PDK Access Control User Guide 2025

Introduction

The pdk.io portal offers an intuitive, user-friendly interface for managing your access control system. Your installer should have granted you access to pdk.io and provided initial training. This guide serves as a reference for using key features, including Groups, People, Permissions, Auto-Open, System Health, Holidays, Reports, and States.

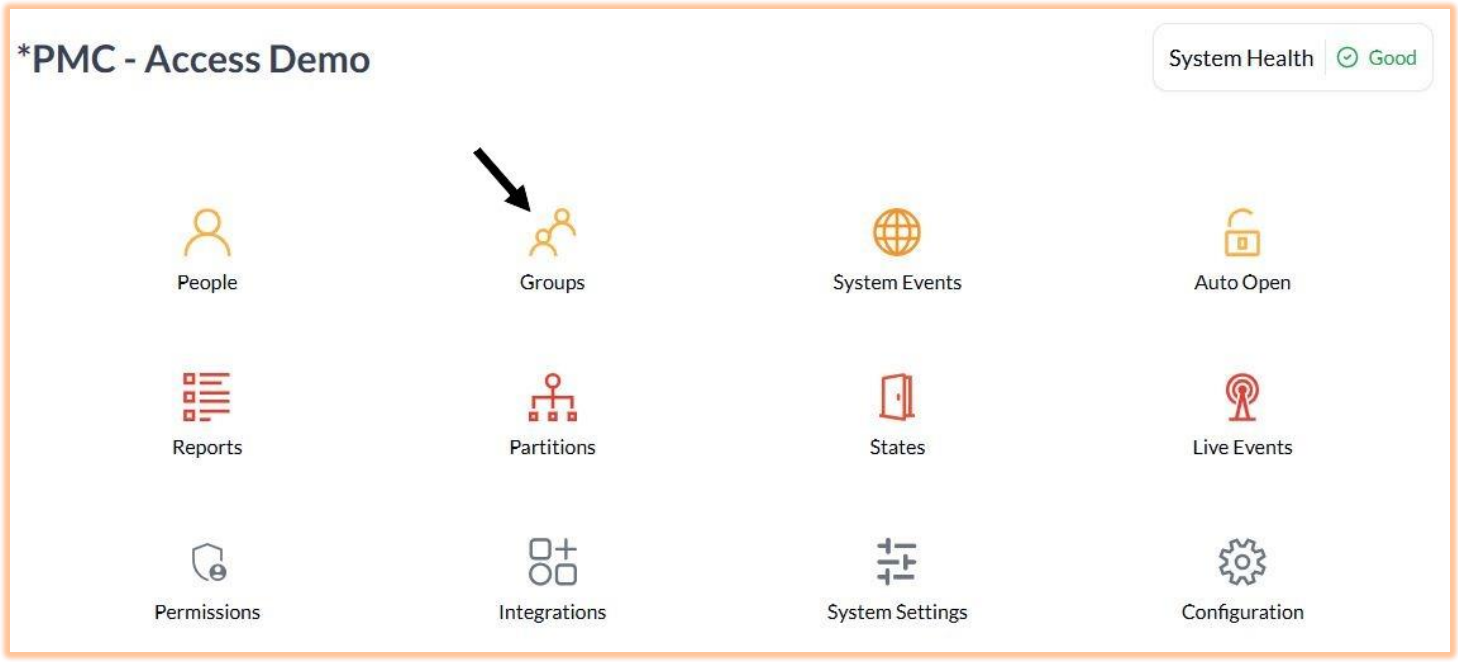
For additional support, please contact Per Mar Security at 800-473-7627 or email permarid@permarsecurity.com.

Table of Contents

A. Groups

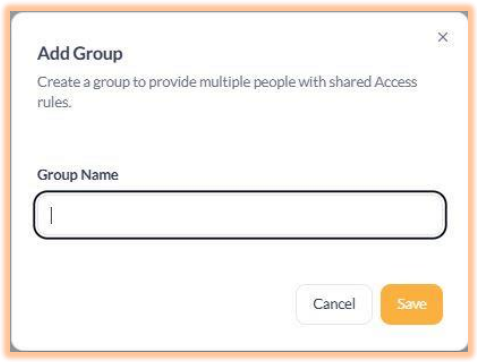
Groups allow you to assign shared access rules to multiple people, determining where and when access is allowed. This streamlines access control management by eliminating the need to create and manage individual access rules for each person. With groups, you can add, modify, or remove access rights for everyone in the group at once, making the process much faster and easier.

Click on **Groups** from the Customer Dashboard.

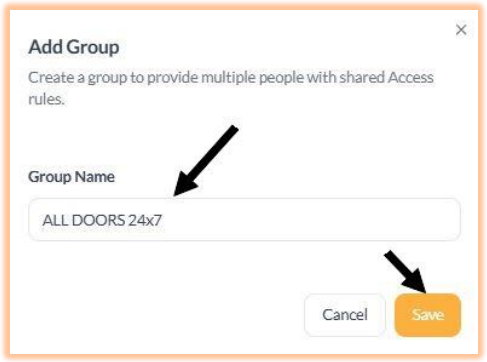


This will take you to the Groups page. To create a new Group, click on **+ Add Group**

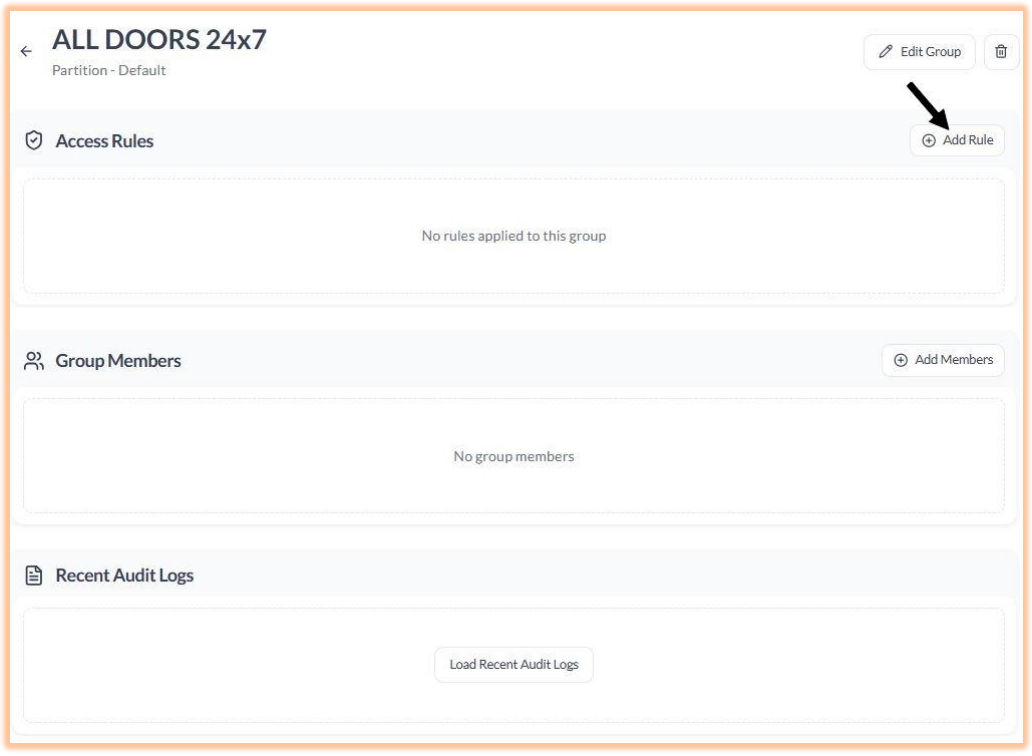
The Add Group window will pop out.



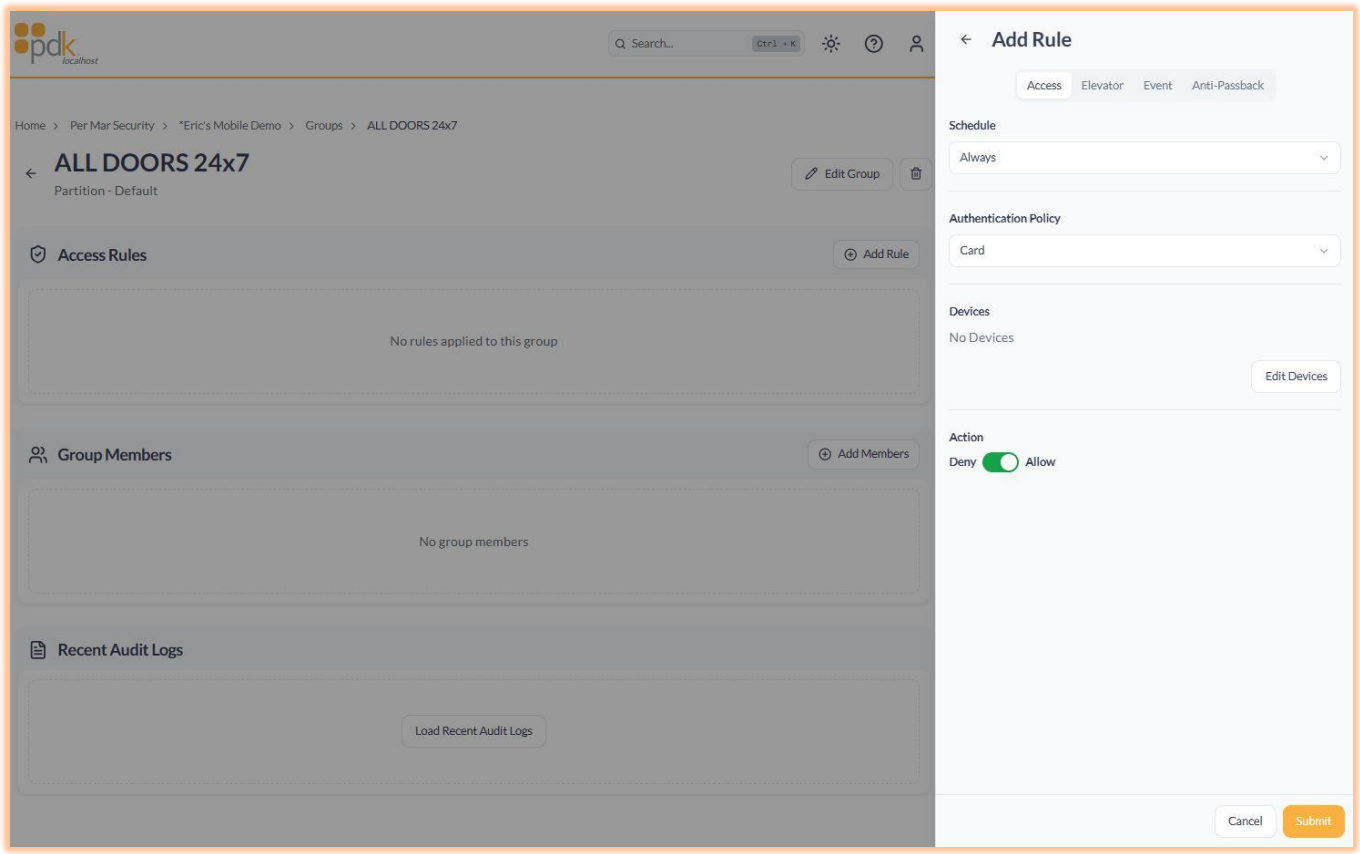
Typically, the first Group created should be ALL DOORS 24x7. It is best to name Groups with a description of how they function. In this case, ALL DOORS 24x7 will be a group that allows access to all doors at any time. (Later, we will create a group with limited access to certain doors on defined days of the week and times.) Enter ALL DOORS 24x7 in the Group Name and click **Save**



This will open the specific Group page. In Access Rules, click **+ Add Rule**



This will open a slide-out drawer to the right. Now we can define when (Schedule) and where (Devices) for the Group.

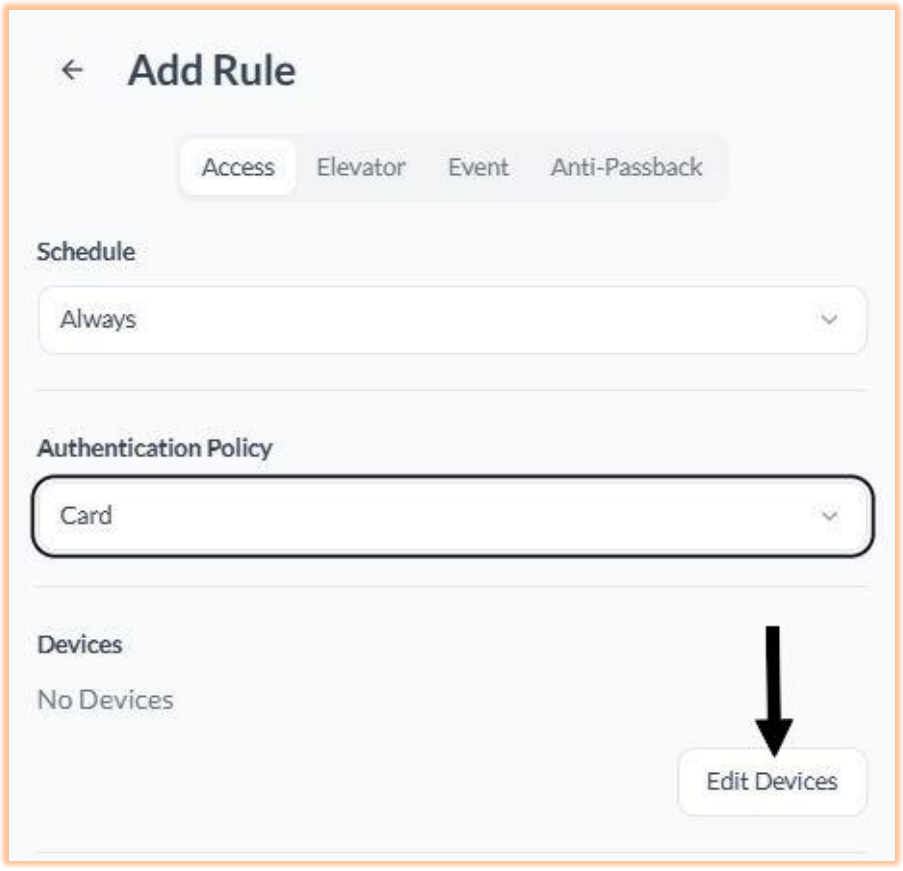


In the Schedule drop-down, there are three options: always, recurring, and single date.

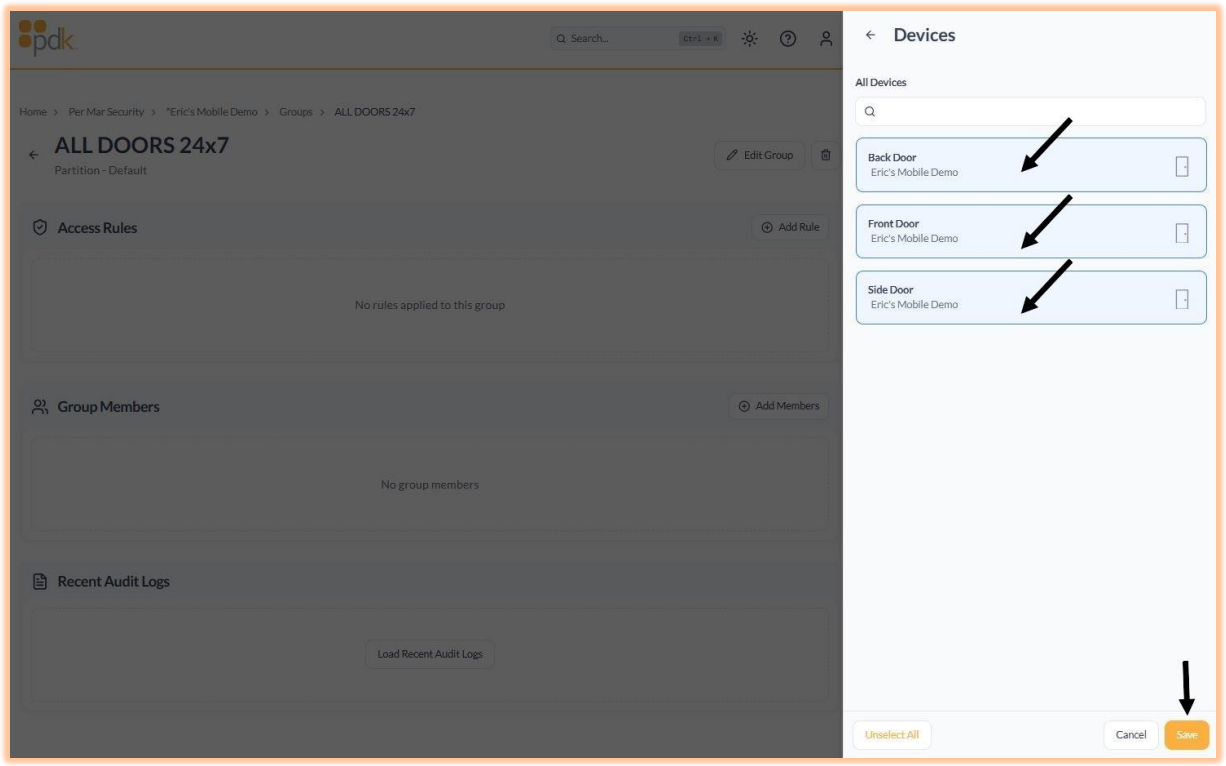
In this example, choose Always since we are creating a 24/7 Access Rule

Note: For most applications, leave the Authentication Policy to Card. Unless you have a Keypad Reader, the other options will not apply. If you do have Keypad Reader(s), speak to your installer about these options.

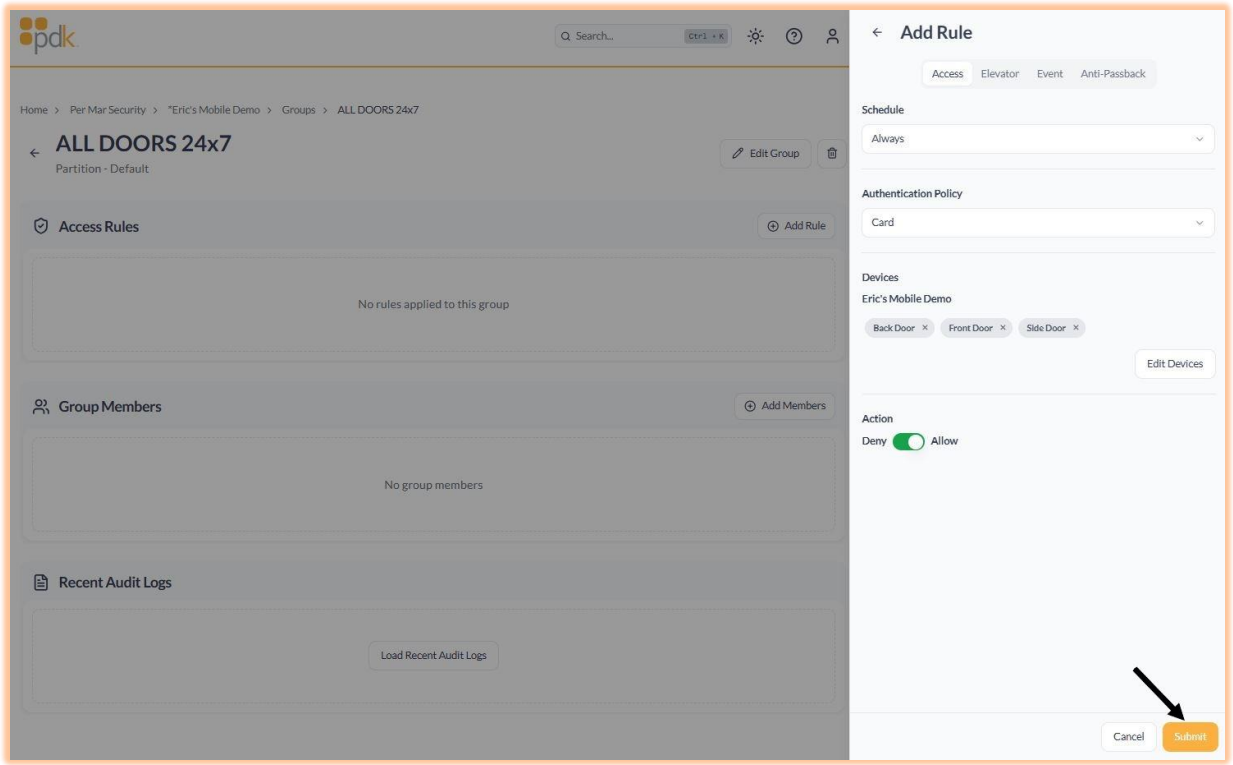
Devices click **Edit Devices**



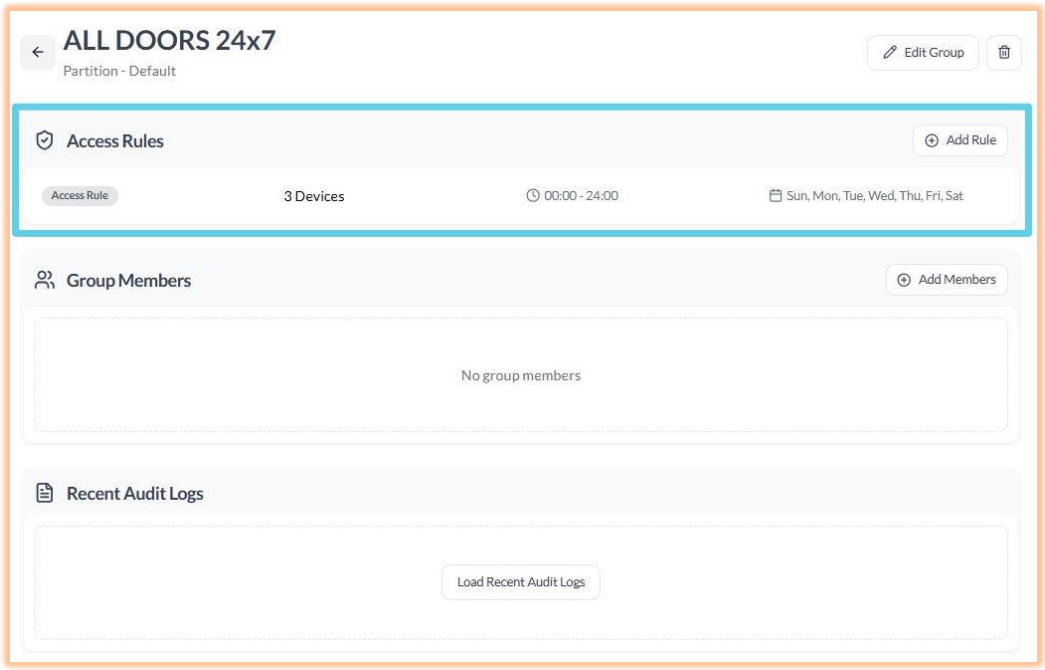
After clicking Edit Devices, a new slide-out drawer will pop over the existing drawer. Since this Group is All Doors 24/7, click on each door tile to select. Then, click **Save**.



