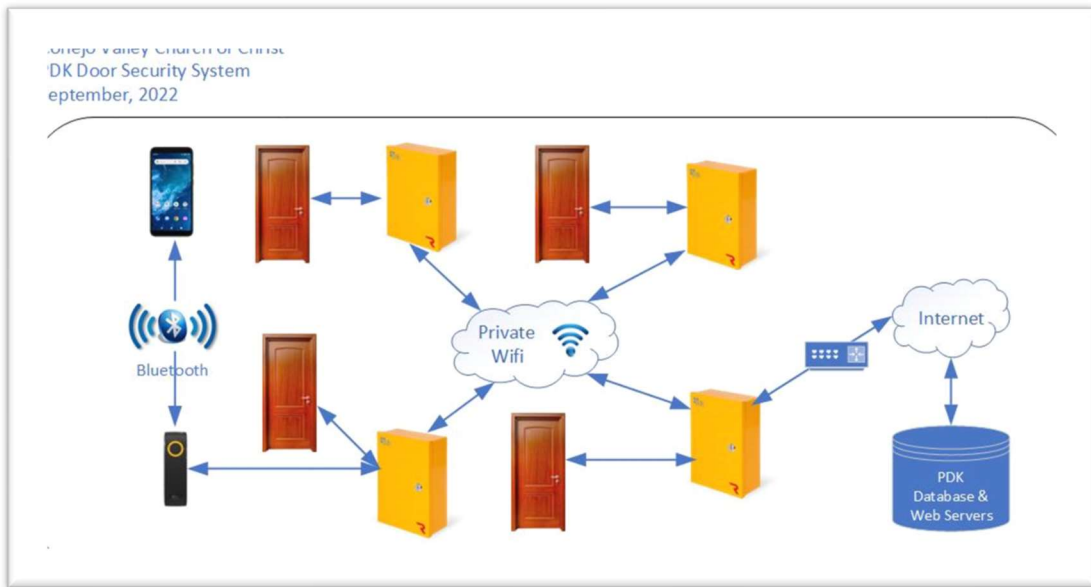
Physical Configuration

The core physical component of the PDK system is the PDK Controller, easily identifiable by their bright orange metal box. PDK Controllers reside in the following places in the church building:

- Kitchen, controlling the main entrance door.
- Children's Ministry Photocopier alcove, controller the back entrance door.
- Right Paw classroom, controlling the door outside that room.
- AV/Network closet, controlling the Office door.

CVCC ProDataKey Administration Documentation

Each Controller is connected to one door and is interfaced to the door's electric opening relay.



The Controller in the AV/Network closet is connected to the church's router, and thus to the Internet. The other three Controllers communicate with that Controller via a private WIFI network.

At the front door, user smartphones communicate with a reader mounted on the door frame. At other doors, phones unlock doors via cellular data communications via the Internet.

All data (users, door configurations, access authorizations, etc.) are maintained in the cloud by PDK.

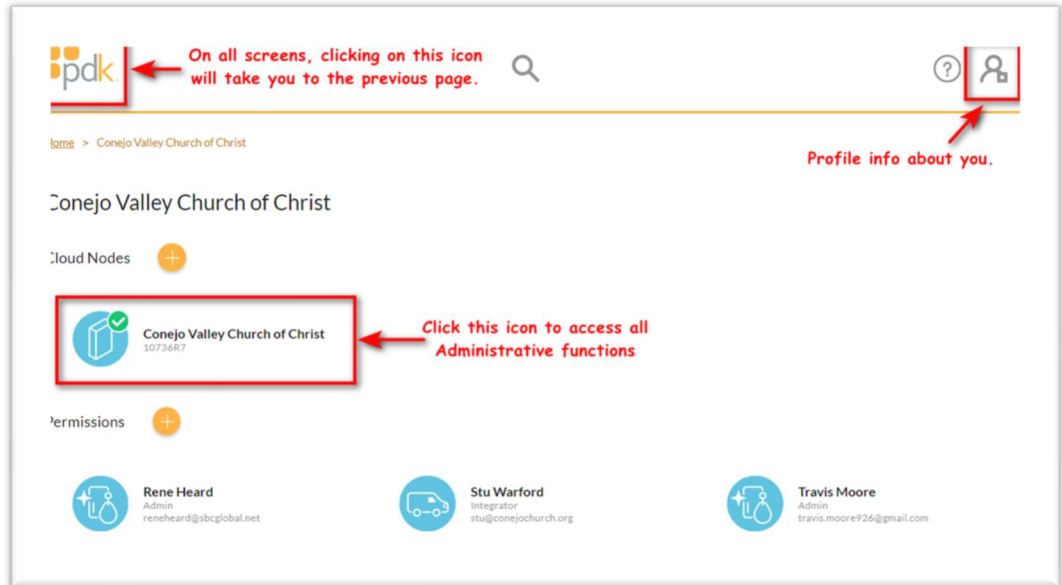
System Administration

it is highly recommended that all administrative actions take place via a web browser (Chrome, Internet Explorer, Firefox, etc.) on a desktop or tablet. The following screen shots are from a desktop browser.