After clicking **Save**, the Device slide-out drawer will disappear. The Add Rule slide-out drawer will show that the Schedule is Always, the Authentication Policy is Card, and Devices will be the four doors selected. (Note: Leave the Action toggle to Allow-green) You can now click **Submit** to save the Access Rule.



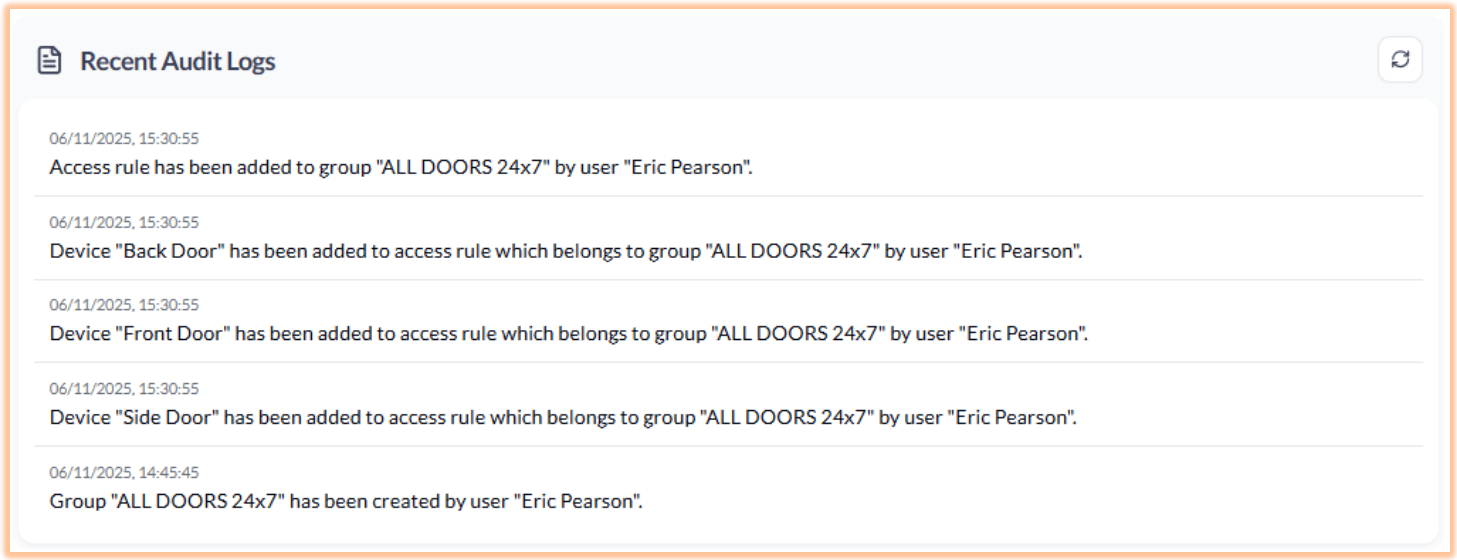
Now you will be back to the specific ALL DOORS 24x7 Group Page.



Access Rules will be populated with the rules created. In this case, the Access Rule has 4 Devices (the 4 Doors selected), and the times and days of the week access is allowed. Since Always was selected, the time is 00:00 – 24:00, and the days of the week are Sun, Mon, Tue, Wed, Thu, Fri, Sat.

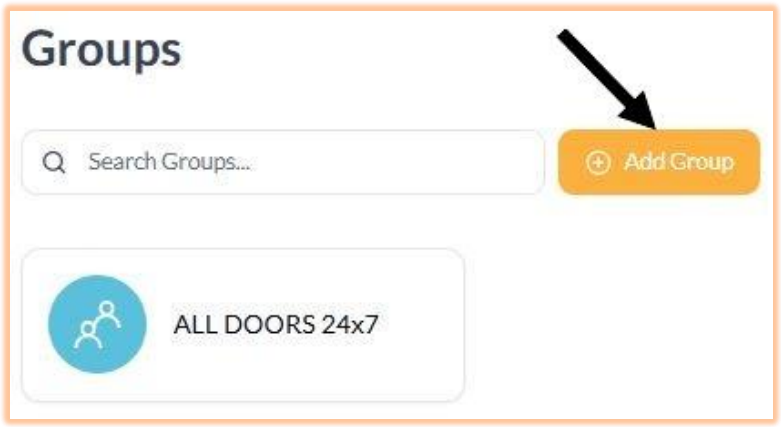
Group Members are empty since no People have been added. If People have been created, you may add People by clicking **+ Add Members** and selecting the People you want to add to this Group. If no persons have been created yet, refer to Add People for instructions. Inside People, you assign any Group or Groups to a person, as well as assigning a Group here.

Recent Audit Logs: Clicking on **Load Recent Audit Logs** will show all the recent changes made to the Group.

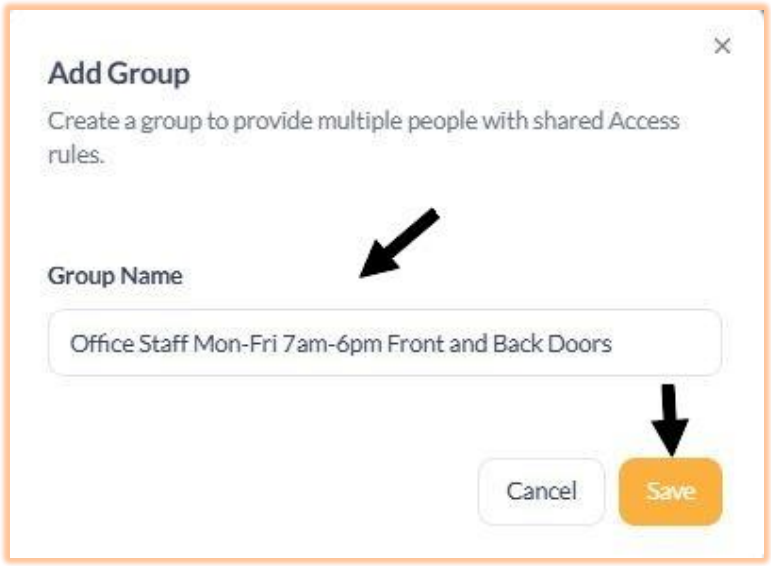


Now let's create a Group with limited door access. In this scenario, we need to limit door access for the office staff to Monday through Friday, 7:00 AM to 6:00 PM, by the Front and Back doors only.

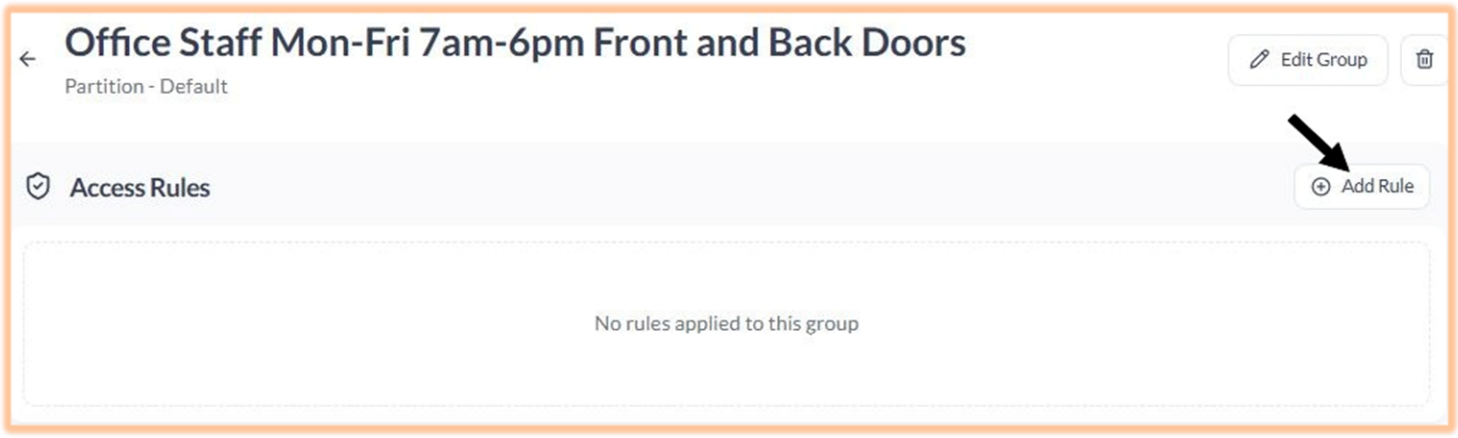
On the Groups page, click **+Add Group**. Notice the ALL DOORS 24x7 Group we created earlier is there.



Enter Group Name: Office Staff Mon-Fri 7am-6pm Front and Back Doors and click **Save**.



This will open the specific Group page. In Access Rules, click **+ Add Rule**



In this Example:

Schedule Select Recurring from the dropdown

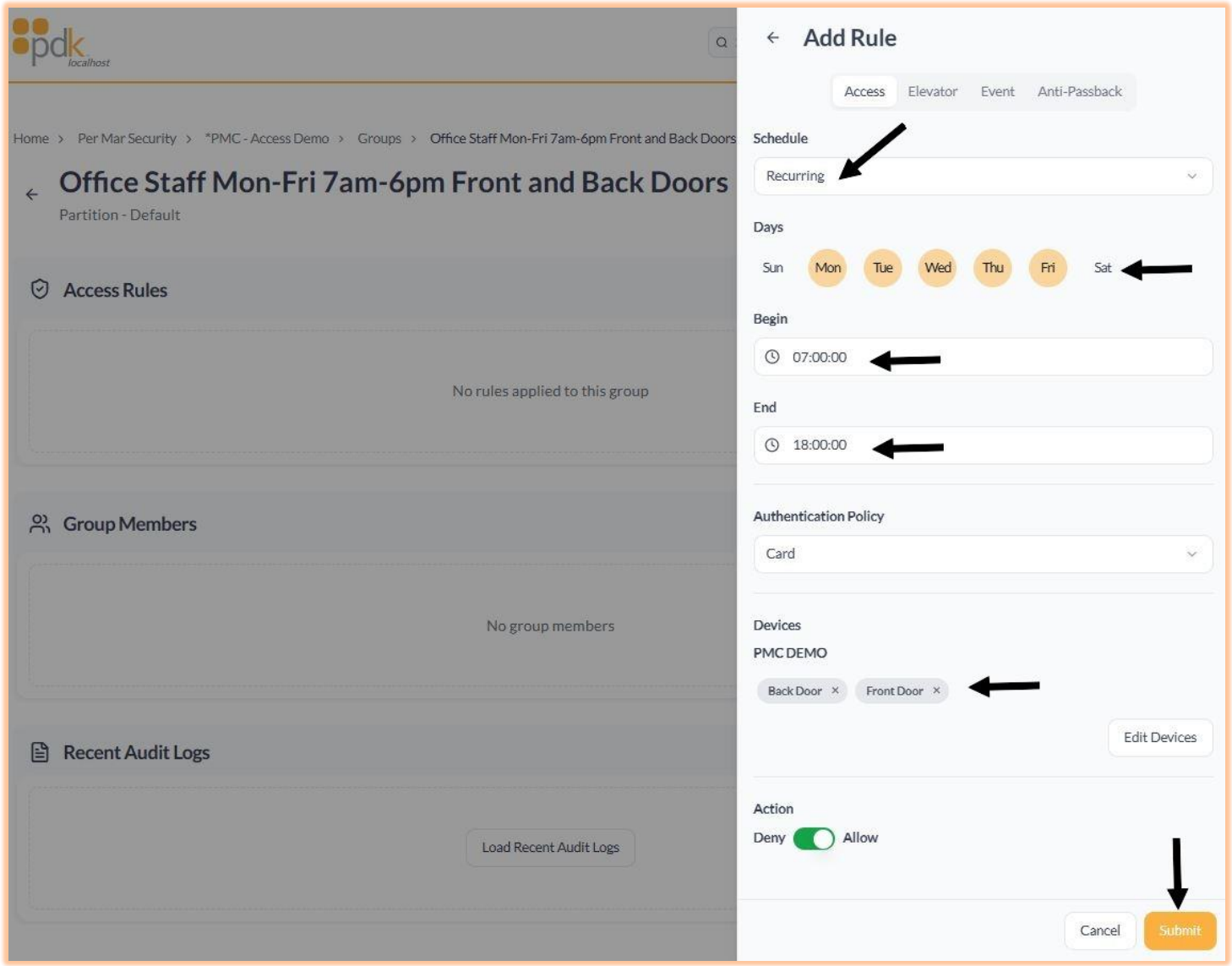
Days Select Mon Tue Wed Thu Fri

Begin 07:00:00 (must be in Military Time)

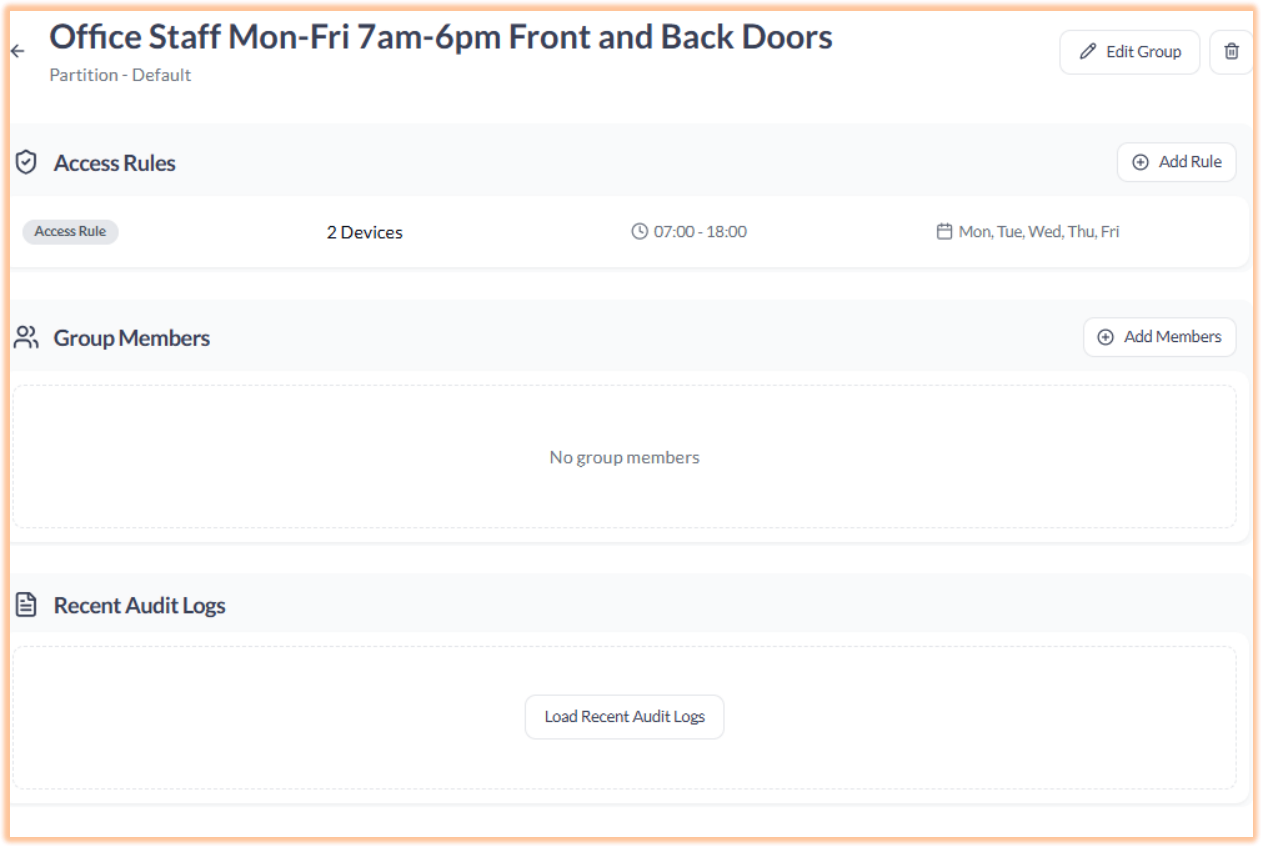
End 18:00:00 (must be in Military Time)

Devices Back Door Front Door

Click **Submit**



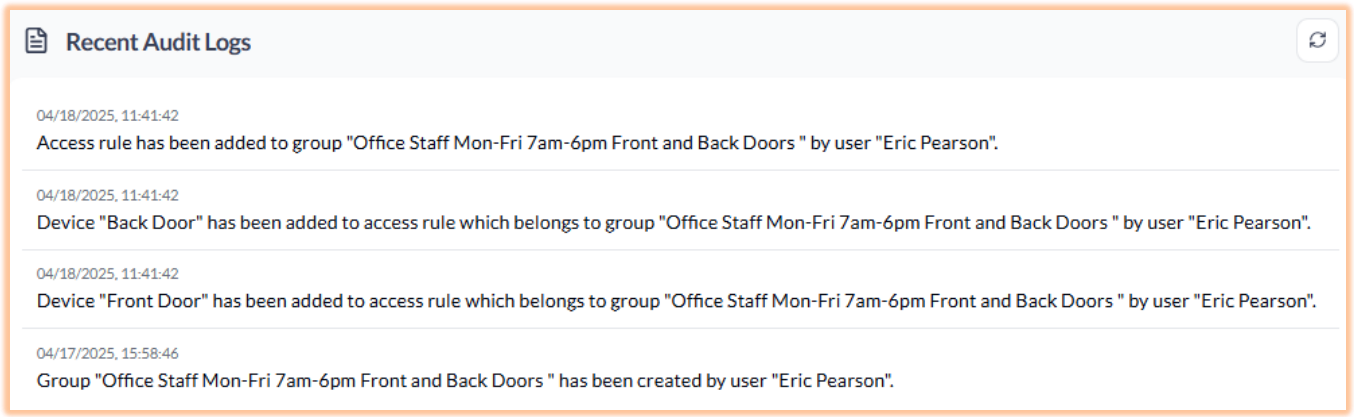
Now you will be back to the specific Office Staff Mon-Fri 7am-6pm Front and Back Doors Group Page.



Access Rules will be populated with the rules created. In this case, the Access Rule has 2 Devices (Front Door, Back Door), and the times and days of the week when access is allowed. Since Recurring was selected and day of the week and time entered, it is 07:00 -18:00 Mon, Tue, Wed, Thu, Fri.

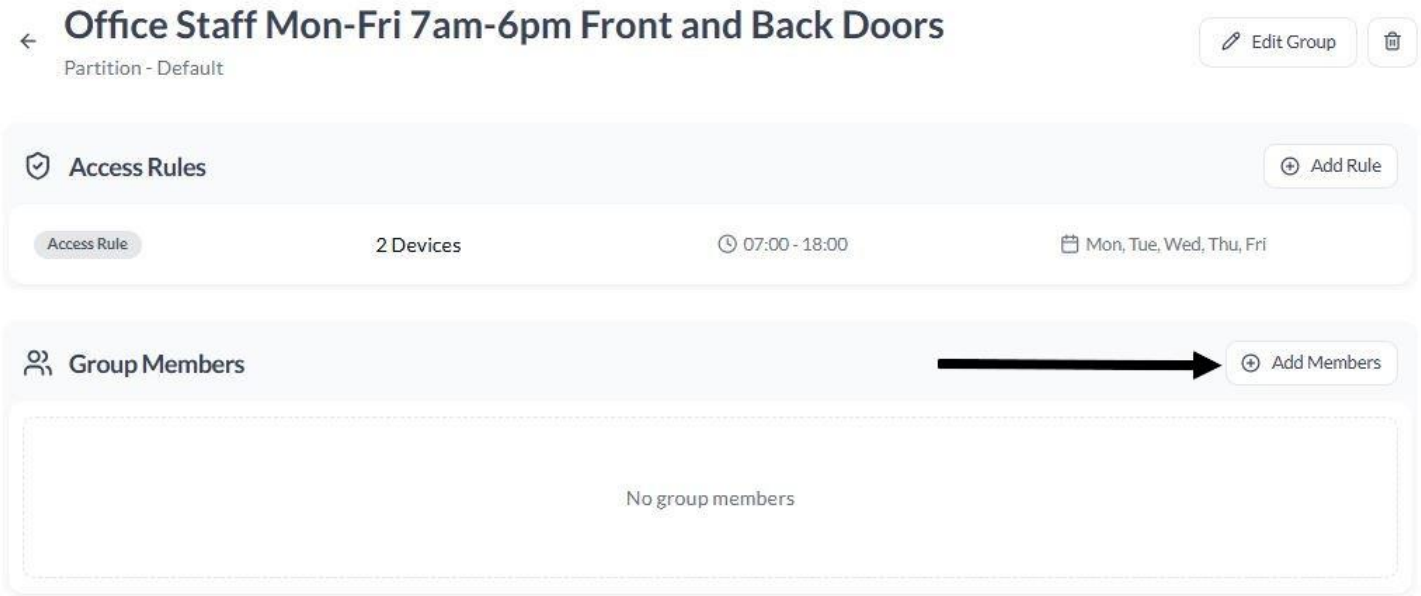
Group Members are empty since no People have been added. If People have been created, you may add People by clicking **+ Add Members** and selecting the People you want to add to this Group. If no persons have been created yet, refer to Add People for instructions. Inside People, you assign any Group or Groups to a person, as well as assigning a Group here.

Recent Audit Logs: Clicking on **Load Recent Audit Logs** will show all the recent changes made to the Group.

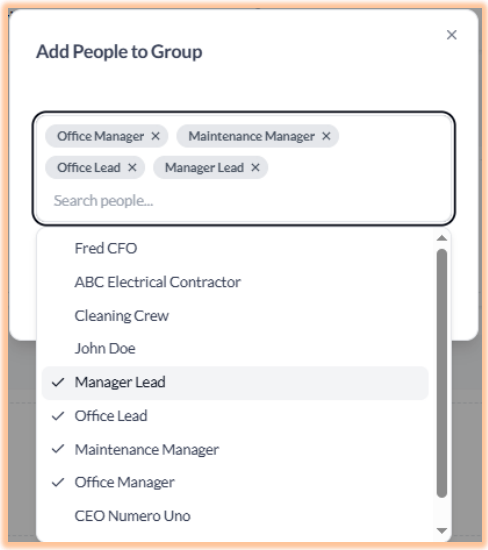


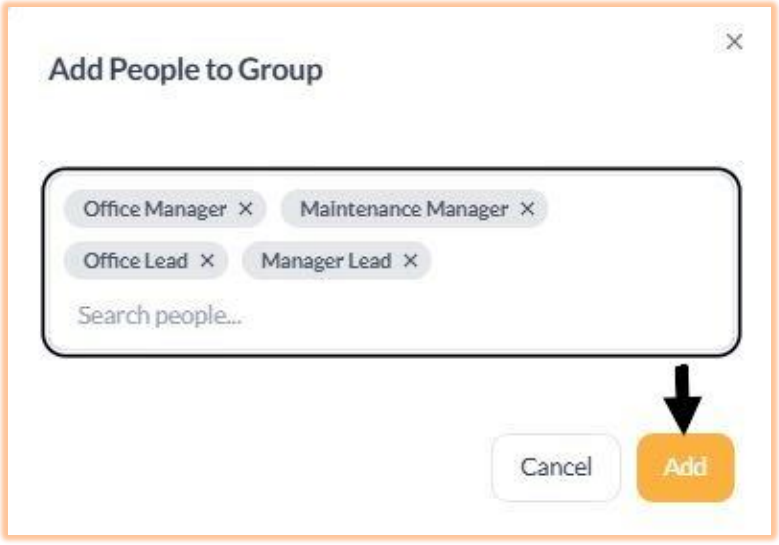
Assigning a Group to a Person

There are two methods to assign a Group to a person. If the person or people are already created, you can add a person or multiple people to a Group within the Group page. Go to a Group that has already been created. Go to Group Members and click + **Add Members**

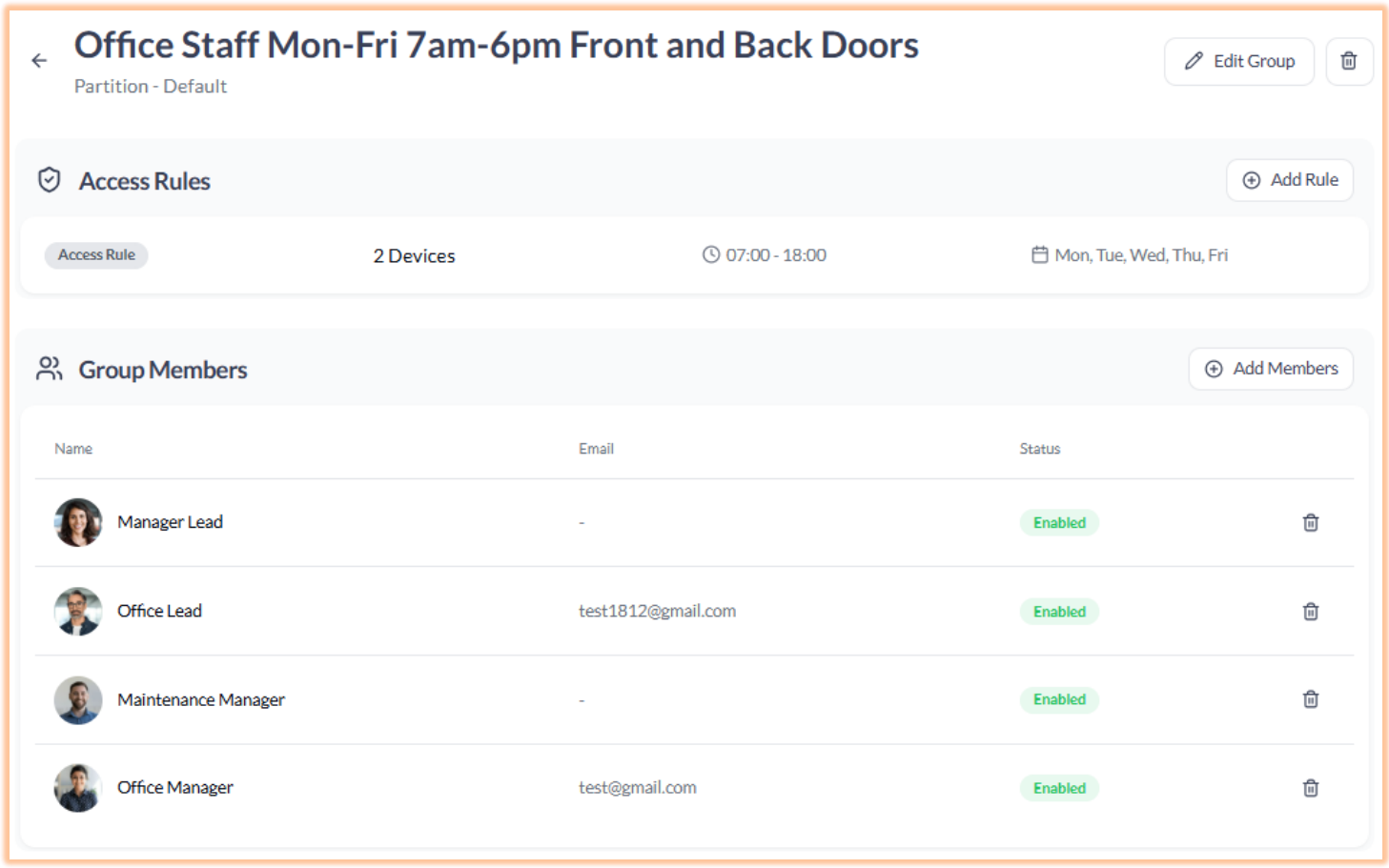


A new pop-up window will appear where you can select the People to add to the group. Click the people to select them. (Note, you may need to hit the Esc button on your keyboard after selecting to see the add button) Click **Add**



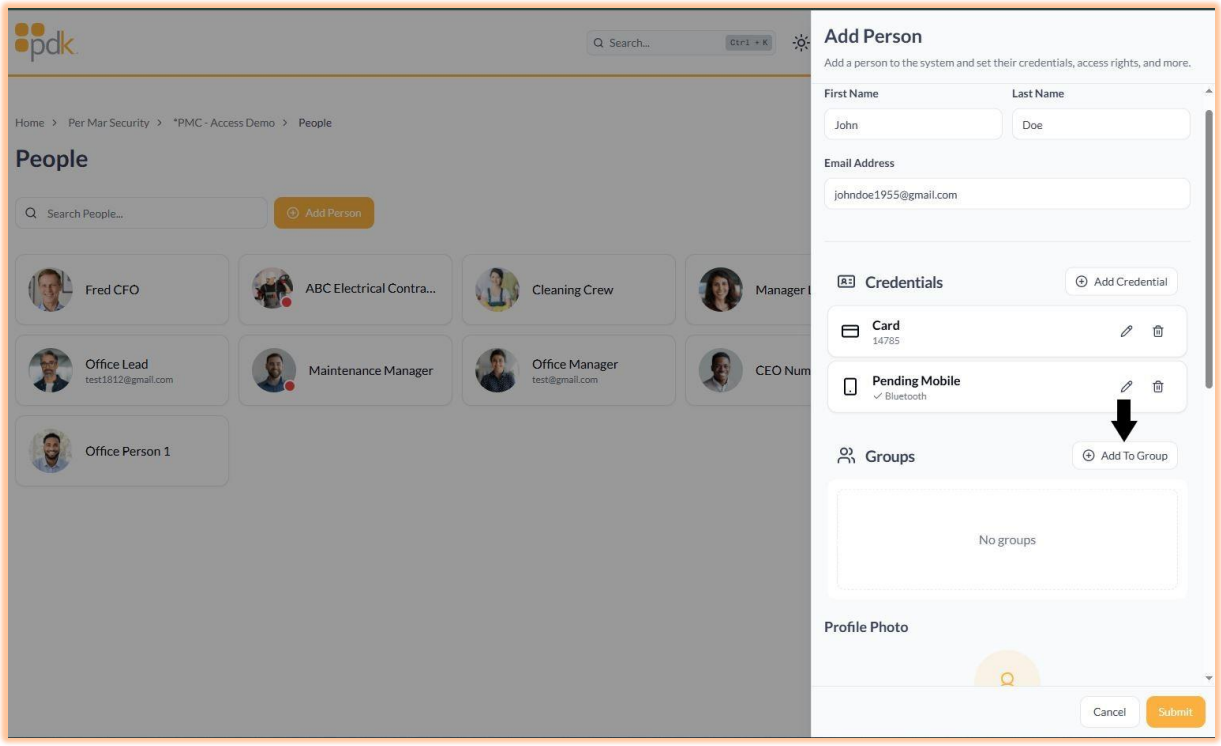


Now you will see these people under Group Members

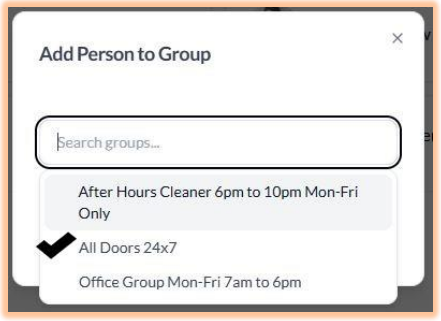


The other method to add a Group to a person is covered in more detail in the People section. Here is a brief overview.

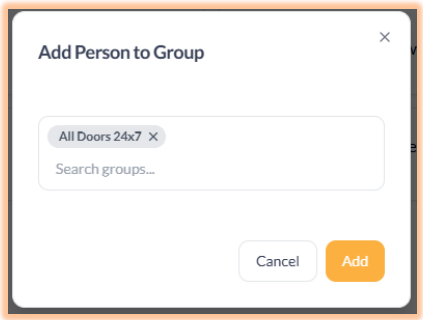
To assign the person to a Group. Click on **+ Add To Group**



A new pop-up window will appear. Select the Group or Groups you want to assign to this person.

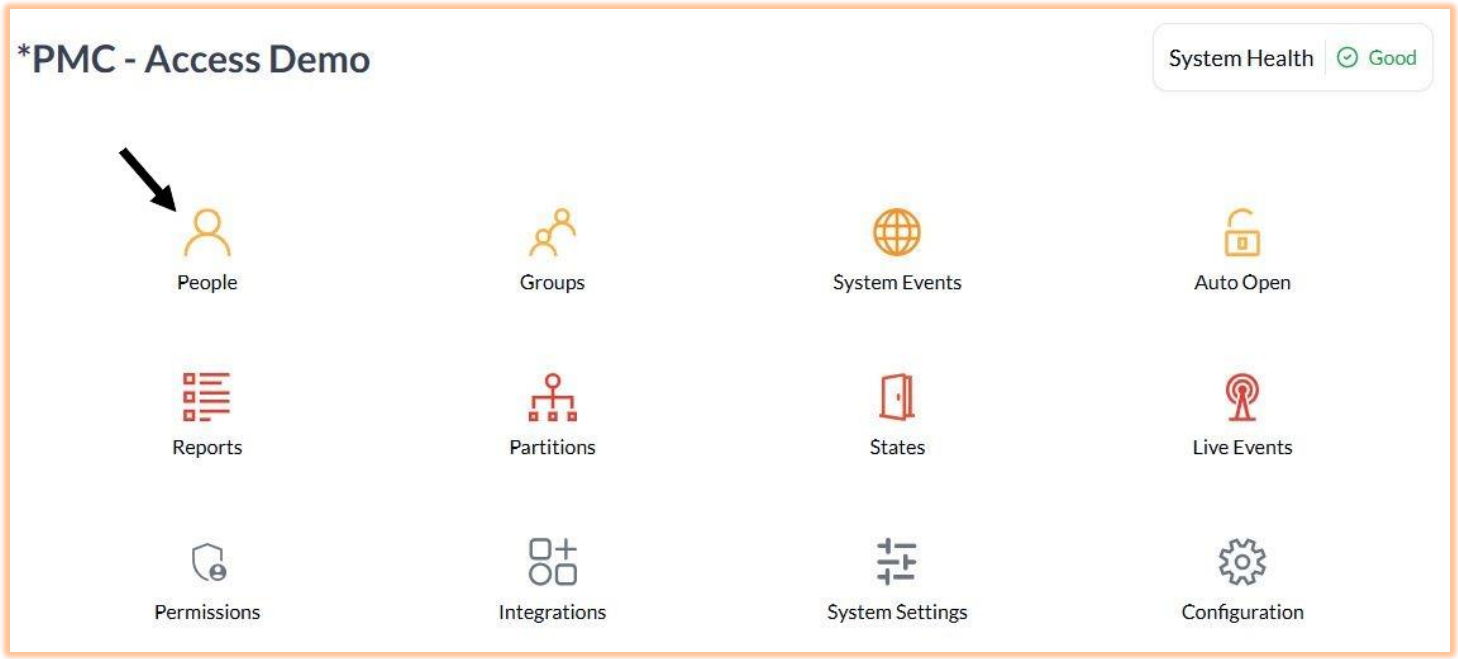


Click **Add** (Note, you may need to hit the Esc button on your keyboard after selecting the Group to see the add button)

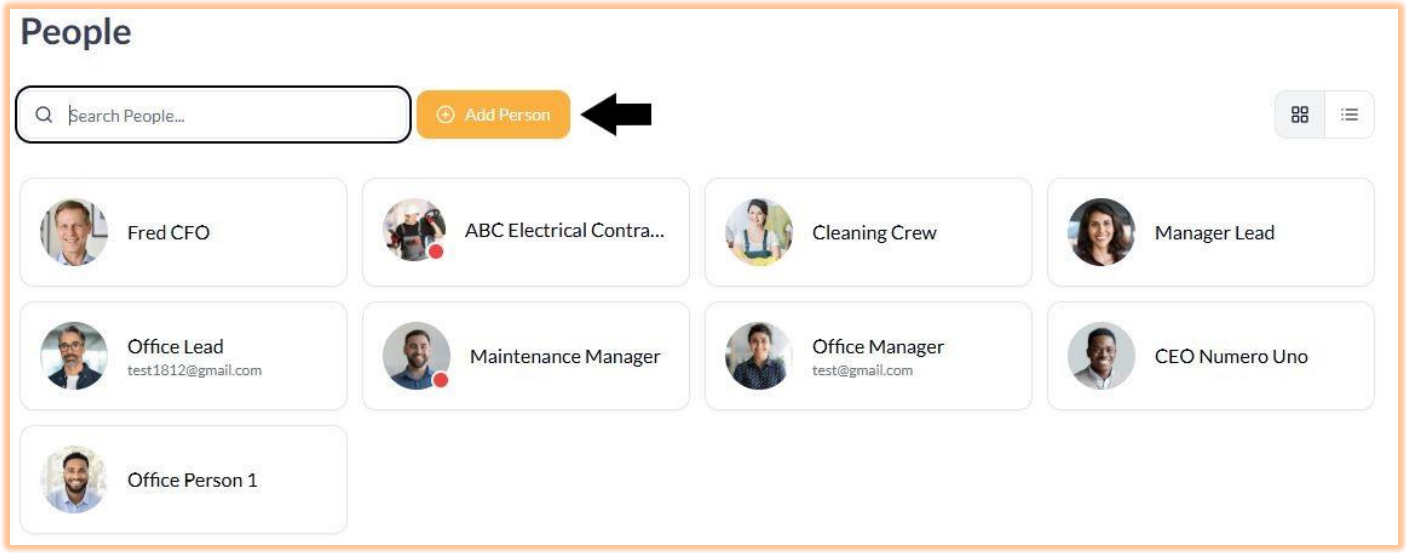


B. People

From the Customer Dashboard, click on **People**.



Click **Add Person**

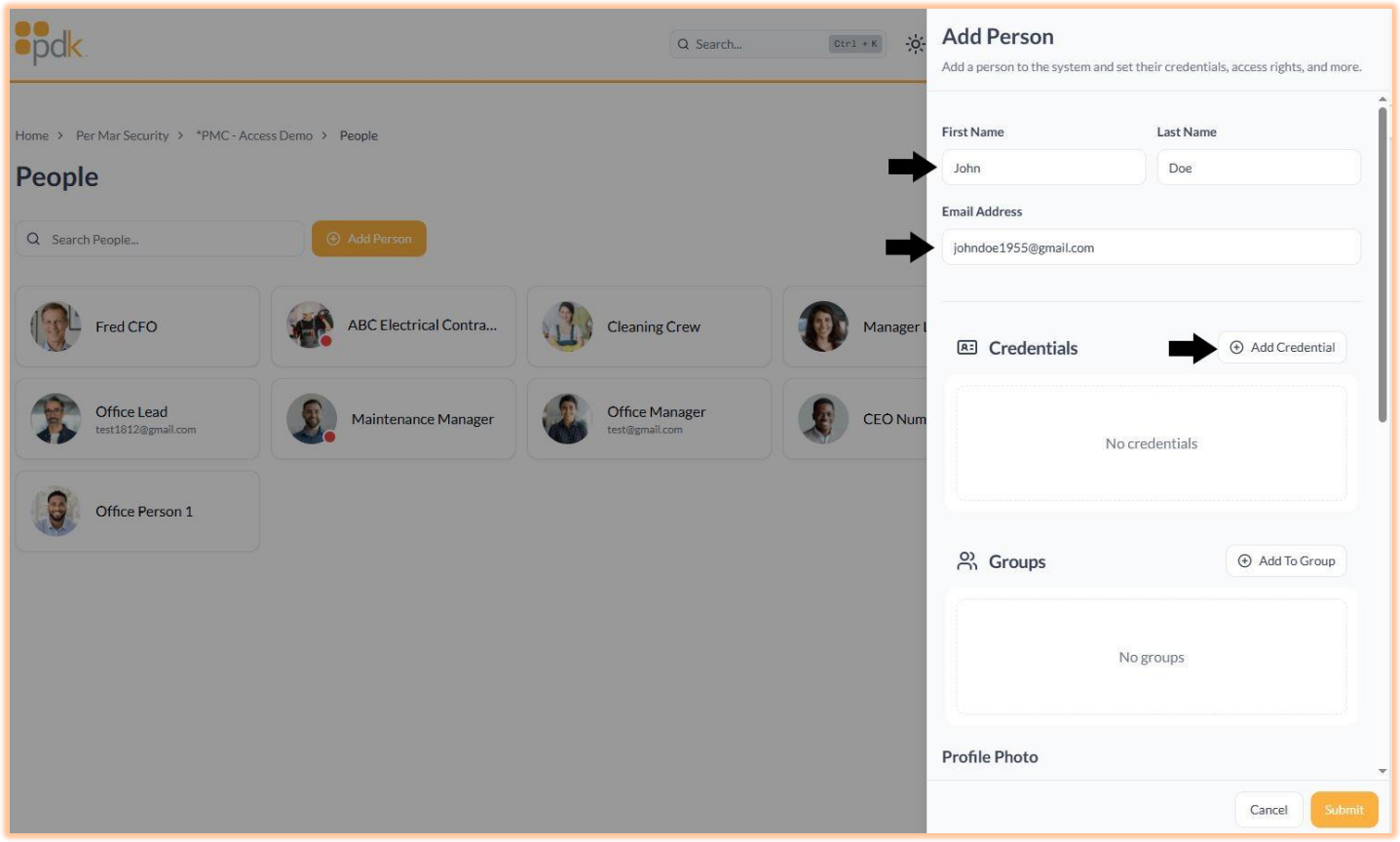


A slide-out drawer will appear to the right.

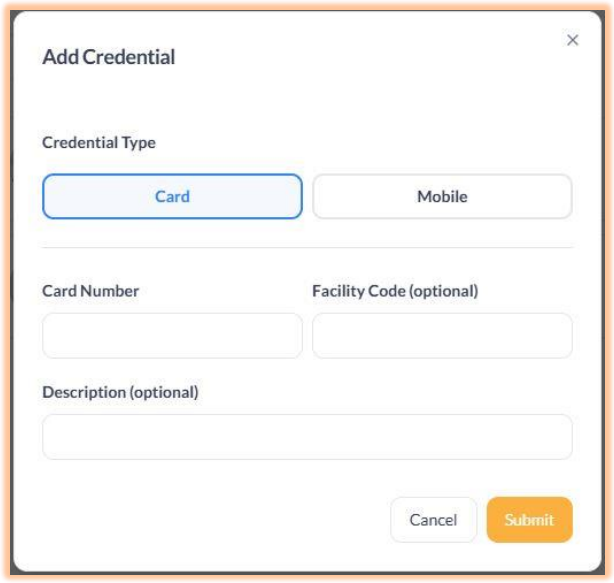
Type in the First and Last Name

If the person will be assigned Bluetooth or Mobile App Credentials, enter the person's email address

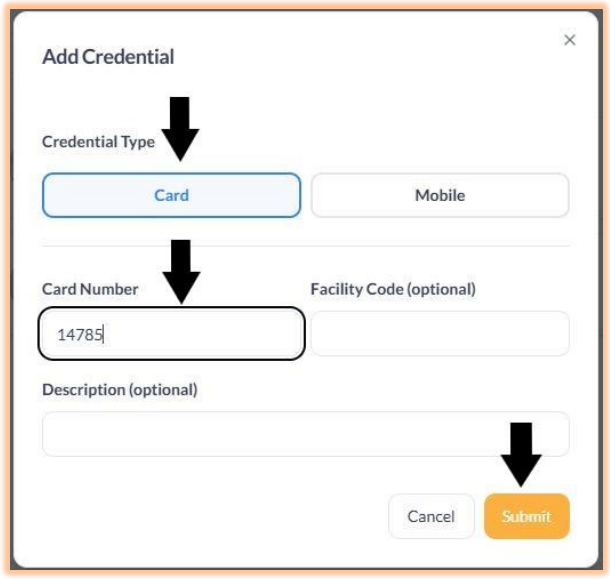
Click **+Add Credential**



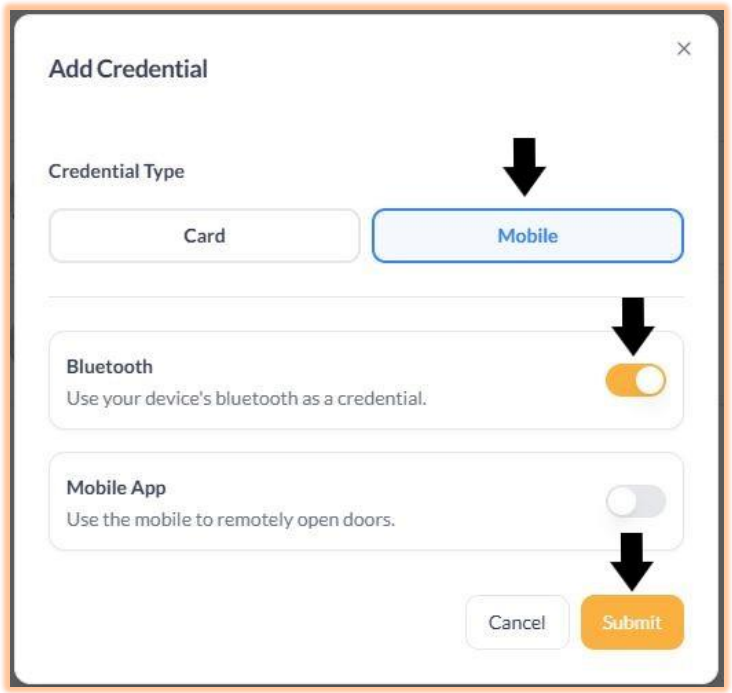
After you click on **+ Add Credential**, a new window will pop up.