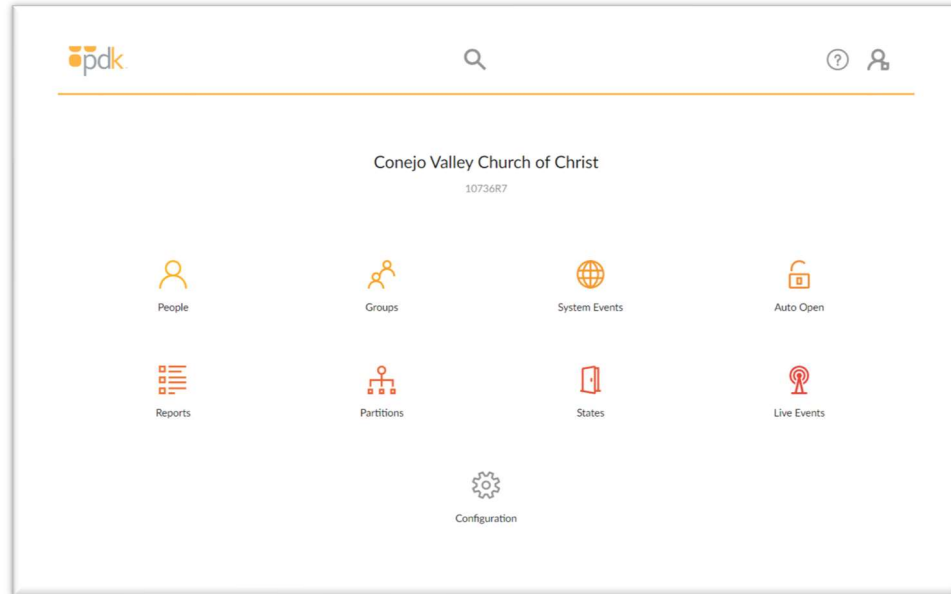
System Navigation

Home Screen

The following is the “Home” PDK screen. Administrators should not perform any administrative functions on this screen.



CVCC Admin Screen



The CVCC Admin Screen will be the screen administrators will use for the vast majority of their work.

People – Click this icon to add new people (members and others) who will need access to the building.

Groups – Click this icon to add new groups to the system.

System Events – The PDK system will allow us to define events which should occur at specified times, such as notifying one of the system admins when a door is open in the middle of the night. We will make limited use of this feature.

Auto Open – This will cause our doors to automatically unlock during public worship services.

Reports – We can define and run reports of all entities and transactions in the system.

Partitions – We will not be using partitions at CVCC.

States – This is where our Doors are defined in the system. You can unlock and lock a door remotely via this icon.

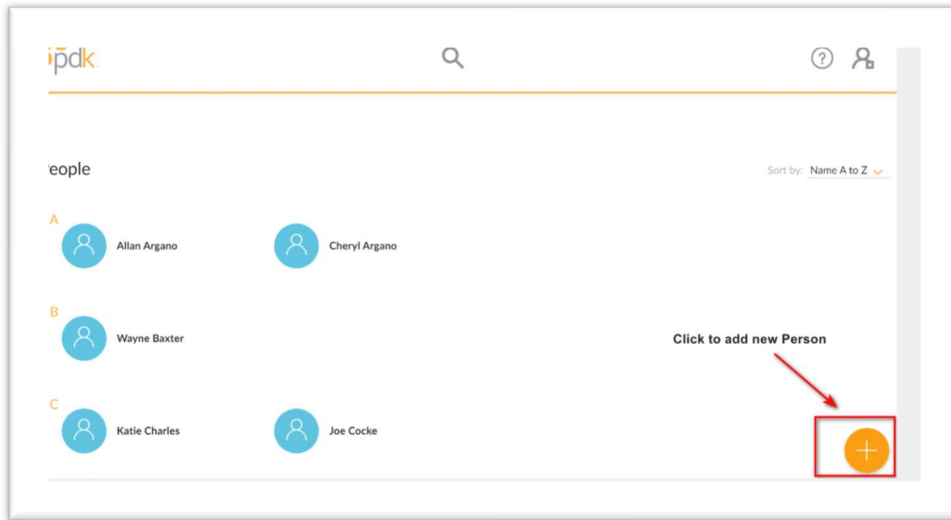
Live Events - Live Events is a feature that shows door events that are happening in real-time. The current state of doors is displayed, as they occur.