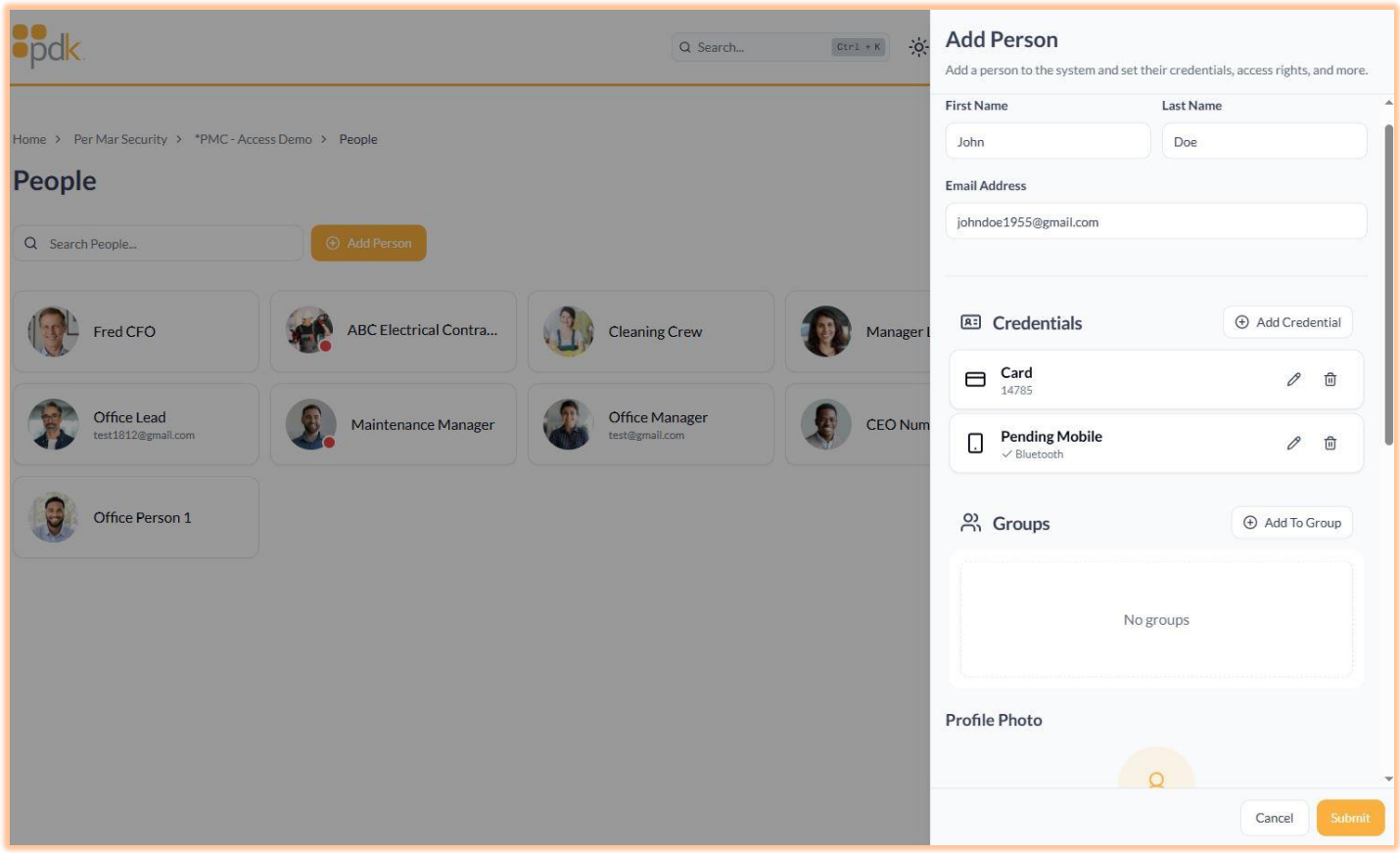
For a Card Credential, select Card and enter the card number. The fields for Facility Code and Description are optional. You may leave those as blanks. Click **Submit**.



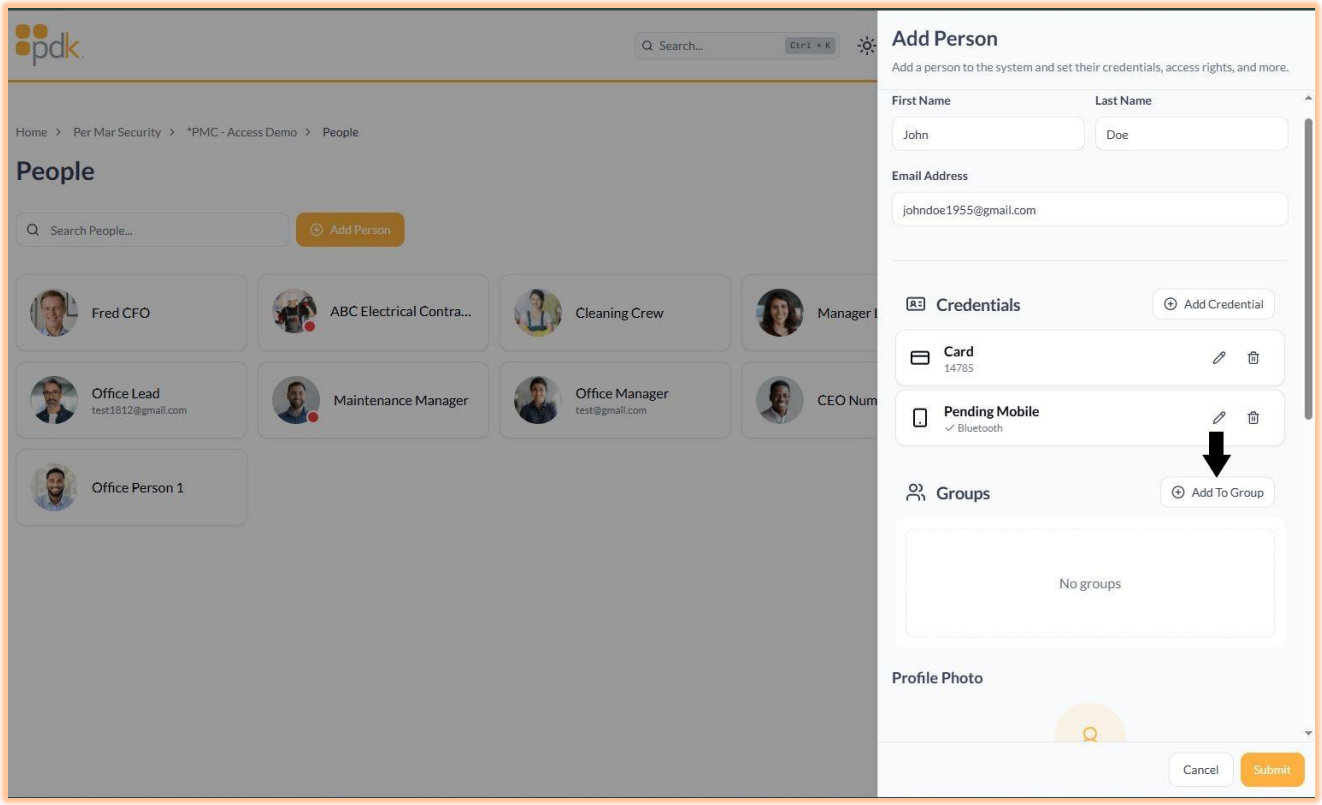
For a Bluetooth Credential, select Mobile and select Bluetooth. Click **Submit**. The Mobile App option is designed primarily for management personnel who need to unlock doors remotely using their phone. This feature is not typically used by the average user. Most users will rely on Bluetooth Credentials on their phone, which functions like an access card. They simply present their phone to the reader to unlock the door. In contrast, the Mobile App option allows authorized users to unlock doors while not on site.



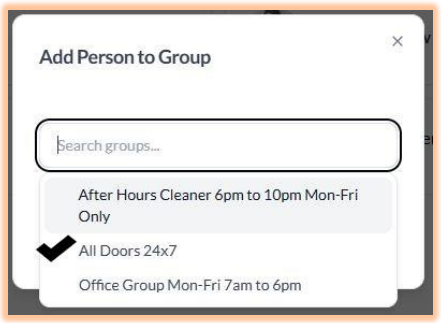
After clicking submit, you will be back in the slide-out drawer. Notice in this case, the person has both a card credential and a Bluetooth credential. If you need to edit either, click the small pencil icon. If you want to delete a credential, click the trash can icon. N*otice the Bluetooth Credential shows Pending Mobile. When a Bluetooth Credential is added to a person, the system automatically generates an activation email to the person's email address you entered above. The person has 72 hours from the time of the email to activate. The email contains instructions for downloading the PDK app and activating the phone as a Bluetooth Credential. If the person does not activate within 72 hours, the activation email will need to be resent.* See Resend Bluetooth Activation Email in the additional person options section.



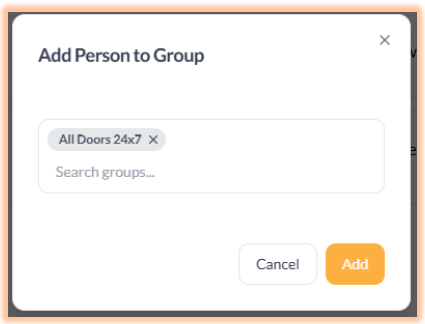
Now we have to assign the person to a Group. Click on **+ Add To Group** The Group determines which doors and at what times a person has access. Group configuration will be covered in the Group section.



A new pop-up window will appear. Select the Group or Groups you want to assign to this person.

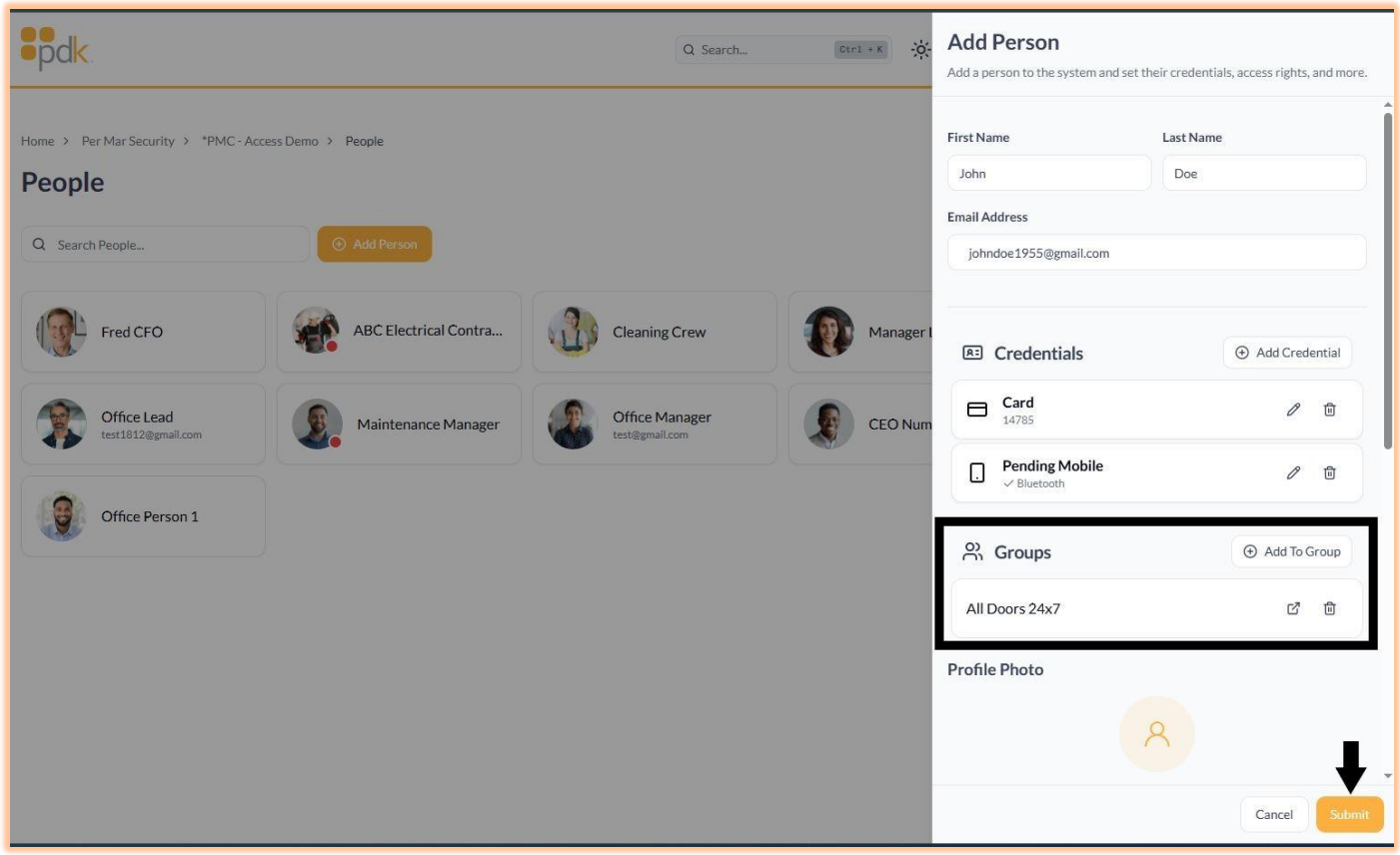


Click **Add** (Note, you may need to hit the Esc button on your keyboard after selecting the Group to see the add button)

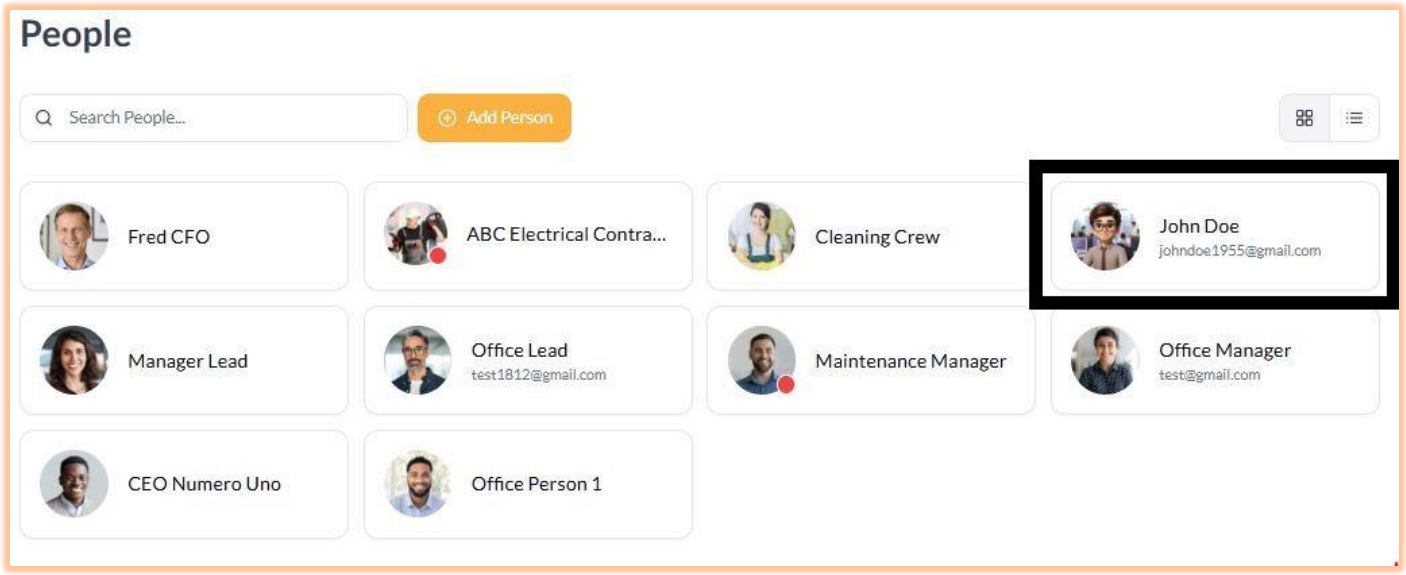


After clicking add, the slide-out drawer will show the Group or Groups assigned. If you need to make changes, click the pop-out icon (box with arrow). You can delete a Group by clicking the trash can icon.

At this point, you can click **Submit** to save and add the person. Additional person options will be covered in the next section.



After clicking Submit, the slide-out drawer will disappear, and you will be back at the People page. The new person added will be visible.



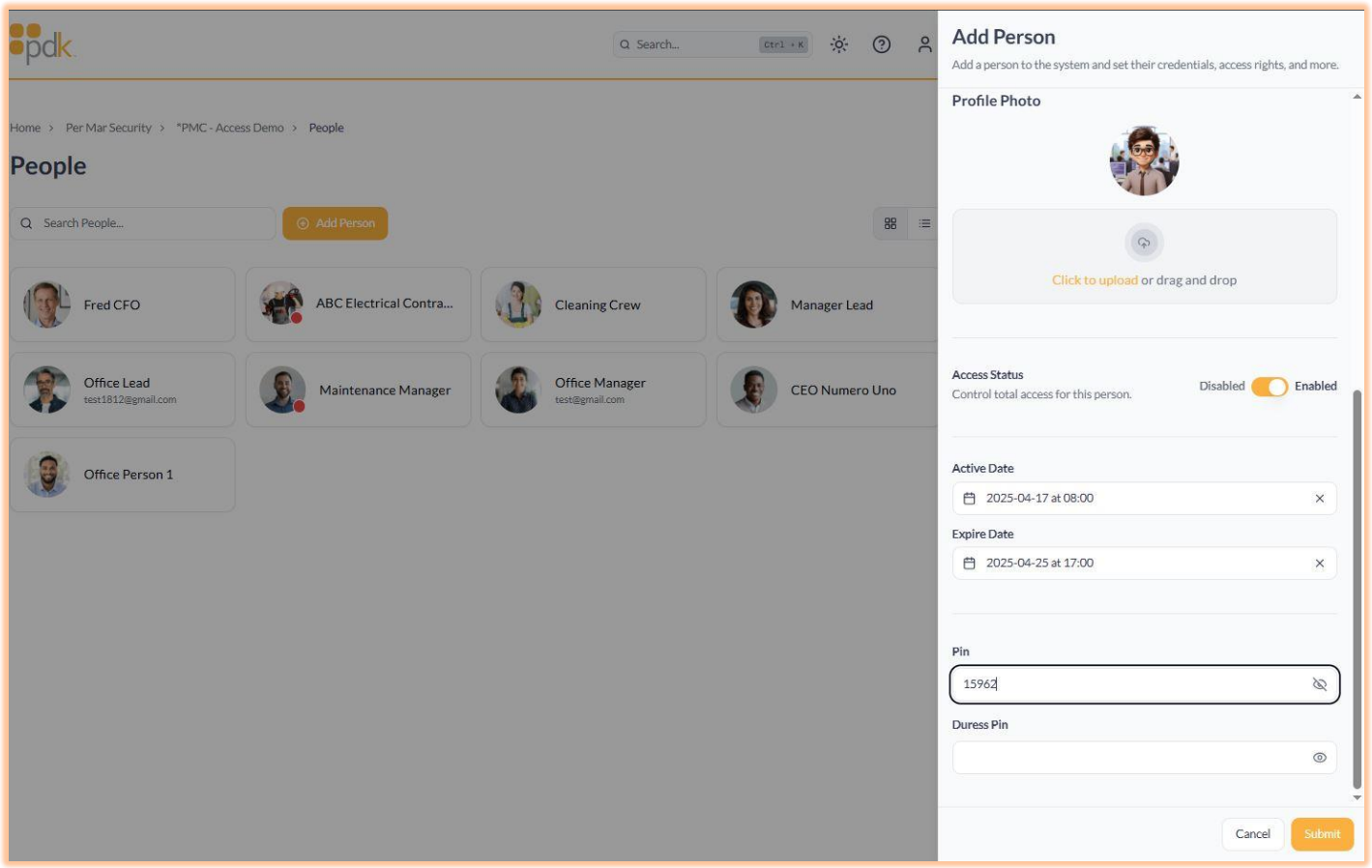
Additional person options

Profile Photo: If desired, you may add a profile photo

Access Status is Disabled or Enabled: The default is Enabled. There are a few reasons you may want to set this to Disabled. If a person loses their card, you may set this to Disabled to prevent the lost card from being used. If the person later finds their card, you can easily set it back to Enable. If a person leaves your organization, but you do not get their card credential back, you can set it to Disabled. Now, if that person tries to use the card, it will not unlock any doors, but PDK will show in reporting that person tried to use the card after it was Disabled.

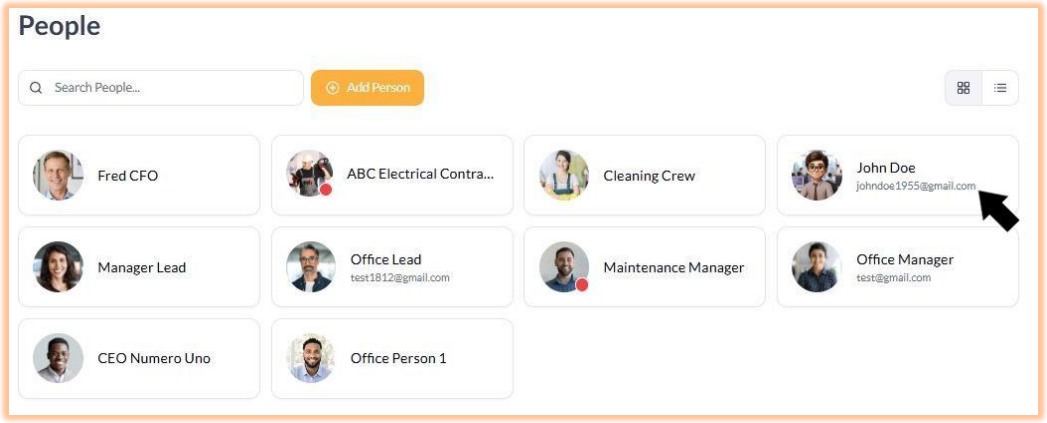
Active Date and Expire Date: Usually, these can be left blank. However, these are useful if the person needs temporary access, such as an outside contractor or a temporary employee. The date and time can be set for when the person's access starts and ends. Note, at the end of the Expiration Date, the person will not be automatically deleted. Their credentials simply will not work. If the person tries to gain access outside the date and time, PDK will show that the person tried to use their credentials to gain access, but access was denied.