Procedure Guide

Creating A New Person

To authorize a person to access the building, add and configure the person as follows:

1. Navigate to the People screen.
2. Press the “+” sign on the People screen

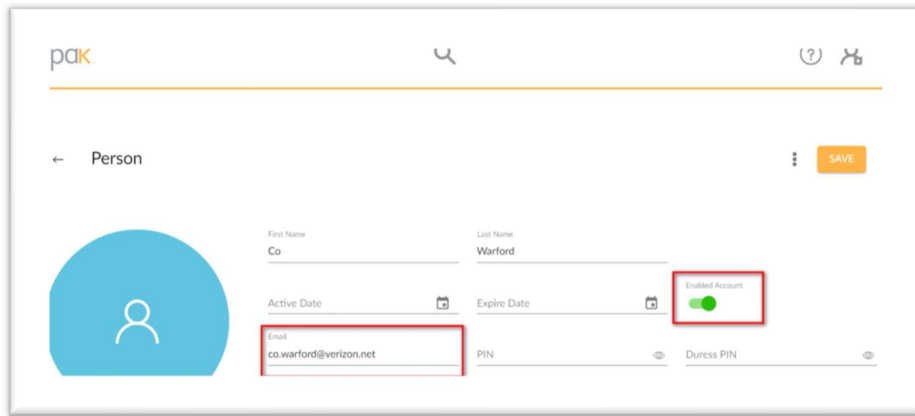


3. Fill out the Add Person form. All that is needed here is the first and last names. Press the Add button.

The screenshot shows the 'Add Person' form. The form has two tabs: 'SINGLE' (selected) and 'IMPORT'. There are two input fields: 'First Name' with the text 'Co' and 'Last Name' with the text 'Warford'. At the bottom right, there are two buttons: 'CANCEL' and 'ADD'.

CVCC ProDataKey Administration Documentation

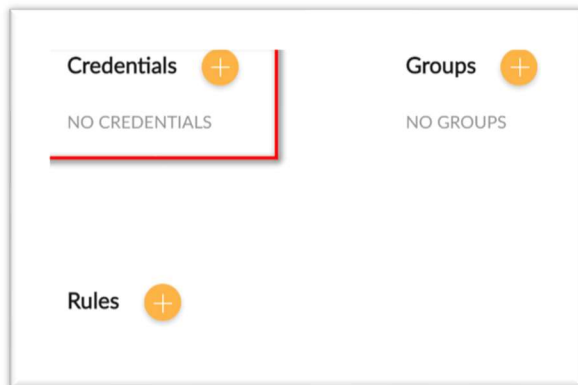
4. Provide the e-mail address the person will use with the system. Make sure the Enabled Account flag is set to the right (green).



The screenshot shows the 'Person' management interface in the pdk system. The interface includes a search bar at the top, a back arrow, and a 'SAVE' button. The profile information is as follows:

Field	Value
First Name	Co
Last Name	Warford
Active Date	
Expire Date	
Email	co.warford@verizon.net
PIN	
Duress PIN	
Enabled Account	Yes (Green)

5. Press the “+” sign next to the Credentials label.



The screenshot shows the administration interface with three main sections:

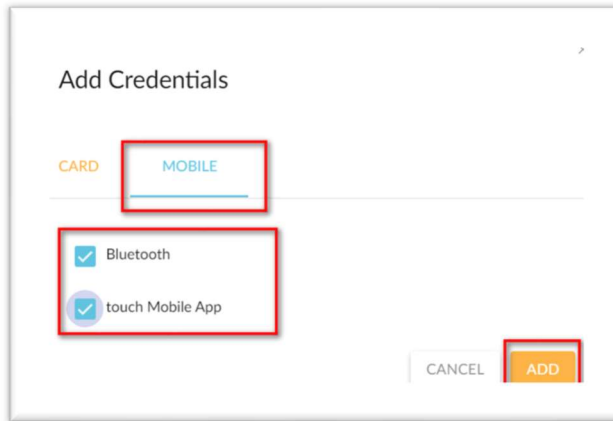
- Credentials** (+) - NO CREDENTIALS
- Groups** (+) - NO GROUPS
- Rules** (+)

The 'Credentials' section is highlighted with a red box, and the plus sign next to it is the target for the next step.

CVCC ProDataKey Administration Documentation

6. Add the appropriate Credentials:

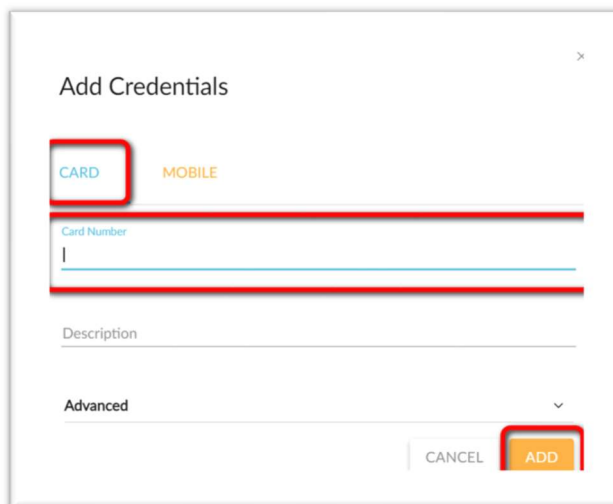
- a. **Mobile Phone:** If the user will use their Smartphone and the ProDataKey app, press the “Mobile” tab, and check both “Bluetooth” and “touch Mobile App”. Click “Add”.



The screenshot shows a dialog box titled "Add Credentials". At the top, there are two tabs: "CARD" and "MOBILE". The "MOBILE" tab is selected and highlighted with a red box. Below the tabs, there are two checkboxes: "Bluetooth" and "touch Mobile App", both of which are checked and highlighted with a red box. At the bottom right, there are two buttons: "CANCEL" and "ADD". The "ADD" button is highlighted with a red box.

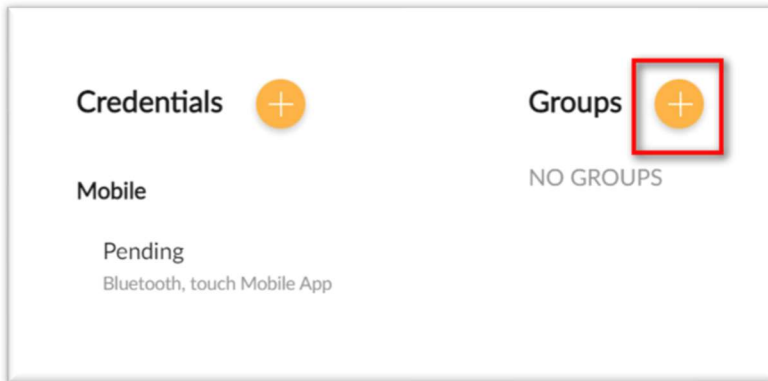
Note: “Bluetooth” is required to allow the smartphone to work with the main entrance door reader. “Mobile App” is required to allow a user to unlock a door without a reader.

- b. **Proximity Card:** If the user will use a proximity card, press the “Card” tab, and enter the last five digits of the eight-digit card number of the card you are issuing to the user. For Example, if the card number is 10057861, then enter 57861. The Description field is optional. Click “Add”.

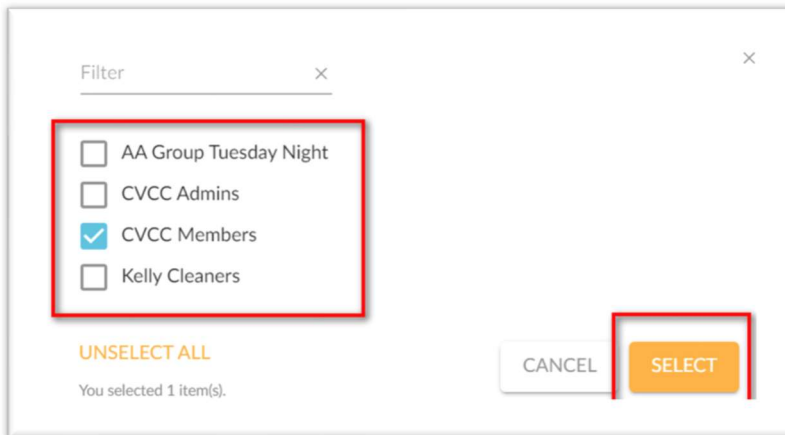


The screenshot shows a dialog box titled "Add Credentials". At the top, there are two tabs: "CARD" and "MOBILE". The "CARD" tab is selected and highlighted with a red box. Below the tabs, there is a "Card Number" input field, which is empty and highlighted with a red box. Below the "Card Number" field is a "Description" input field. At the bottom right, there are two buttons: "CANCEL" and "ADD". The "ADD" button is highlighted with a red box.