PIN and Duress PIN: PIN is only for use on access systems with readers that have a keypad. Please talk with your installer about these options if you have keypad readers.



Edit or Delete Person

Once a person has been added, you may edit or delete that person by clicking the person's tile.



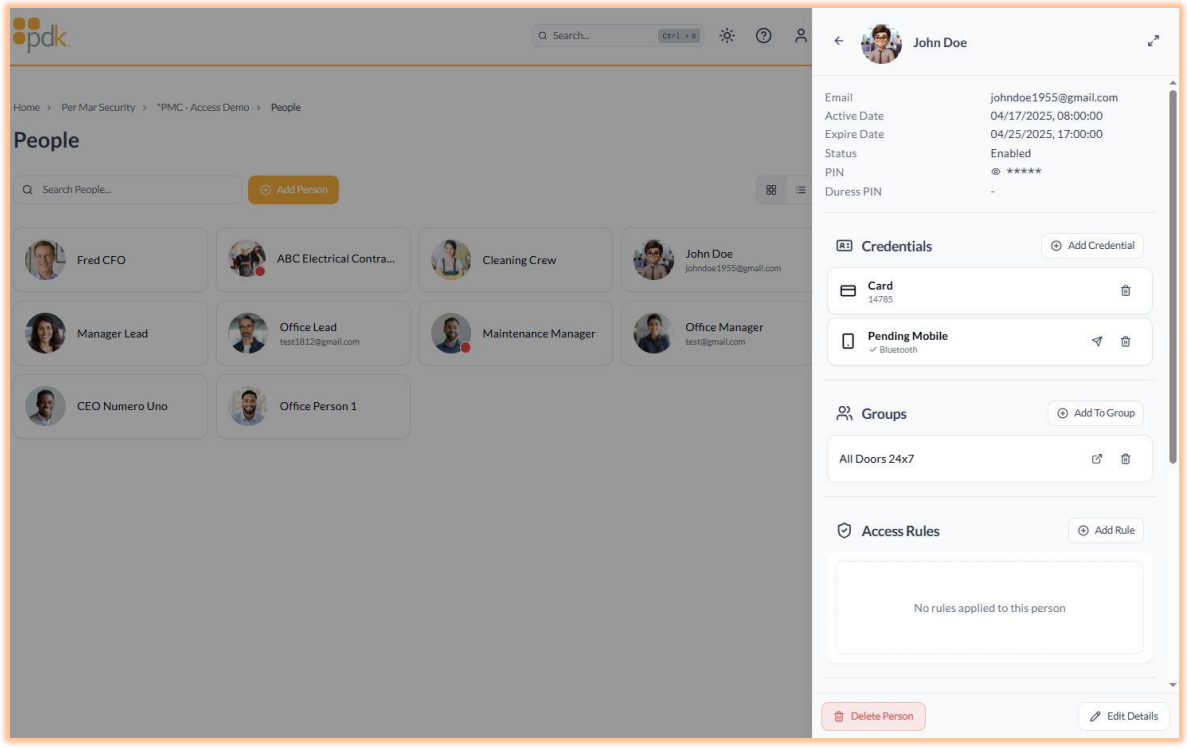
A slide-out drawer will appear to the right. There you can edit or delete the person.

Edit Details: Clicking here will take you to another page where you can edit their name, email address, profile photo, access status, active date, expire date, and PIN code.

Delete Person: Clicking here will pop out another window asking if you are sure you want to delete.

Access Rules: Are special rules that only apply to a particular person and are not part of the rules in Groups. Typically, this is blank. Please check with your installer if you need to assign a special rule for a particular person.

Resend Bluetooth Activation Email: Under Credentials, if there is a Pending Mobile, you may click the paper airplane icon to resend the Bluetooth Activation Email.



C. Permissions

Permissions within PDK.io specify which functionalities are available to a user on the Dealer or Customer Account level. Each Permission role (Admin, Manager, or Reporter) specifies what PDK.io features are available. A Permission granted at the Dealer level provides a Permission level to all Customer Accounts for the Dealer. A Permission granted within the Customer Account (from the Customer Dashboard) will provide those functionalities for just that Customer Account. Persons with Integrator or Admin Permissions can add Permissions, at their Permission level or lower, to other persons.

Function availability by Permission

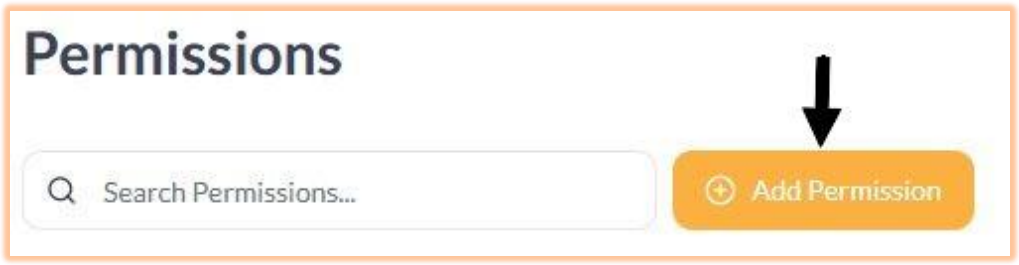
Each Permission level defines which functions from the Customer Dashboard are available for the Person. Each Permission, from Integrator to Reporter, is more limited in scope compared to the previous Permission level.

- Admin - This Permission allows you to access and manage all functions of a Customer Account except Configuration. An Admin can also issue Admin or lower Permissions to others.
- Manager—This Permission allows managers to access the following items in a Partition they are assigned to people, Groups, Auto-Open, Reports, System Events, and States, in addition to viewing Live Events. Managers can only add, edit, or delete items in their assigned Partition.
- Reporter - This Permission can only access Reports and Live Events.

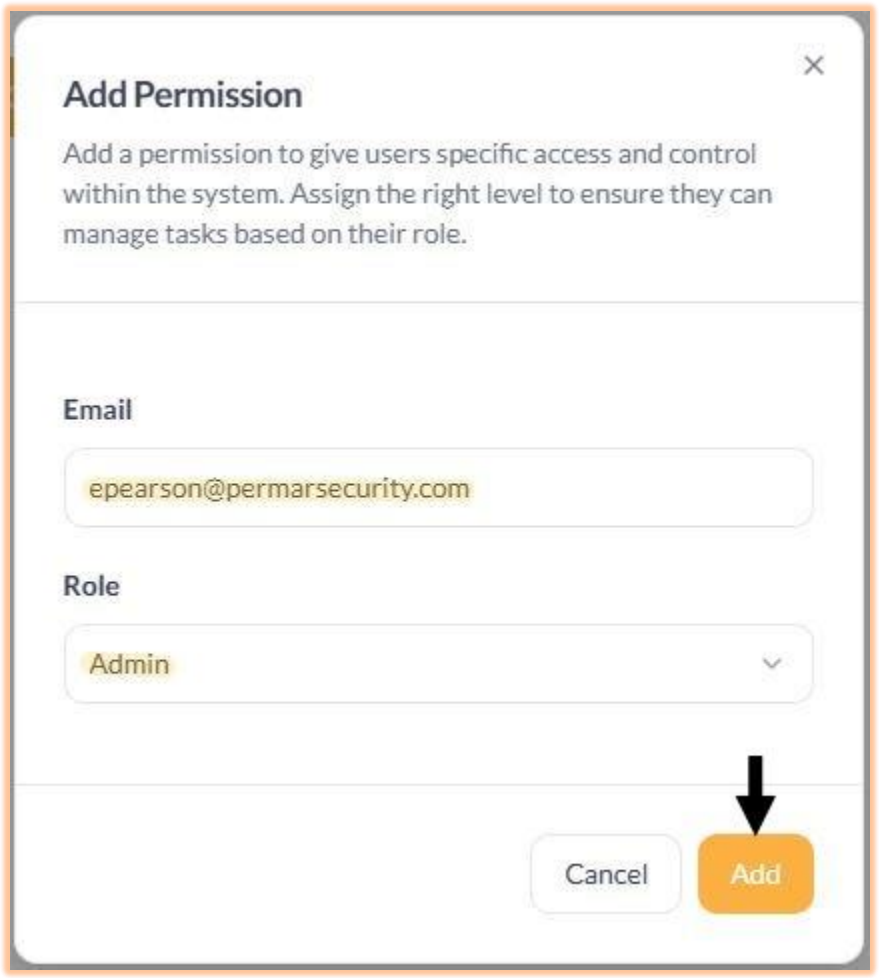
Adding a Permission to a Customer Account

From the Customer Dashboard, click **Permissions.**

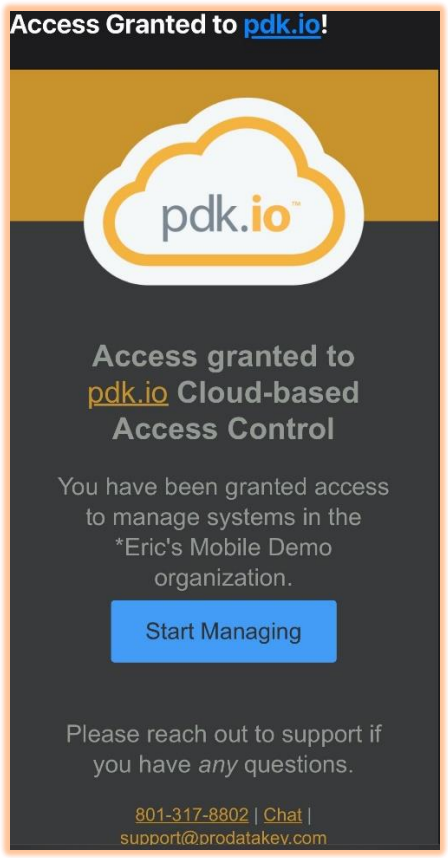
On the Permission page, click **+ Add Permission**



A new window will appear. Enter the email address of the person you are adding and select their permission level from the Role dropdown. Click **Add.**

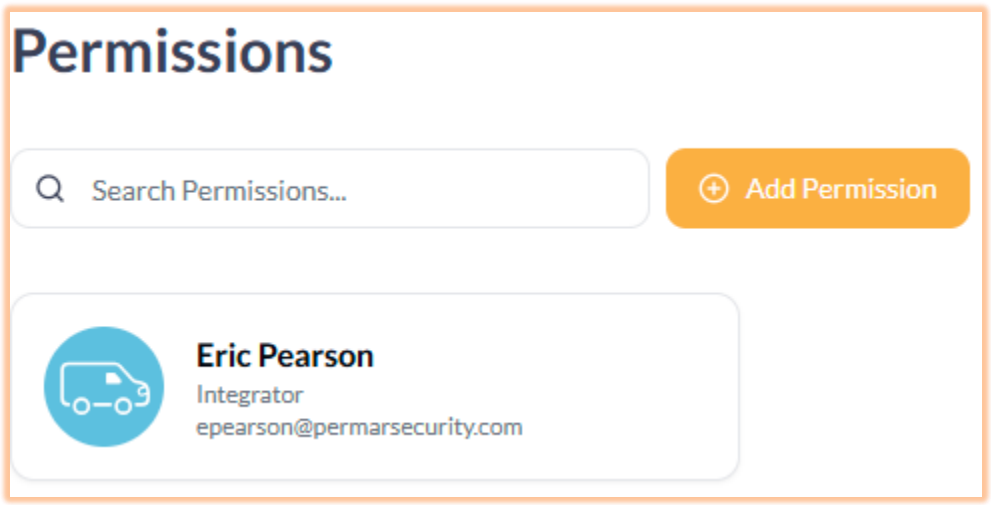


The person will receive an email from ProDataKey Cloud Systems. It will look like this.



From the email, they will be directed to complete their permission account by entering their name, phone number, company name, and title. Note: Until the Permission has been activated by the person, the person will be displayed as (Invitation Pending) in Permissions, rather than the person's name.

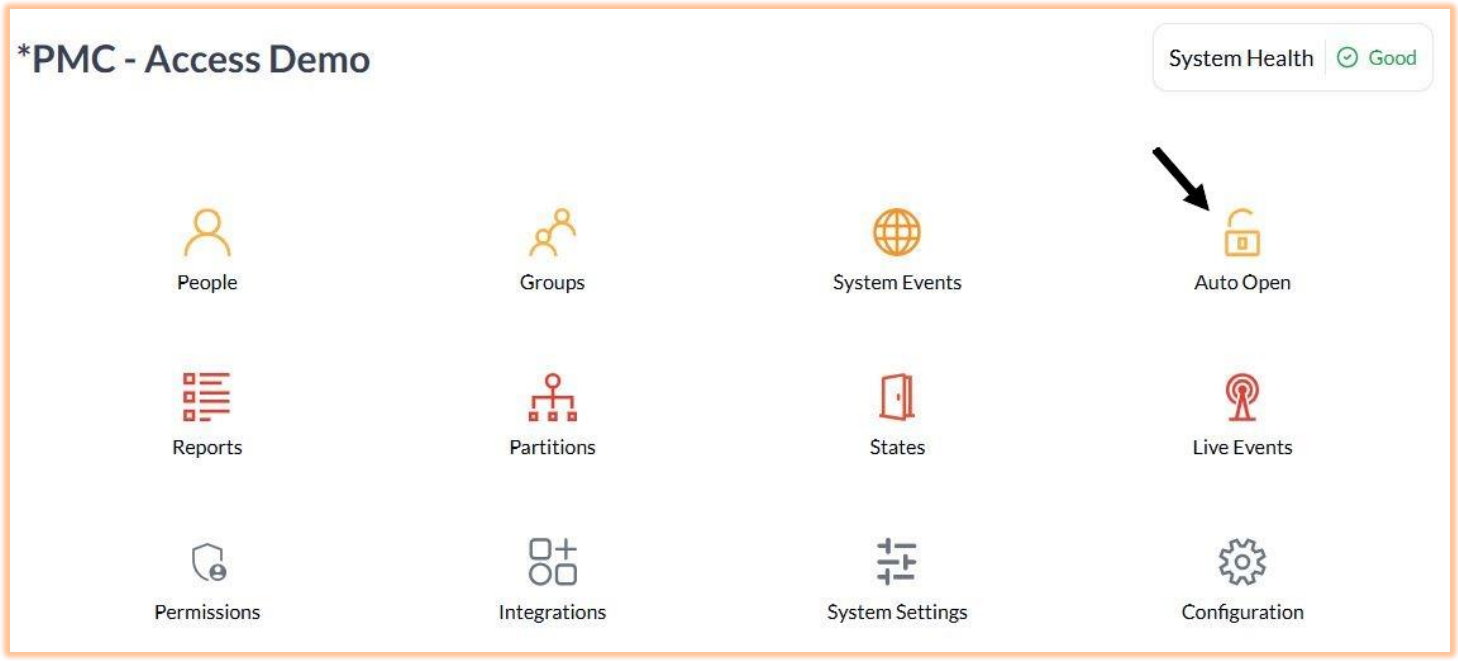
Persons with Permissions will show up inside the permissions page. Additional people can be added. It is recommended that at least two people have admin-level permissions to pdk.io. The customer who has Admin level Permissions to the account can add additional users themselves by the same process



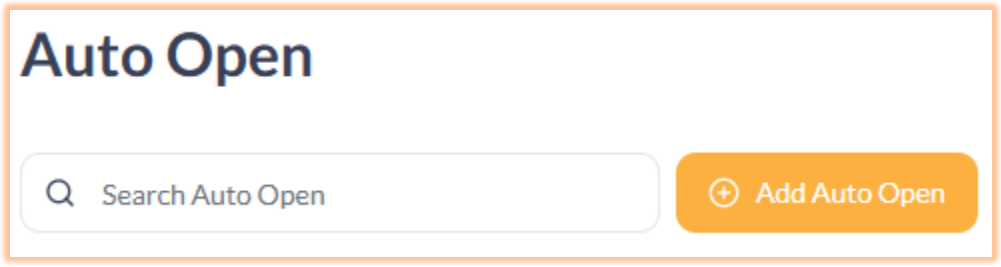
D. Auto Open and Holiday Schedules

Auto Open is where rules are created to set a door/device to 'Open' (unlocked) or 'Closed' (locked) for a specified time frame. As an example, let's create a typical weekly open schedule and a holiday on which the facility will be closed.

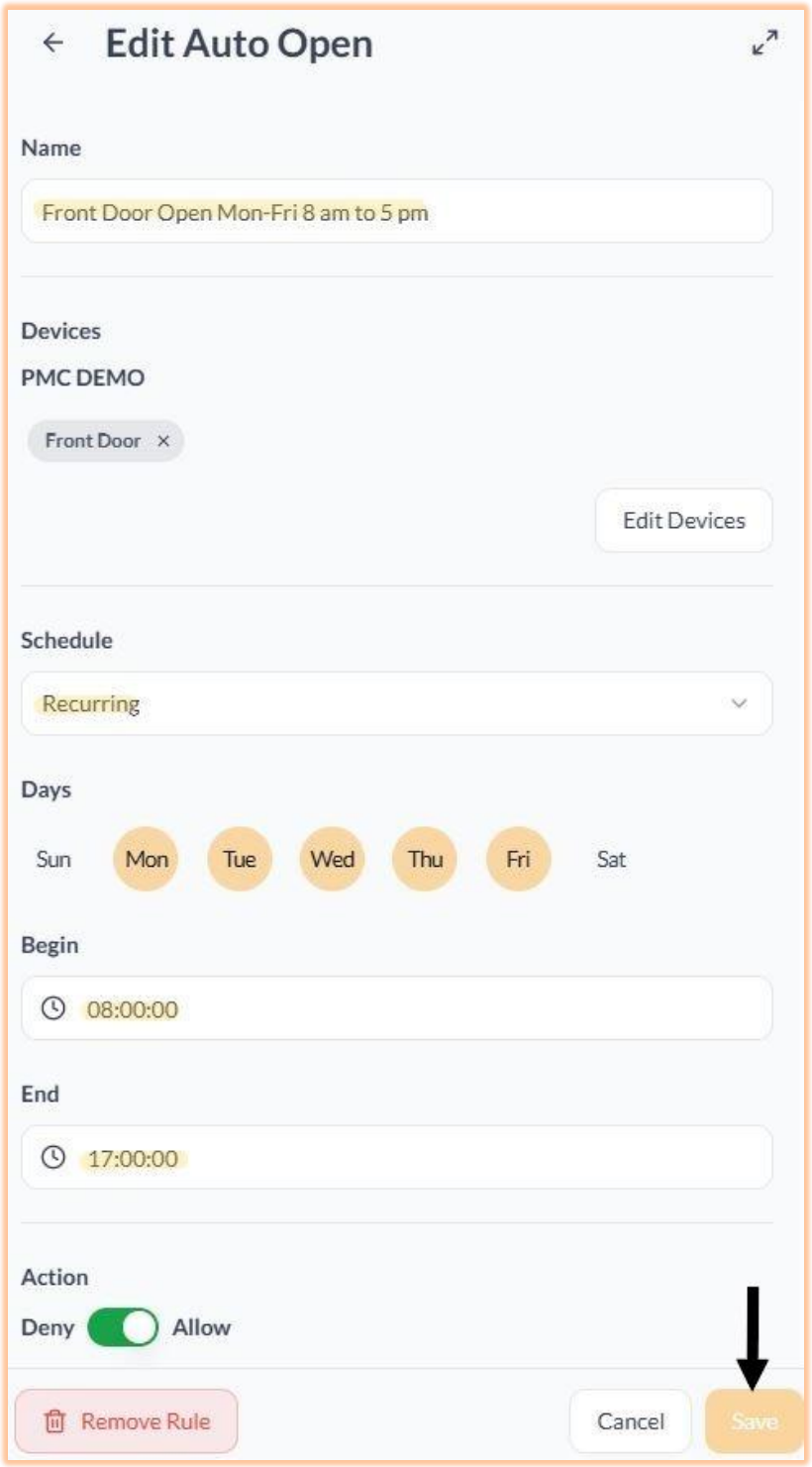
From the Customer Dashboard, click **Auto Open.**



Inside Auto Open, click **+ Add Auto Open**



A slide-out drawer will appear to the right.



Name: Name the Auto Open Schedule with a clear description of the location and times, such as: Front Door Open Mon-Fri 8 am to 5 pm

Devices: Which door or doors do you want to follow this schedule? Click **Edit Devices** to select.

Schedule: You have three choices from the dropdown.

- Always would mean the door or doors would always be open. (Typically, not used for most schedules)
- Recurring (default choice) refers to a schedule that repeats daily at specified times.
- Single Date is intended for scheduling an event to take place on the chosen future date.

Days: If Recurring is chosen from the schedule dropdown, you will have the option to select the day or days of the week for the schedule.

Begin and End: These are the times of the day for the schedule. If you choose multiple days, such as Mon Tue Wed Thu Fri, it will be the same times for each day. If you need different times on different days, you will need to create different Auto Open Schedules for days with different times. Note: Times are entered as military time, including seconds. For 8:00 am, enter 080000. For 5:00 pm, enter 170000. The system will automatically enter the colons.

Action: For an Open schedule, set to Allow.

Once everything has been entered. Click **Add** to create the schedule.

Holiday schedules. The access control system does not know when the facility is closed for holidays. The holiday schedules must be created to prevent doors from opening on an auto-open schedule. A holiday schedule does not prevent credential access. You may access doors on the holiday schedule with your credentials. The holiday schedule only overrides the auto-open schedule. Creating a holiday schedule is very similar to creating an auto-open schedule.

Name: Name the holiday schedule with the name of the holiday and the year. Note: The holiday schedule does not repeat year after year. Each year, you must create all the holiday schedules with specific dates for the corresponding year. Here is an example for Memorial Day 2025

Devices: Choose the same door or doors on the auto-open schedule.