7. Press the “+” sign next to the Groups label.

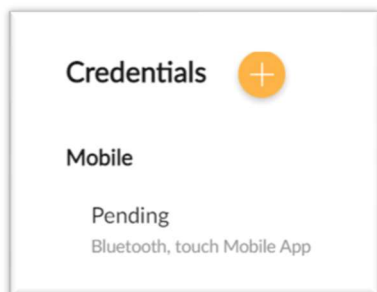


8. Check the appropriate Group(s) for the person. Click “Select”.

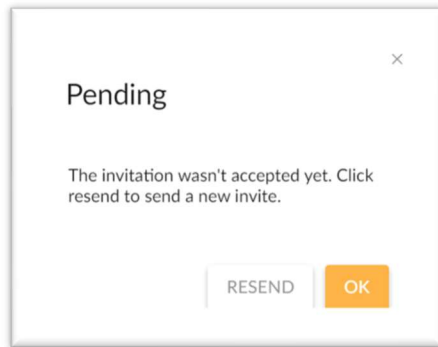


Note: Do not define any “Rules” for the person. In our implementation, rules are defined at the Group level.

Setting up an individual in this manner will cause the system to send the person an e-mail, inviting them to install the ProDataKey software and providing a button for them to use to “authenticate” themselves to the system. The person’s Credential status will change to “Pending” until they do so.



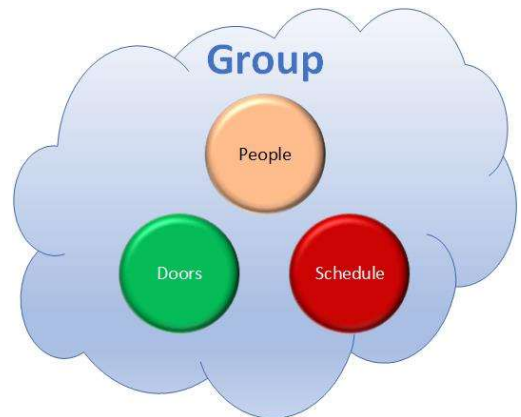
If the person indicates they have not received the e-mail, have them check their “Spam” folder. Click on “Pending” to cause the system to resend the e-mail invitation.



Defining a Group

Groups are an association of people. In essence, Groups are an easy way of providing People with access to a group of doors with a particular schedule.

PDK provides the option of defining door access rules to each individual user in the system. But instead, we will be defining door access rules for different Groups, and then associating each individual user with a Group.



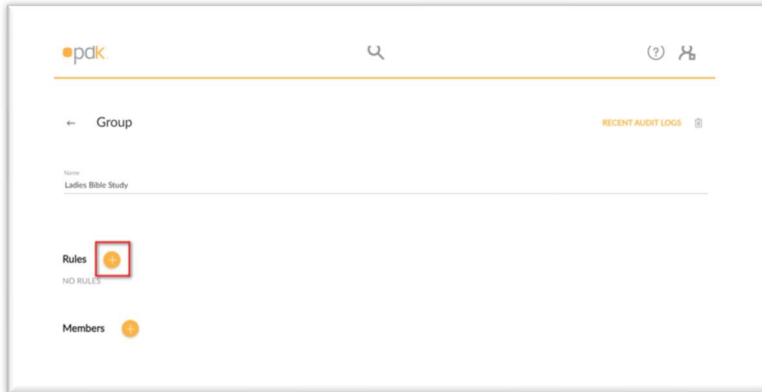
To define a Group within the system:

1. Navigate to the Groups screen.
2. Click the “+” button.
3. Add a Name for the Group. Click “Add”.

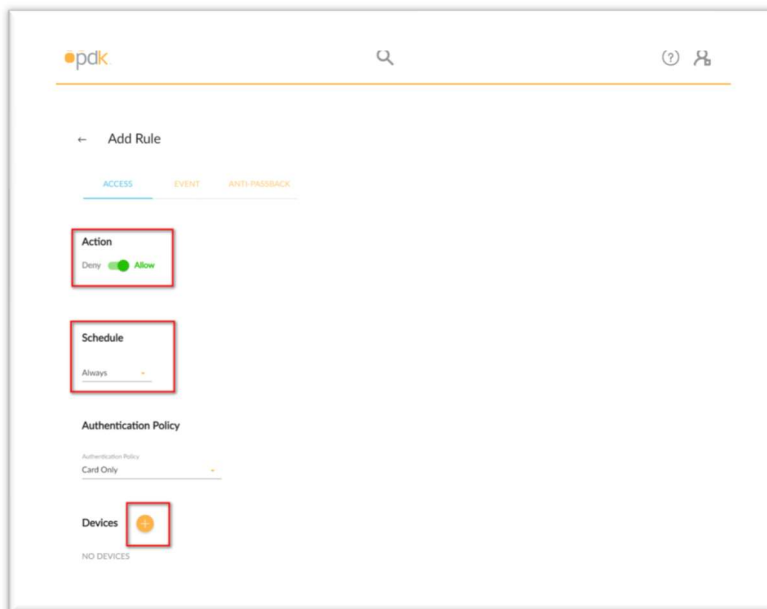


CVCC ProDataKey Administration Documentation

- Click on the “+” sign next to the Rules label.