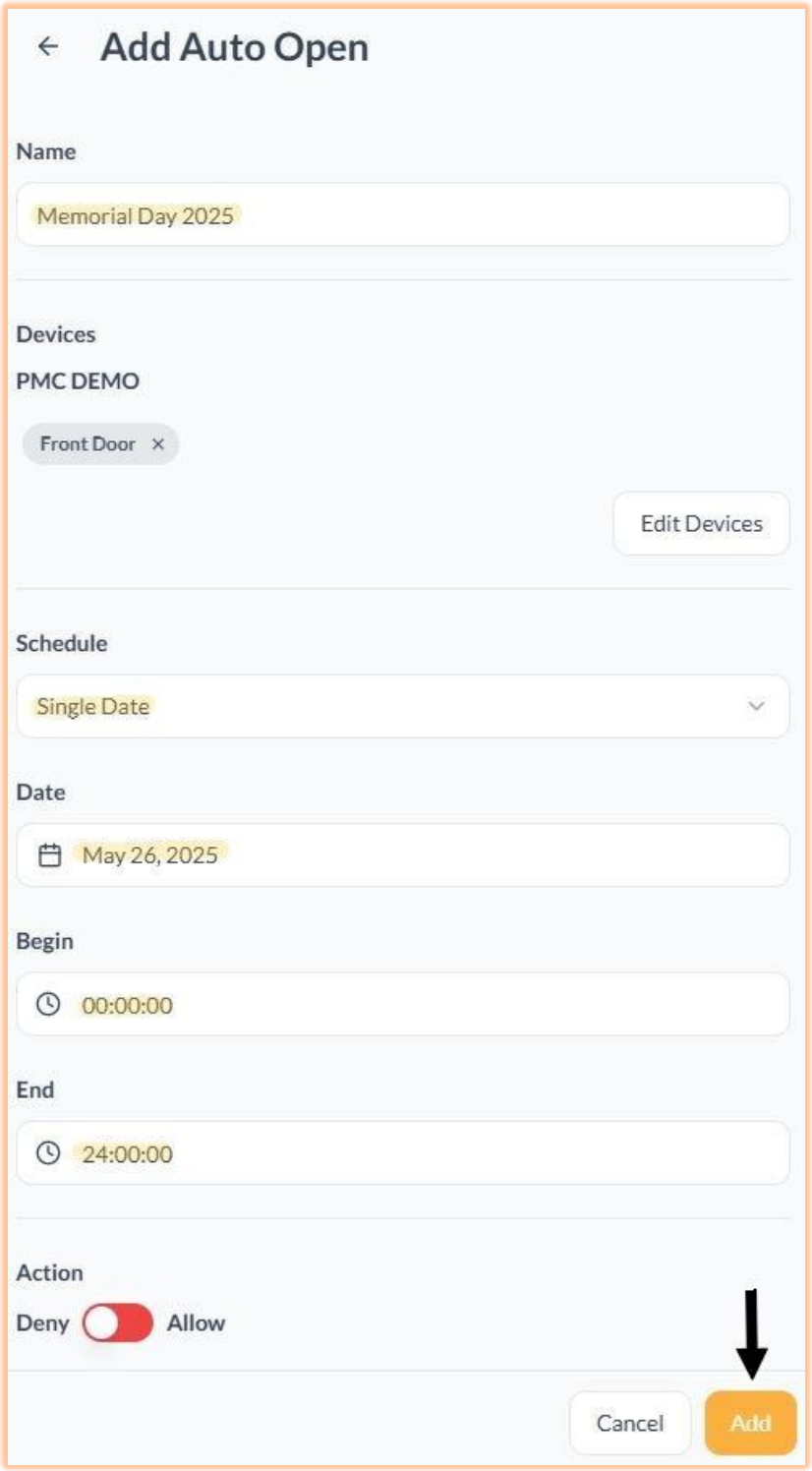
Schedule: Choose Single Date from the dropdown.

Date: Choose the date of the holiday for the specific year.

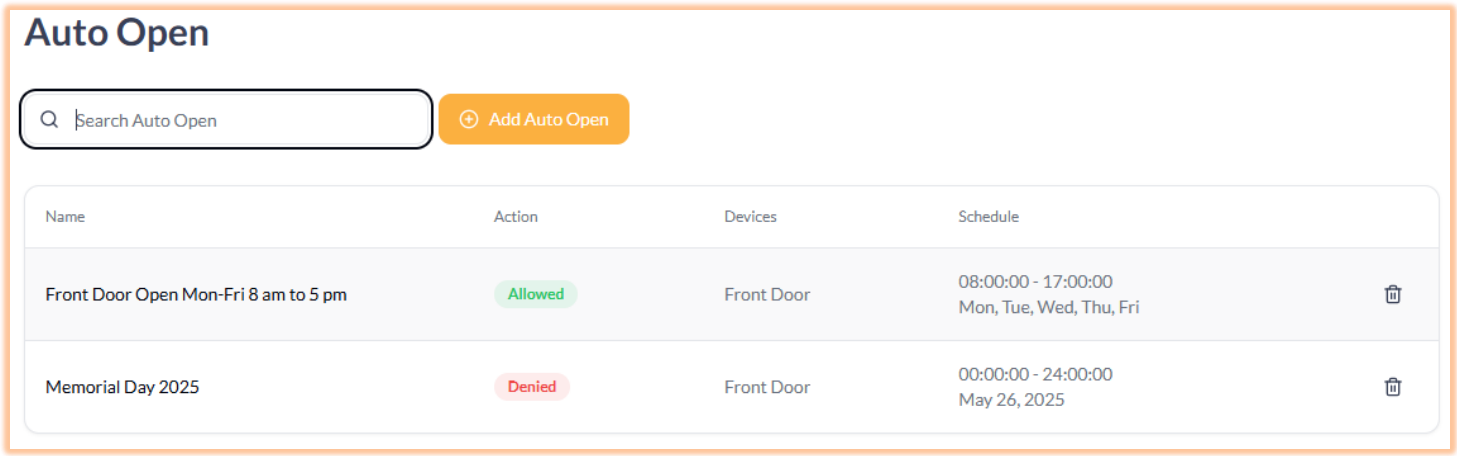
Begin and End: Leave at the default 00:00:00 and 24:00:00

Action: Select Deny. This step is very important. Unless this is changed to deny, the doors on the schedule will open instead of being locked.

Once everything has been entered. Click **Add** to create the Holiday schedule.



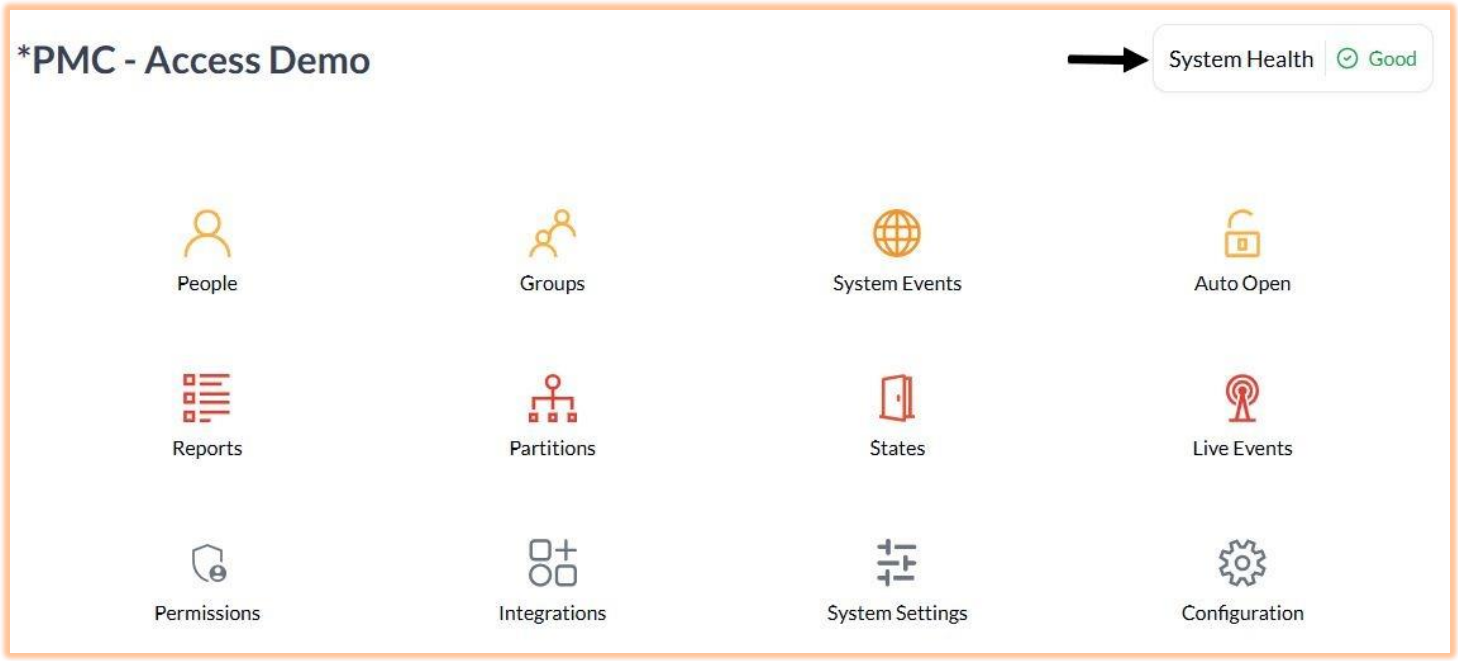
Once a Front Door Auto-open and Memorial Day Holiday schedule has been created. The Auto-open page will look like this. Note: Memorial Day 2025 Action is Denied, denoting it is a holiday schedule overriding the auto-open schedule. When additional schedules are created, they will be displayed on the Auto-open page.



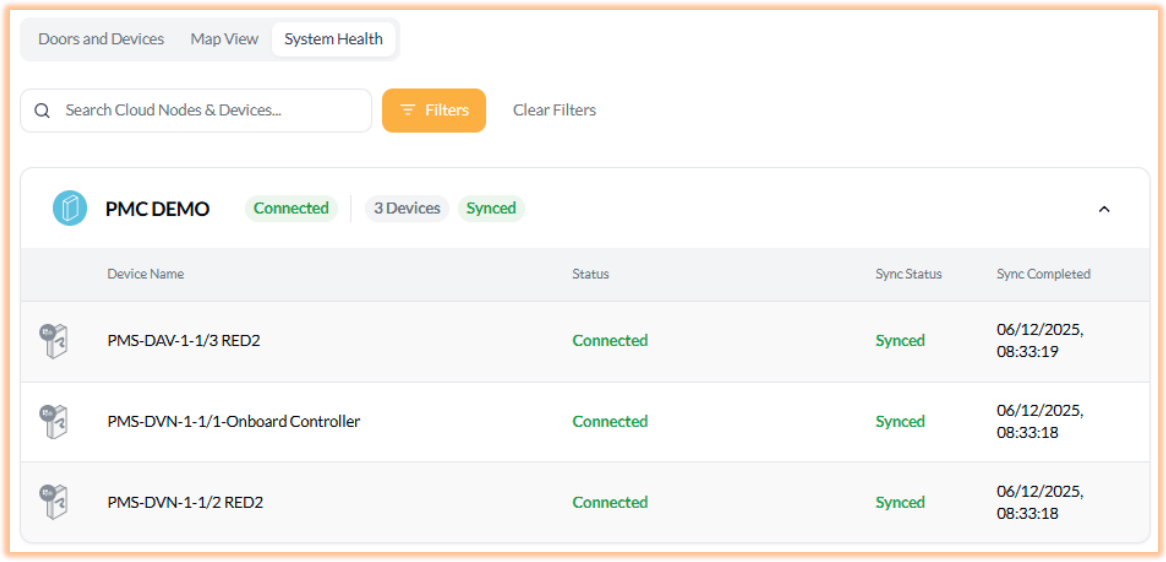
Holiday schedules should be created to prevent inadvertent door unlocking when the facility is closed. In the case of a “snow day,” where an Auto-open schedule has already unlocked doors, such as a case when the customer is going home early because of weather, the customer can FORCE TOGGLE the unlocked door(s) from PDK.io or the PDK Phone App from the State pages. The FORCE TOGGLE will lock an unlocked door. The door will remain unlocked until the next auto-open schedule. The reader will still work as normal for credential reads to unlock the door.

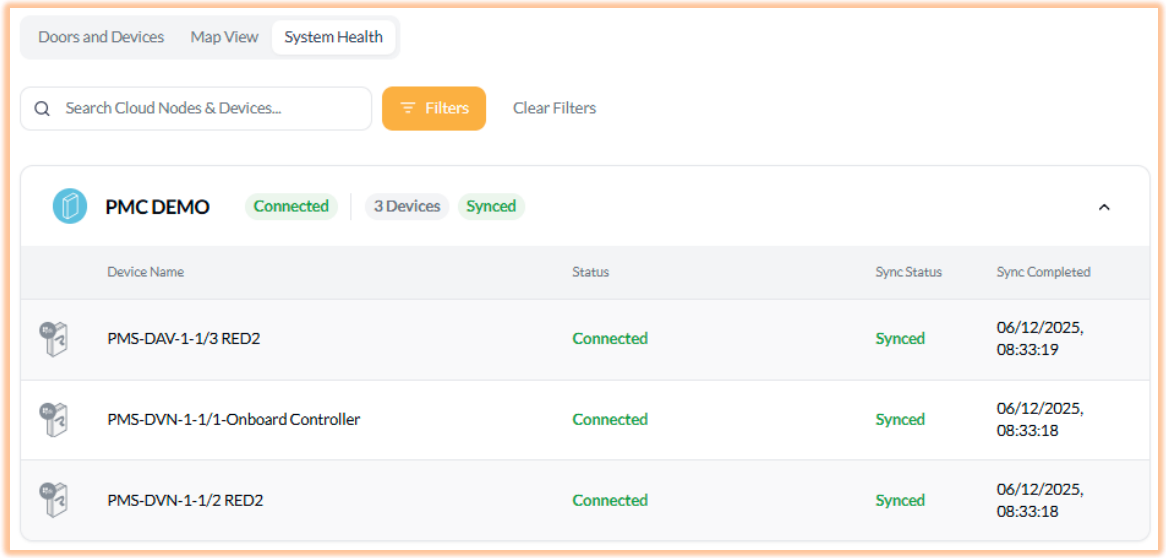
E. System Health

The System and Health window allows a user to quickly determine the current condition of the hardware (Cloud Nodes, Controllers, and connections) in the Customer Account**.** To access System Health, click on **System Health** from the Customer Dashboard.



The System Health page will open. The connected controllers with their Connection and Sync Statuses are displayed.





Status

Each Cloud Node and Controller added to the Customer Account will display the current Status of the Hardware.

- Connected - The hardware is currently connected to the Cloud Database, meaning any changes can be synced to the hardware**.**
- Disconnected - The hardware is currently not connected to the Cloud Database, meaning no changes can be synced to the hardware.

Sync Status

Each Red Cloud Node and Red Controller will show the current Sync Status.

- Pending - This status indicates that there are pending changes waiting to be synced with the Cloud Node or Controller. This can commonly occur due to pending Cloud Node updates, offline Controllers (which will sync upon re-connection), and other temporary conditions.
- Syncing - This Status shows the Cloud Node or Controller is currently downloading and synchronizing the local database with the Cloud-based database.
- Synced - This Status shows that the local database is synchronized with the current Cloud-based database.
- Failed - If the Cloud Node or Controller is in this Status, contact Per Mar Security

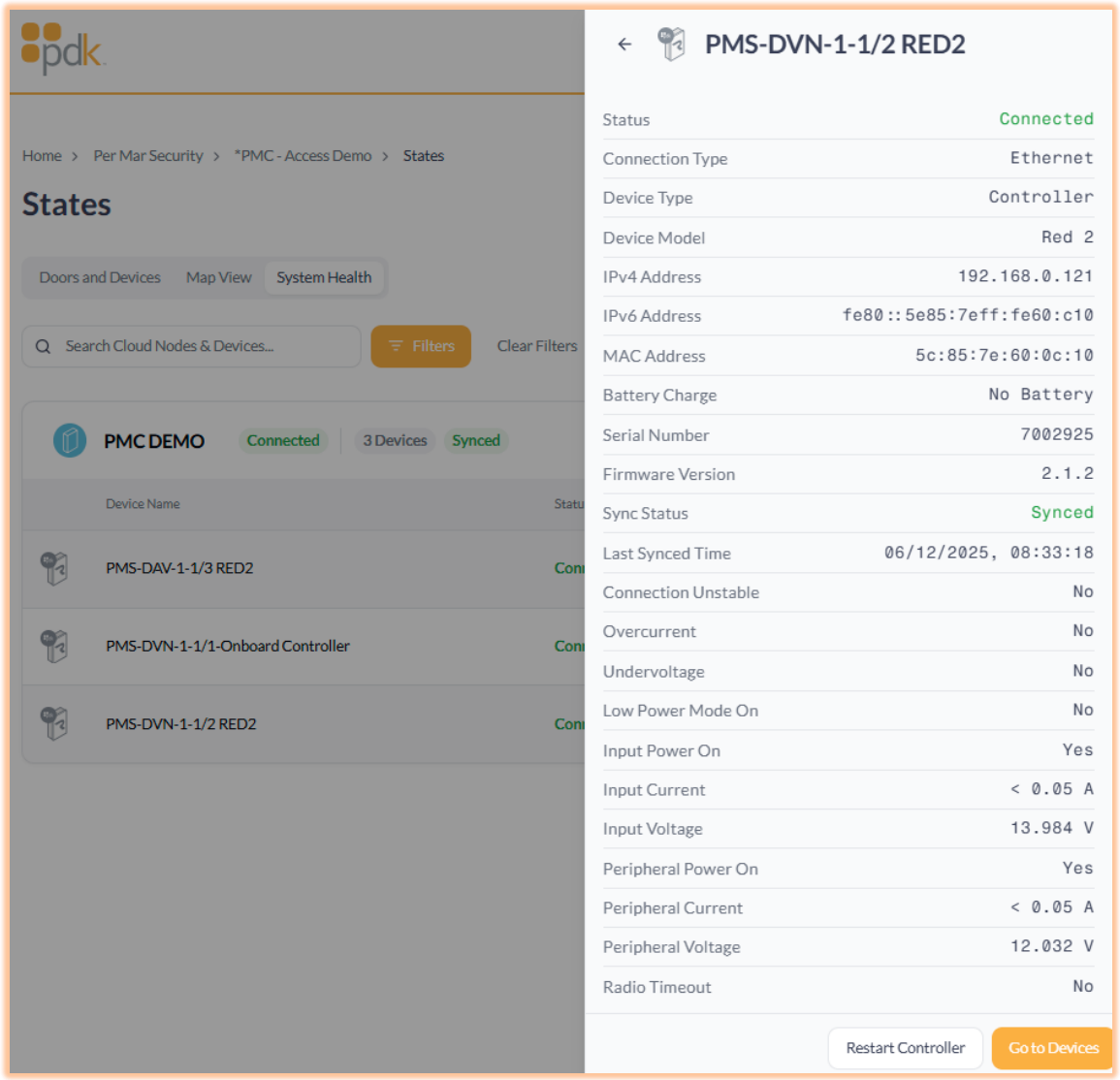
Sync Completed

- Displays the most recent date and time the controller was synchronized with the system data. System changes only trigger synchronization for the controllers directly affected by those changes. For example, if updates are made to only a subset of access doors, only the controllers associated with those specific doors will sync to reflect the date of the system change.

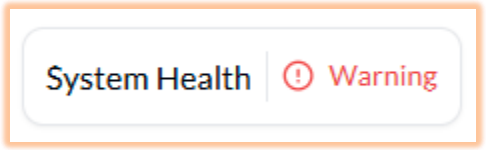
Clicking any Controller will slide out the drawer for Controller Health Details. From here, you can check more details of each controller. These details are more useful for technicians.

Clicking on **Go to Devices** will take you to the States page with the Doors connected to that controller.

Restart Controller while visible is not available for use by the customer.

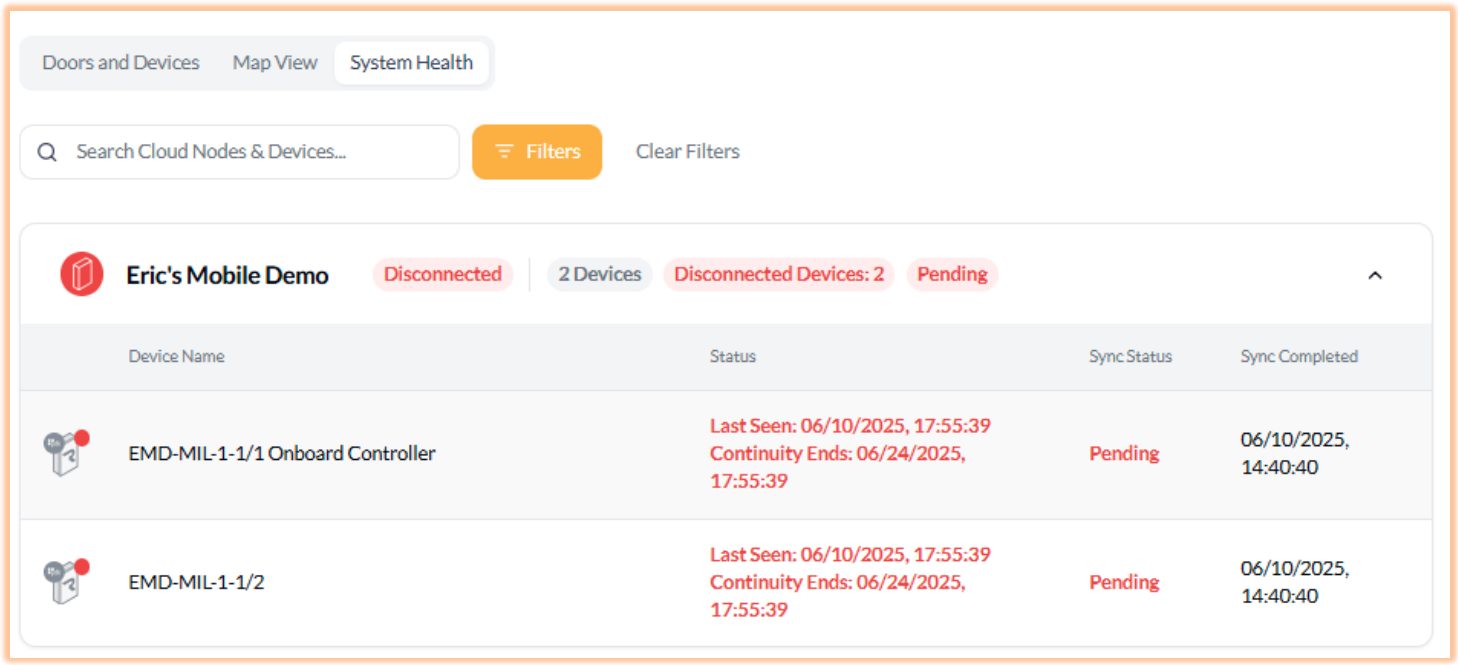


System Health Warning



If your System Health displays a warning, this may indicate a connection or syncing issue between the cloud node and your controllers. If your building loses internet service or experiences a network interruption, the controllers will appear as disconnected. During such interruptions, the access control system will continue to operate normally; however, no system changes can be made until connectivity is restored. Any changes attempted during the outage will automatically sync once the network is back online.

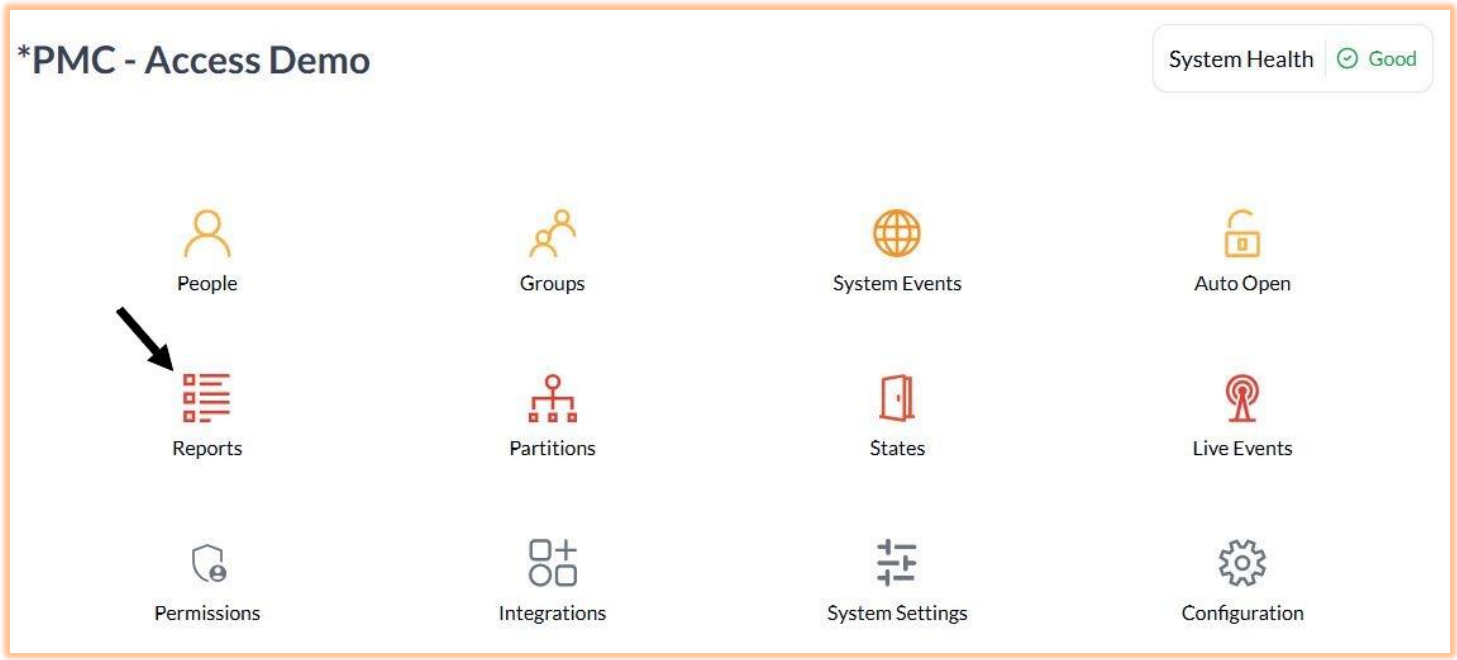
If your controllers show as disconnected, first check with your internet service provider or IT department to ensure your network is functioning properly. If your network is operating correctly but the controllers remain disconnected, please contact Per Mar Security for assistance.



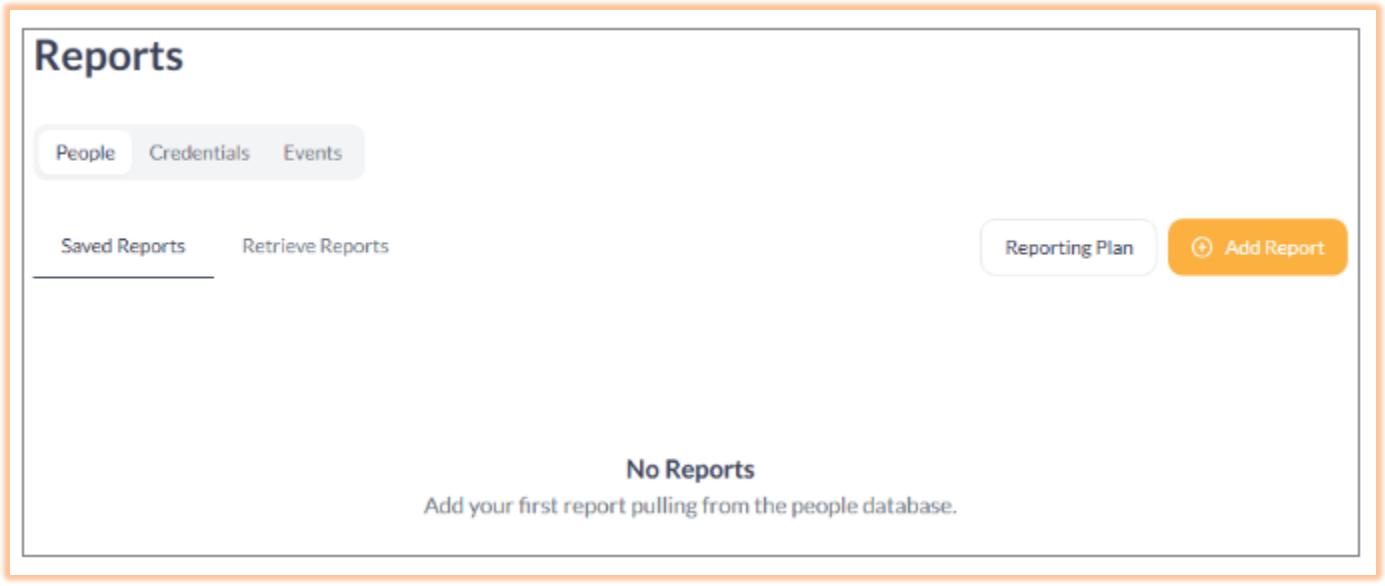
F. Reports

Reports allow a user to set up, save, and retrieve Reports that contain details about People, Credentials, and events on the Customer Account.

To access Reports, click on **Reports** from the Customer Dashboard.



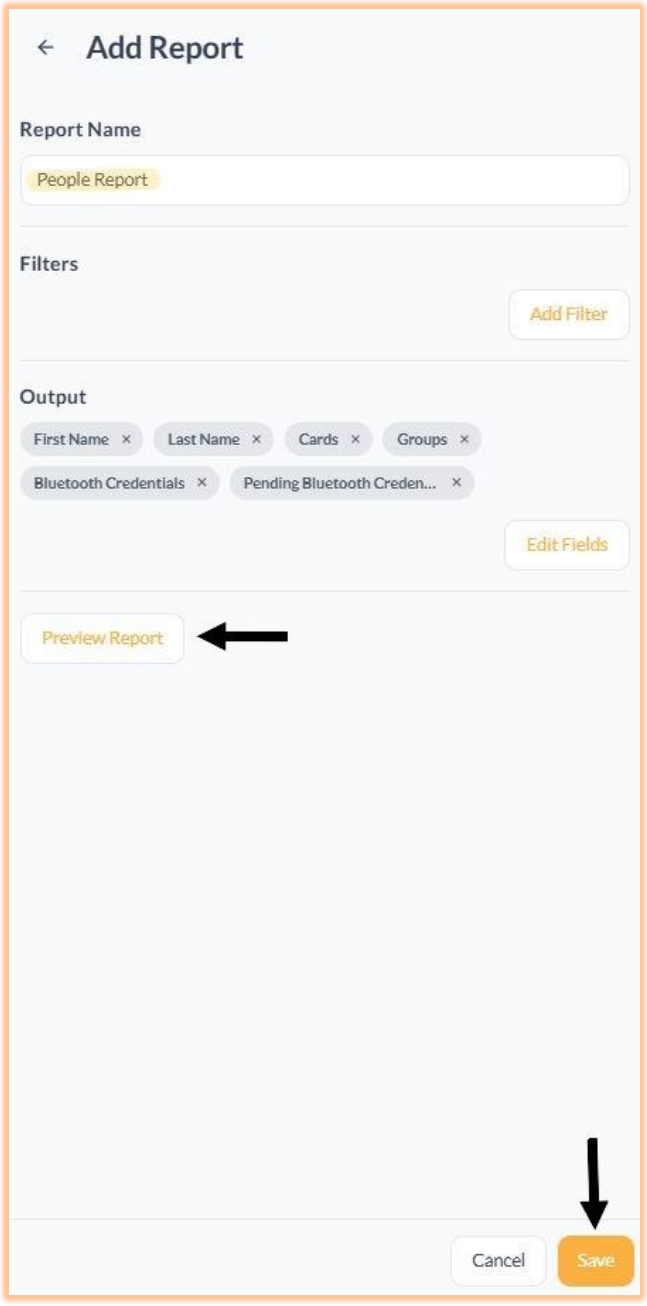
Inside the Reports page, there will be three options for report types: People, Credentials, and Events. Inside each tab, there will be options for Save Reports and Retrieve Reports.



Running a People Report

Inside the Reports page, select the People tab, and click **+ Add Report.**

A slide-out drawer will appear to the right



Report Name: Enter a descriptive Name for the People Report.

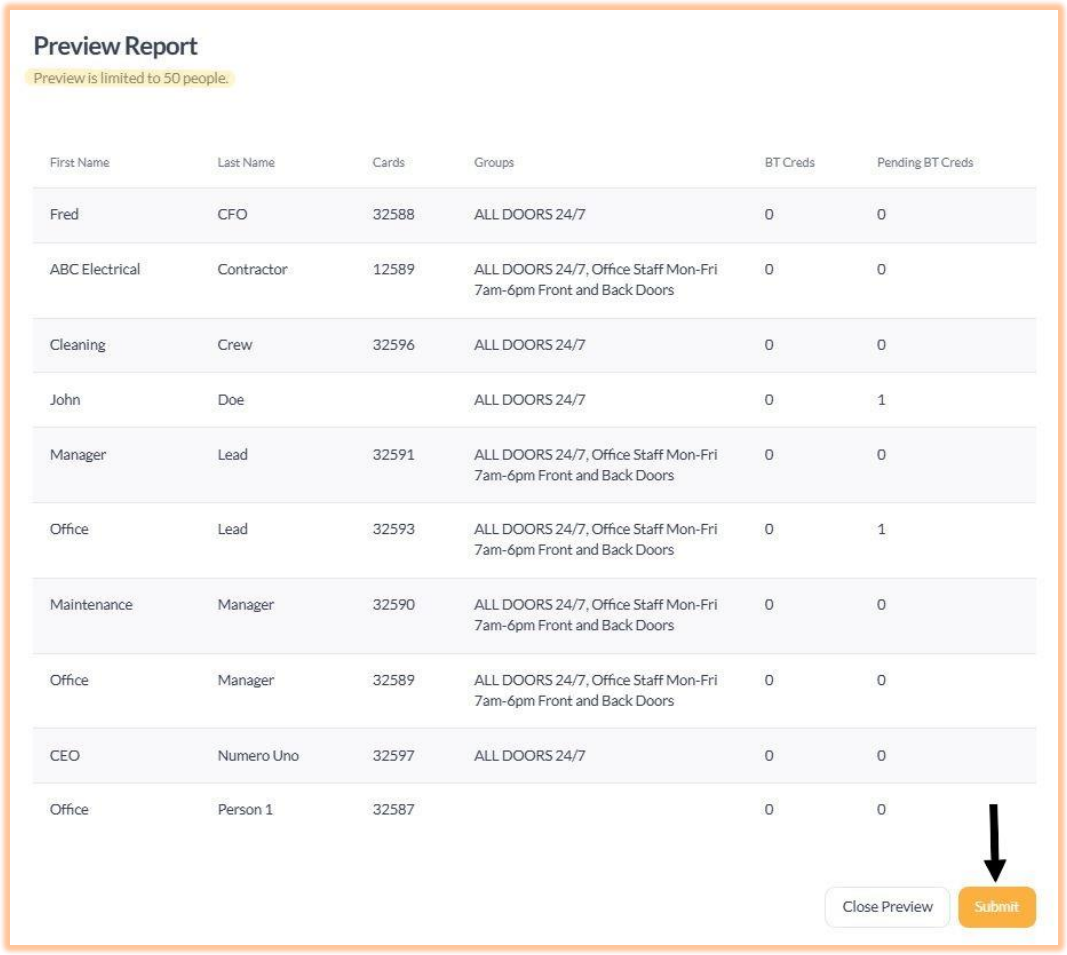
Filters: By clicking **Add Filter**, you can select the filter options for the Report, such as First Name, Last Name, and Email. You can select between including the selected item(s) or excluding the selected item(s) from the Report.

Output: By clicking **Edit Fields,** you can filter the outputs for the People Report, such as cards, Groups, and Bluetooth Credentials. In this example, the Filter Outputs are First Name, Last Name, Cards, Bluetooth Credentials, and Pending Bluetooth Credentials.

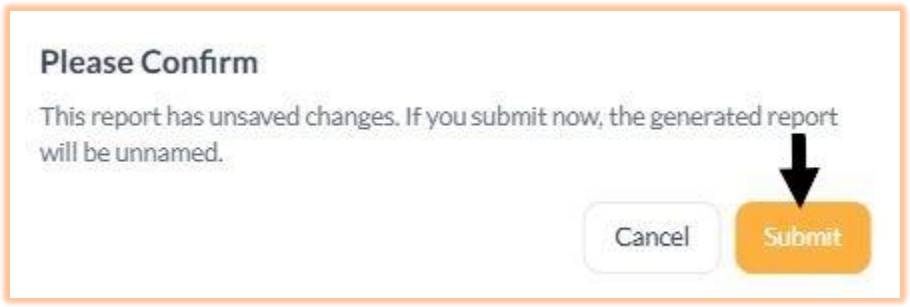
Preview Report: Allows viewing of the report before saving.

Save: Saves the report profile in the Saved Reports section to be viewed and run later.

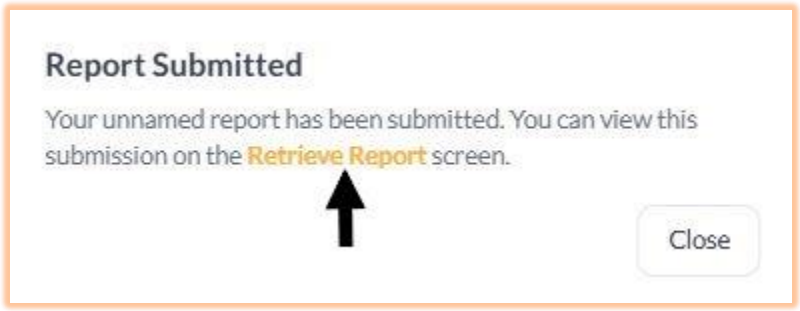
By clicking Preview Report, a new pop-up window will appear. Note that the preview is limited to 50 people.



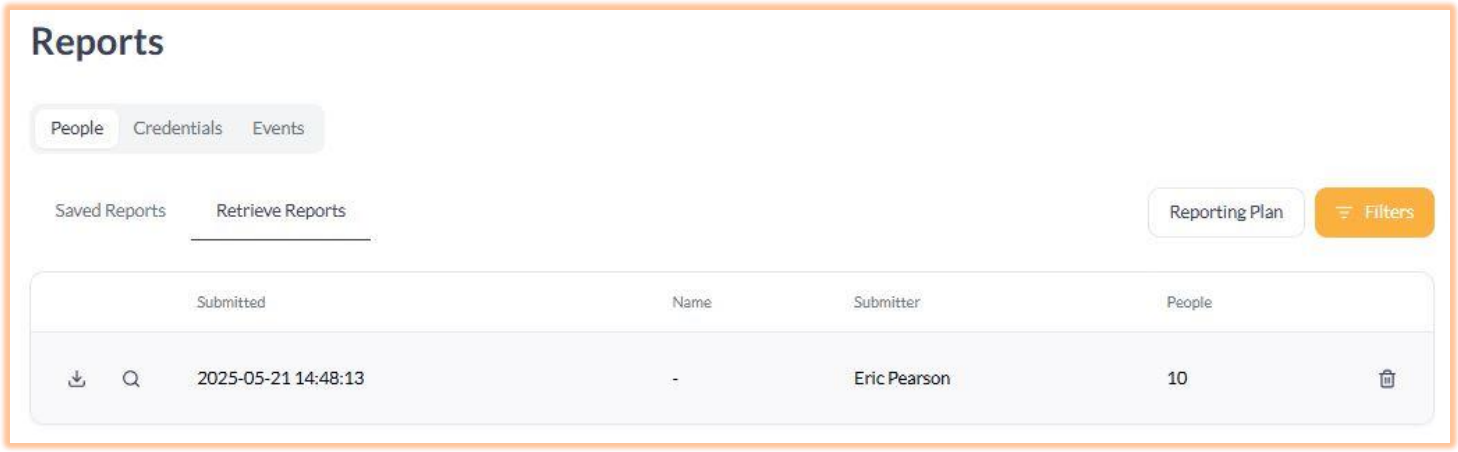
Clicking **Submit** will bring up a Please Confirm pop-up window**.** Click **Submit.**



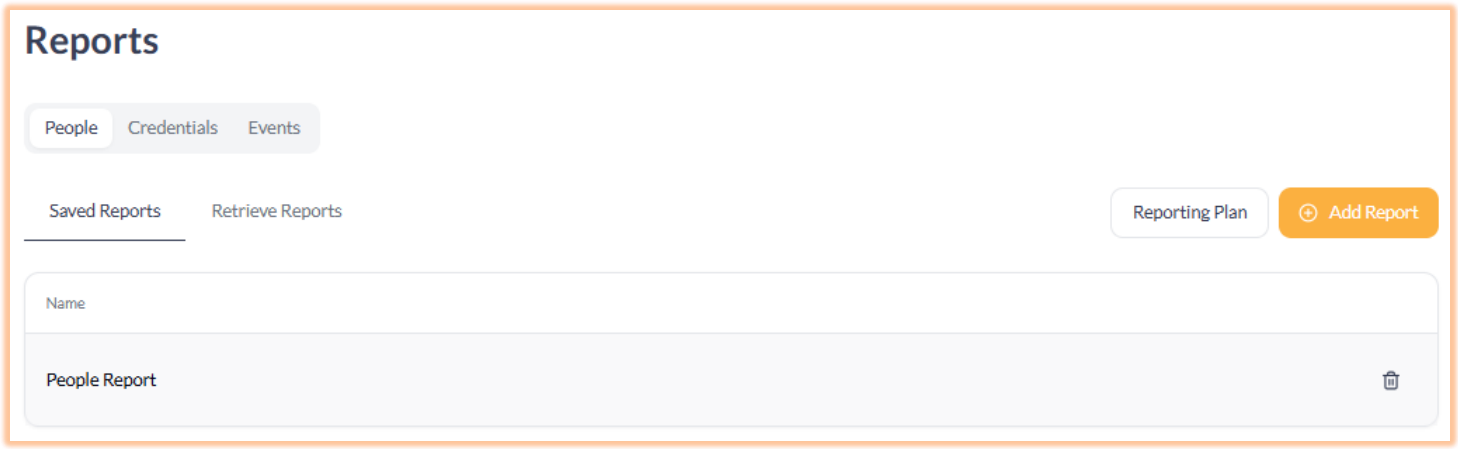
Click **Retrieve Report** from Report Submitted pop-up window.



After clicking Retrieve Report, the Retrieve Reports window will open. From there, you can download or view the report.



Report profiles that have been saved can be previewed and submitted from Saved Reports in the People tab.



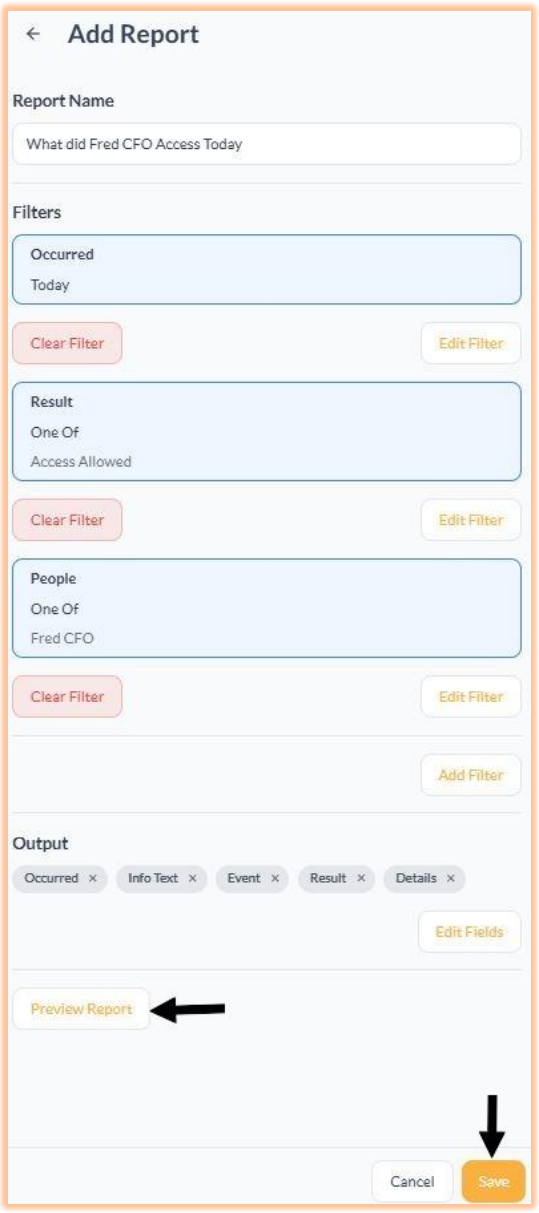
Running an Event Report

Event Reports allow a User to run Reports based on the Events that have occurred on the Customer Account. Events can be filtered by Occurred, Events, Results, Devices, Persons, Cards, Connections, and Groups.

Inside the Reports page, select the Events tab, and click **+ Add Report.**

A slide-out drawer will appear to the right

Numerous filters can be applied to an Event Report. In this example, the report was filtered to Occurred: Today, Result: Access Allowed, and People: Fred CFO.