- Set the Action to “Allow”.



- Set the Schedule as appropriate for all members of the Group. The Scheduling options are available:
 - Always** – Any Group member can open the door(s) 24 X 7.
 - Recurring** – Any Group member can open the door(s) according to a recurring schedule, e.g. 7PM to 9PM on Tuesdays only. Most Group access Rules will use a recurring schedule.
 - Single Date** – Any Group member can open the door(s) during a specific date and time.

CVCC ProDataKey Administration Documentation

The screenshot shows the 'Schedule' configuration interface. It includes a dropdown menu for scheduling options, time selection fields for start and stop times, and a day-of-week selector. Red boxes and arrows highlight specific elements: the 'Recurring' dropdown, the '19:00:00' and '21:00:00' times, and the 'TU' day selector.

Schedule

Recurring

Start Time
19:00:00

Stop Time
21:00:00

SU | MO | **TU** | WE | TH | FR | SA

Three scheduling options:
- Always
- Recurring
- Single Date

Note military time format

Highlighted DOW is selected

7. Select the Devices (doors) you want this Group to access. Press the “+” sign next to the Devices label.

The screenshot shows a 'Filter' dialog box with a list of devices. The 'Front Door' device is selected, indicated by a checked checkbox. The 'SELECT' button is highlighted with a red box.

Filter

Front Door

Office

Rear Door

Right Paw

UNSELECT ALL

You selected 1 item(s).

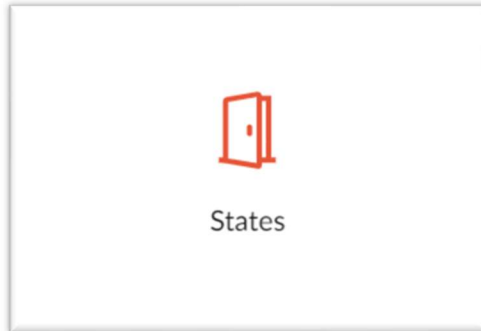
CANCEL SELECT

You can ignore the Event and Anti-Passback tabs on the **Add Rule** screen.

Unlocking a Door Remotely (Ad Hoc)

To open a door remotely, either in the building or from any internet connection:

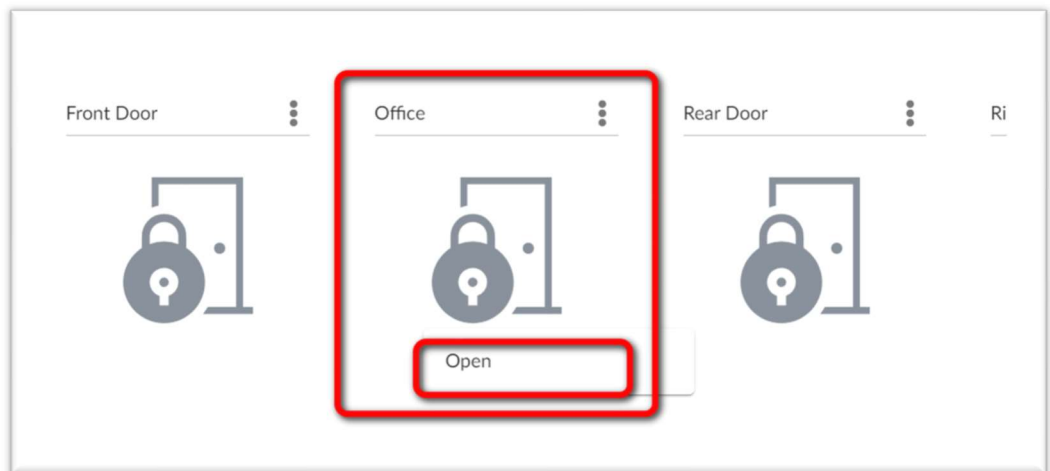
1. Navigate to the States screen.



You can unlock a door for 10 seconds, for up to 90 minutes, or indefinitely.


Unlock a Door for 10 seconds

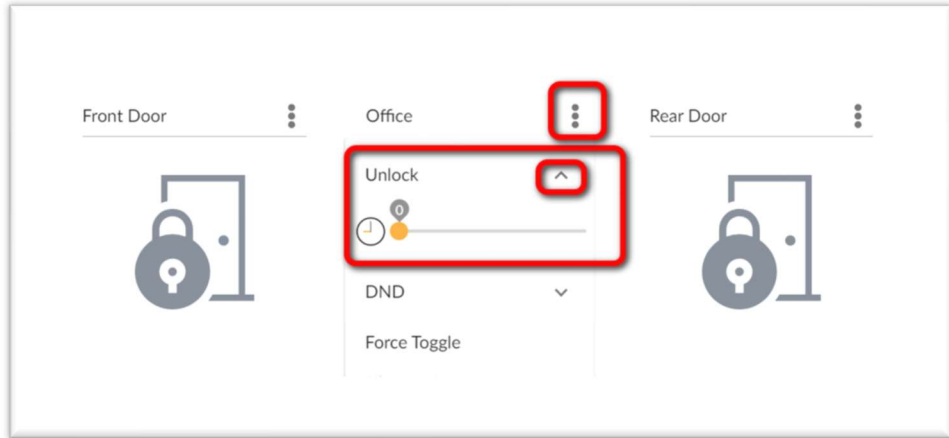
- Click on any Door, and select **Open** to unlock the door for 10 seconds.



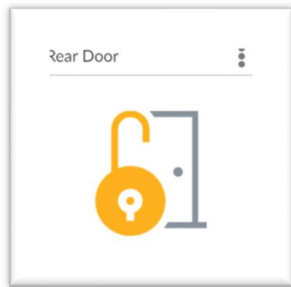
After 10 seconds the door will automatically relock.


Unlock a Door for up to 90 minutes

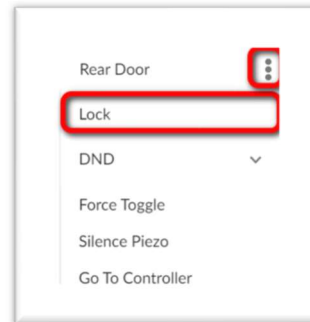
1. Click on the symbol  next to the Door you want to unlock.
2. Click on the down arrow next to Unlock. A slider will appear.
3. Slide the slider right and left to set the amount of time you want the door to remain unlocked, from zero to 90 minutes.



While the door is unlocked the door icon on the Door and Devices screen will change to indicate the door is in an unlocked state




To cancel this state, simply click on the  symbol and click on the **Lock** button.

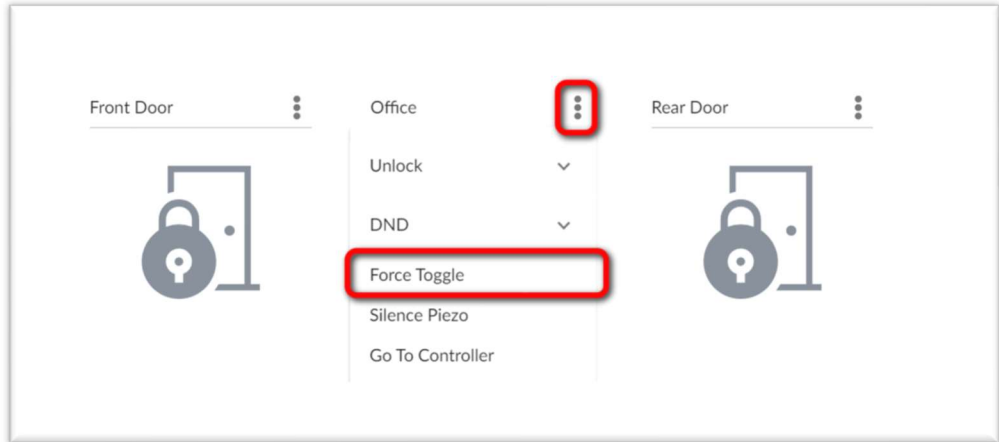


Open a Door indefinitely (Force Toggle)

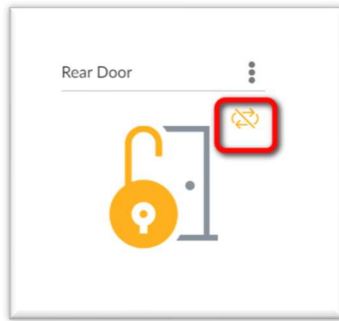
Note: Be very careful unlocking a door indefinitely. It will remain unlocked until the Force Toggle is cancelled.


1. Click on the  symbol next to the Door you want to unlock.
2. Click on **Force Toggle**. The door will unlock and remain unlocked indefinitely.


CVCC ProDataKey Administration Documentation



While the door is unlocked the door icon on the Door and Devices screen will change to indicate the door is in an unlocked state.



The  icon indicates the door is unlocked via a **Force Toggle** process.

To cancel the Force Toggle, simply click on the  symbol and click on **Force Toggle** again.

Auto Open and Blackout Rules

There are times when the building should automatically unlock and remain unlocked for a set period of time. The prime example of this would be our weekly Sunday morning worship service. But there may be other examples, such as when AA groups use the building or when we have a special one-time event, such as our Trunk or Treat event.