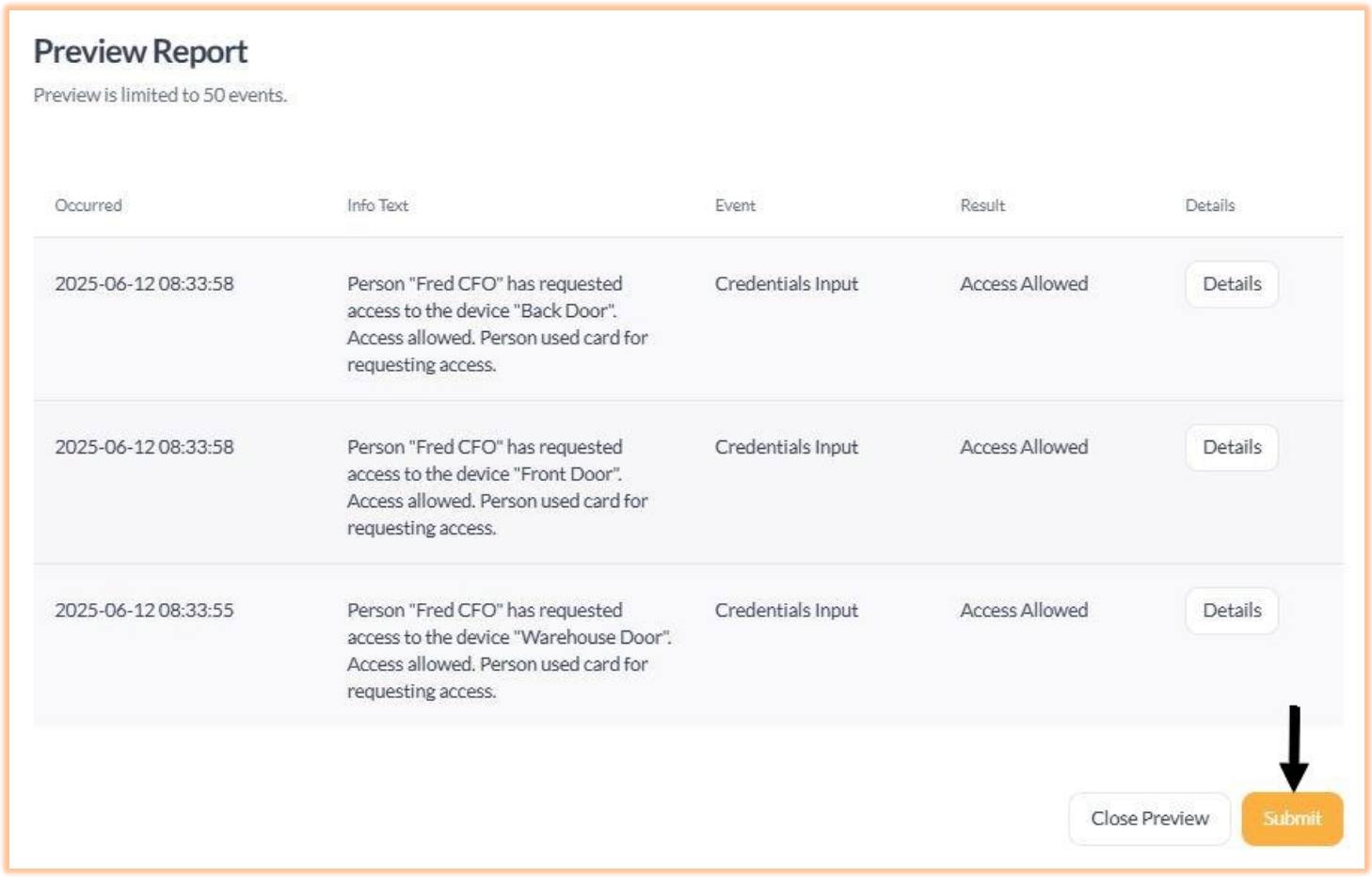


Output: By clicking **Edit Fields,** you can filter the outputs for the Event Report: Occurred, Info Text, Event, Result, and Details. For Event Reports, it is best to select all output which is the default.

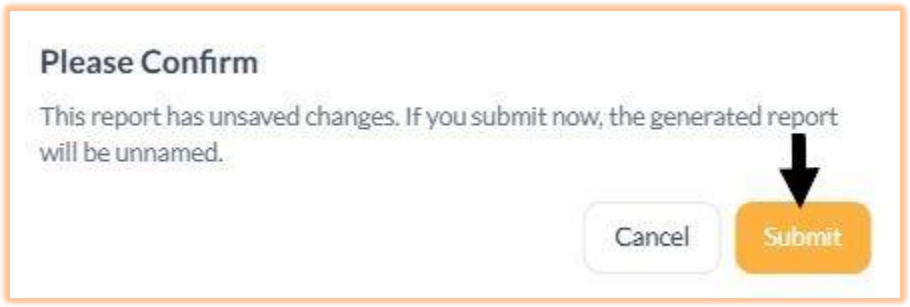
Preview Report: Allows viewing of the report before saving.

Save: Saves the report profile in the Saved Reports section to be viewed and run later.

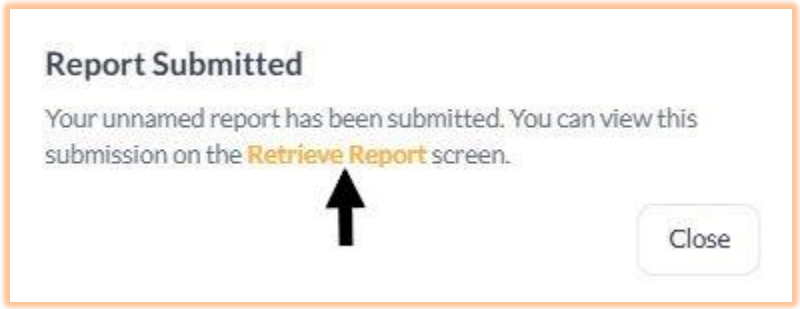
By clicking Preview Report, a new pop-up window will appear. Note that the preview is limited to 50 events or the last 7 days.



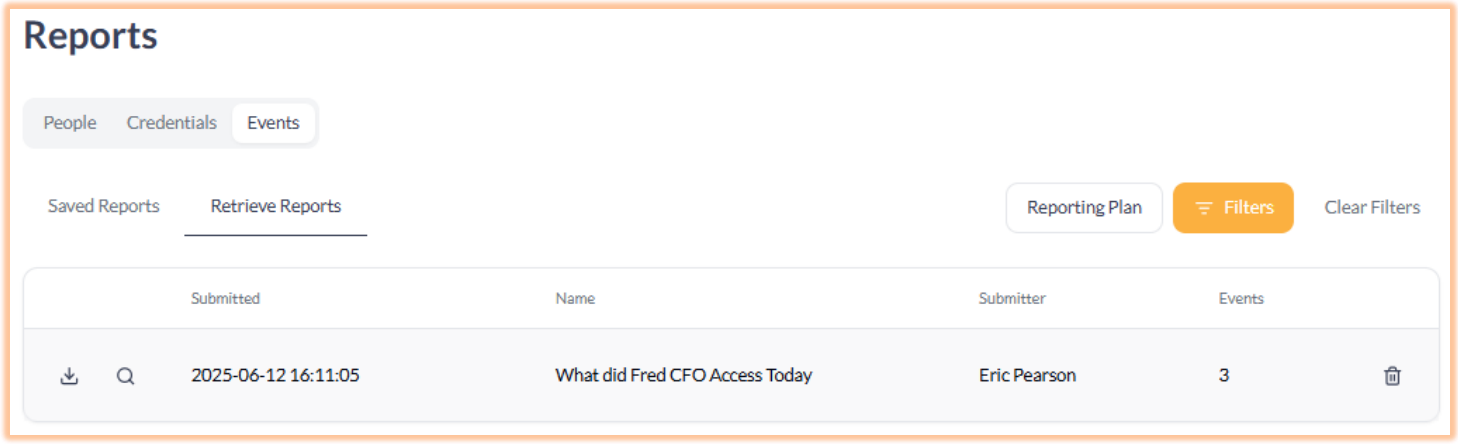
Clicking **Submit** will bring up a Please Confirm pop-up window**.** Click **Submit.**



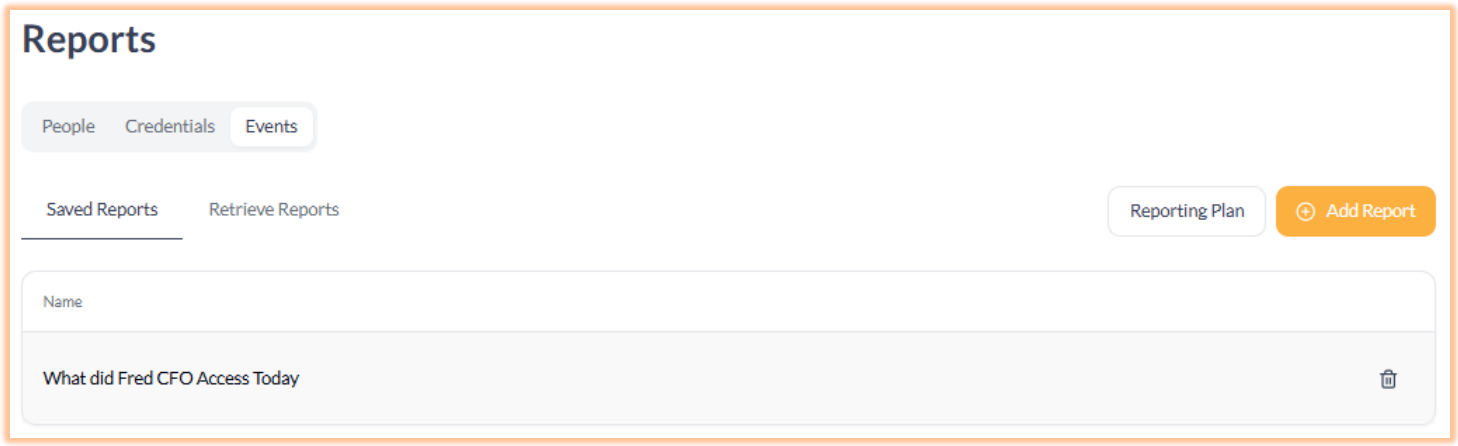
Click **Retrieve Report** from Report Submitted pop-up window.



After clicking Retrieve Report, the Retrieve Reports window will open. From there, you can download or view the report

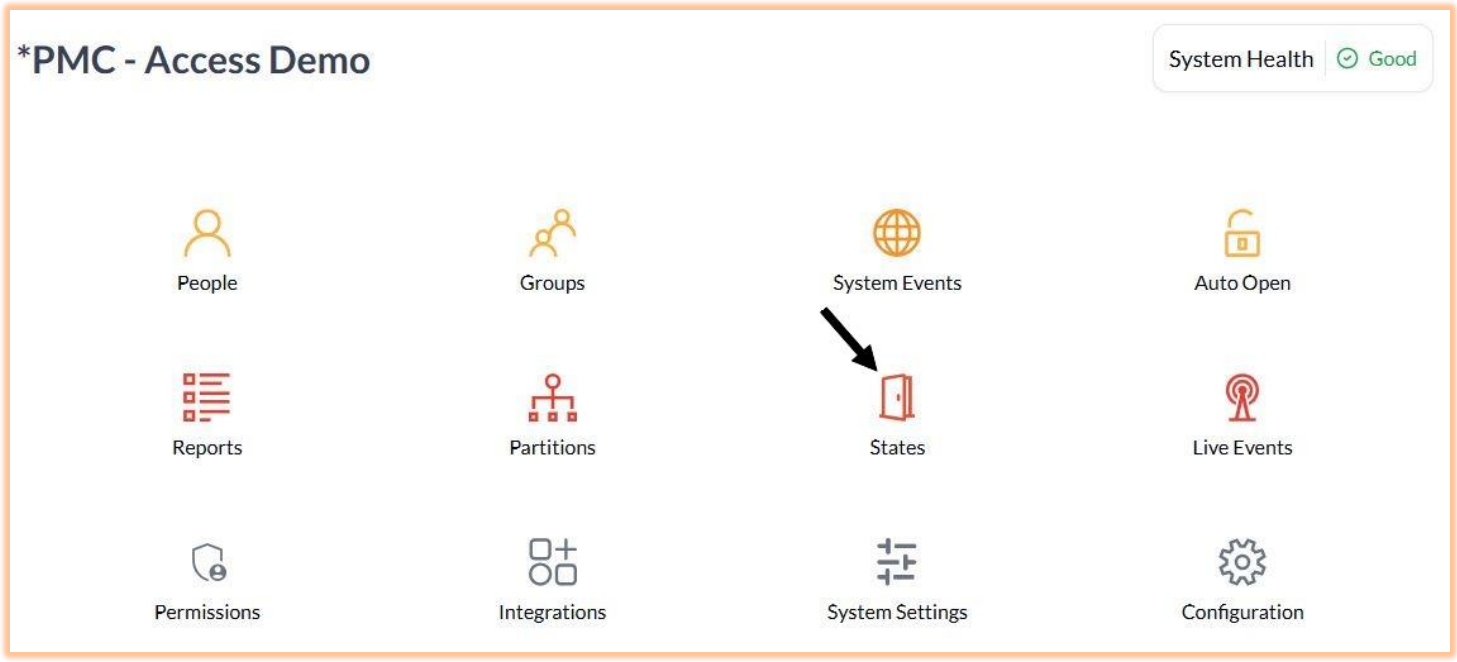


Report profiles that have been saved can be previewed and submitted from Saved Reports in the Events tab.

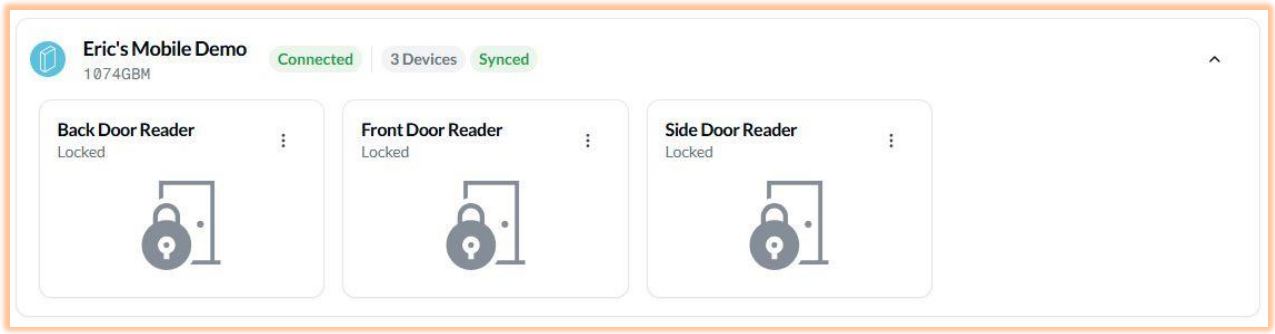


G. States

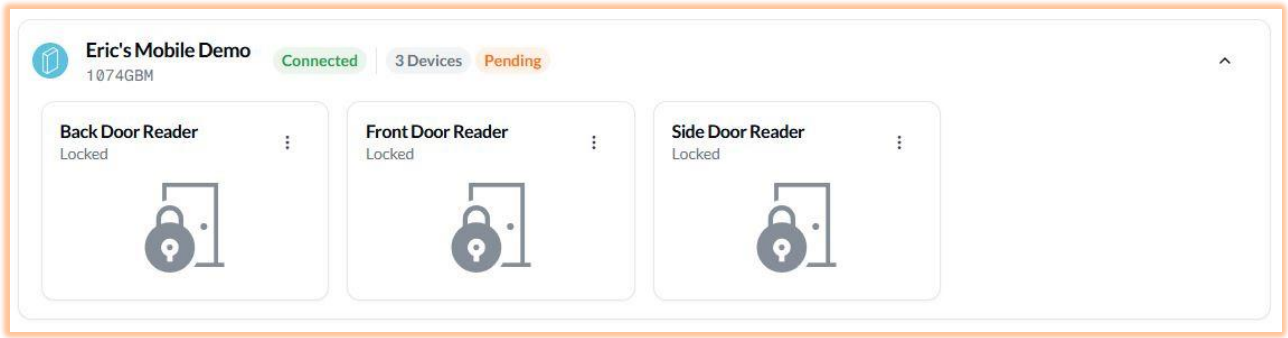
The States page allows you to view and control the state of connected doors and devices. To access States, click on **States** from the Customer Dashboard.



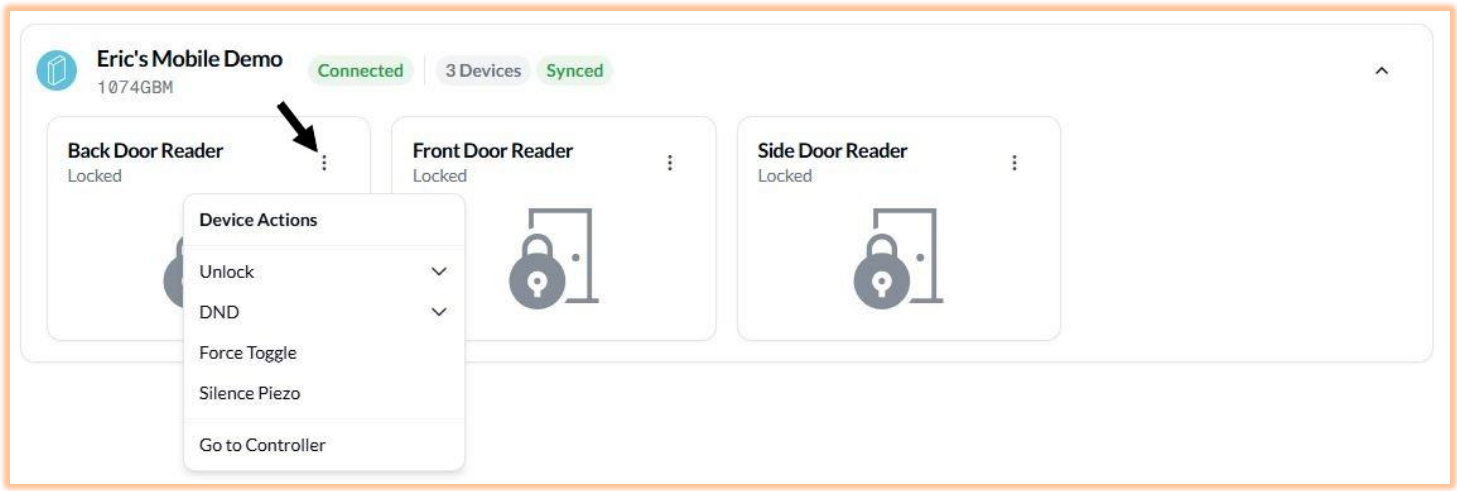
The **States** page will display the status of the doors and devices of the account. Here we see three doors in the system. The three doors are locked. The controllers are **connected** to the cloud and **synced**.



In this view, the three doors are locked, and the controllers are connected. **Pending** shows that the controllers are currently syncing recent changes. Depending on the size of the system and the number of recent changes, it may show pending for a few seconds or several minutes.



Clicking on the 3 vertical dots will bring up the Device Actions pop-up.



Unlock/Lock

If the door/device is currently locked/deactivated, 'Unlock' will be shown. If the door/device is currently unlocked/activated, 'Lock' will be shown. Clicking on the option will perform the action shown (locking or unlocking the door). Clicking the downward arrow next to the option, you can specify a time up to 90 minutes to remain unlocked.

DND (Do Not Disturb)/DND Cancel

This option will place the door/device into DND, or Do-Not-Disturb, which will lock/deactivate the door/device and place it into a condition where credentials will be denied unless specific rules are created by a user. When the door/device is in DND mode, tapping/clicking the DND Cancel option will remove the DND option. By tapping/clicking the downward arrow next to the option, you can specify a time of up to 90 minutes to remain in DND mode.

Force Toggle

The Force Toggle option allows users to unlock a currently locked door for an indefinite period or to cancel an existing Force Toggle command that is being sent.

If the door is locked, clicking this option will unlock it until a second Force Toggle command is sent.

If the door is currently unlocked through a credential input or an unlock command, Force Toggle will cause it to remain unlocked until another Force Toggle command is sent. If the door is unlocked due to an auto-open schedule, clicking the Force Toggle option will lock the door. The door will remain locked until the next auto-open schedule. Credential inputs will unlock the door as normal.

Silence Piezo

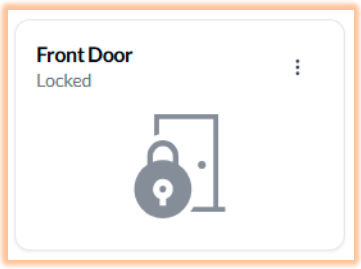
With the Red-series reader wired using OSDP, the piezo buzzer in the reader is controlled by the software and not a dedicated relay. If the piezo buzzer in the Red-series reader has been triggered and you wish to end the activation early, click this option.

Go to Controller

Clicking this option will take you to the Controllers and Hubs view for the controller for this door/device.

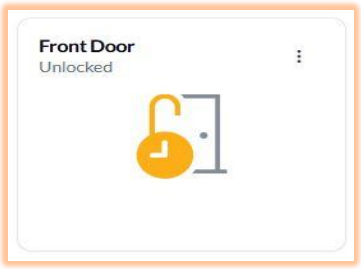
States Icons Explained

Door Locked



Door Unlocked

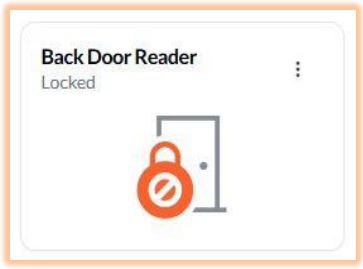
Door Unlocked with Auto-open



Door force-toggled locked

Door force-toggled unlocked

Door DND Do not Disturb

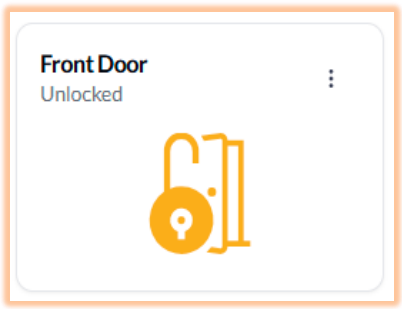


Controller Issues

The following states if a door position switch is installed.

Door Locked. Door Position Open.

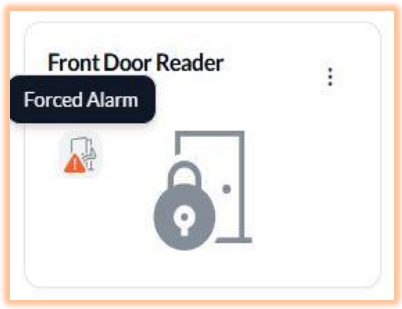
Door Unlocked. Door Position Open



The following states if a door position switch is installed and the door force alarm is enabled on the device.

Door Forced Open. Door Position Open.

Door Forced Open. Door Position Closed.



The following state is only if a door position switch is installed and the door prop alarm is enabled on the device

Door Position Open. Door held open longer than the door prop alarm time.