The automatic unlocking of doors for a specific period can be accomplished with the definition of an AutoOpen rule. An unlimited number of AutoOpen rules can be defined, and each can be defined as either a one-time or a recurring rule.

Auto Open are recurring or one-time periods where the building locks should be automatically unlocked. For example, all doors should be unlocked during our Sunday worship periods.

When setting up a *recurring* Auto Open rule, such as for Sunday Morning Worship services, there may be times when we want to override the recurring rule and NOT have the door unlock. For example, although we want the doors to automatically unlock on almost every Sunday, we don't want them to unlock on a Sunday where we are not meeting at the church building, such as on a Cowboy Church Sunday. We can temporarily suspend an Auto Open rule with a Blackout rule.

Blackout rules reverse the effect of a defined AutoOpen rule, and are useful in those situations where we won't use the building during a normal AutoOpen schedule.

Multiple AutoOpen and Blackout periods can be defined. Blackout periods override AutoOpen periods for the same time period.

Both AutoOpen and Blackout rules are defined on the AutoOpen page.

Defining an AutoOpen / Blackout Rule

1. Navigate to the AutoOpen screen. Any defined AutoOpen/Blackout rules will be displayed.
2. Click the + button.
3. Provide a Name for the AutoOpen rule, such as "Weekly Tuesday AA Meeting"
4. Set Action. **Allow** will define this as an AutoOpen rule. **Deny** will define this as a Blackout rule.
5. Set the Schedule option:
 - **Always**: sets the rule to always be active 24 X 7 X 365.

CVCC ProDataKey Administration Documentation

- **Recurring:** sets the rule to be active according to a recurring schedule, e.g., every Sunday from 8:30AM to 1PM.
 - **Single Date:** sets the rule to be active for a single date/time period only, e.g., Tuesday, December 4 from 1PM to 3PM.
6. Set the date and time periods accordingly.
 7. **Devices** – Press the + button and select the doors to be unlocked by the rule.

← Auto Open

Name

Action

Deny Allow

Schedule

Recurring

Start Time: 00:00:00

End Time: 24:00:00

SU MO TU WE TH FR SA

Devices +

NO DEVICES


Ordering Proximity Cards

The PDK system uses industry standard 125 kHz 26 bit H10301 proximity cards, available from most office supply and on-line stores, such as Amazon.

Troubleshooting

Here are some tips, should a user have problems using their smartphone with the system.

1. Have the user reboot their phone and try again.
2. Double check the following in the user account in PDK.IO:
 - a. Is the user account Enabled?
 - b. Does the user have assigned Mobile credentials for their smartphone?
 - c. Are both the Bluetooth and Mobile App boxes checked on their Mobile credential?
 - d. Does the user belong to an appropriate user Group?
 - e. Is the users' Group authorized for the particular door and for the appropriate day and time?
3. If the person indicates they have not received the enrollment e-mail, have them check their "Spam" folder.
4. Review the person's Recent Audit Logs. Within the PDK.IO application:

People -> (User) ->  -> Recent Audit Logs.
5. If all else fails, do the following:
 - a. Have the user uninstall the ProDataKey app on their phone.
 - b. Delete the Mobile credentials from the user.
 - c. Add new Mobile credentials to the user. The user should receive an invitation to add the app to their phone and to Activate their credential.

CVCC ProDataKey Administration Documentation

Following is a single page snapshot showing how a Person should be configured.

The screenshot displays the 'Person' configuration page in the CVCC ProDataKey administration system. The page includes a header with the 'pdk' logo, a search icon, and user profile icons. The main content area shows the following details for a person named Joe Cocke:

- First Name:** Joe
- Last Name:** Cocke
- Active Date:** (calendar icon)
- Expire Date:** (calendar icon)
- Email:** jceps11254@gmail.com
- PIN:** (input field)
- Duress PIN:** (input field)
- Enabled Account:** A toggle switch is shown in the 'ON' position, highlighted with a red box and the annotation: "Account must be set to Enabled".

Below the profile information are three sections, each with a red box and an annotation:

- Credentials:** Shows a 'Mobile' credential with ID 'SM-G991U' and supported methods 'Bluetooth, Mobile App'. An annotation points to this section: "Mobile credentials should be set to Bluetooth for most users. Administrators should also be granted Mobile App credentials."
- Groups:** Shows the person is assigned to the 'CVCC Members' group. An annotation points to this section: "All members should be in the CVCC Members group. Non-members should be associated with a non-member group. System administrators should belong to the CVCC Administrators group."
- Rules:** Shows 'NO RULES'. An annotation points to this section: "Do not add Rules to anyone. Rules should be applied to everyone via their Group assignment."