

PDK.io Software User Manual



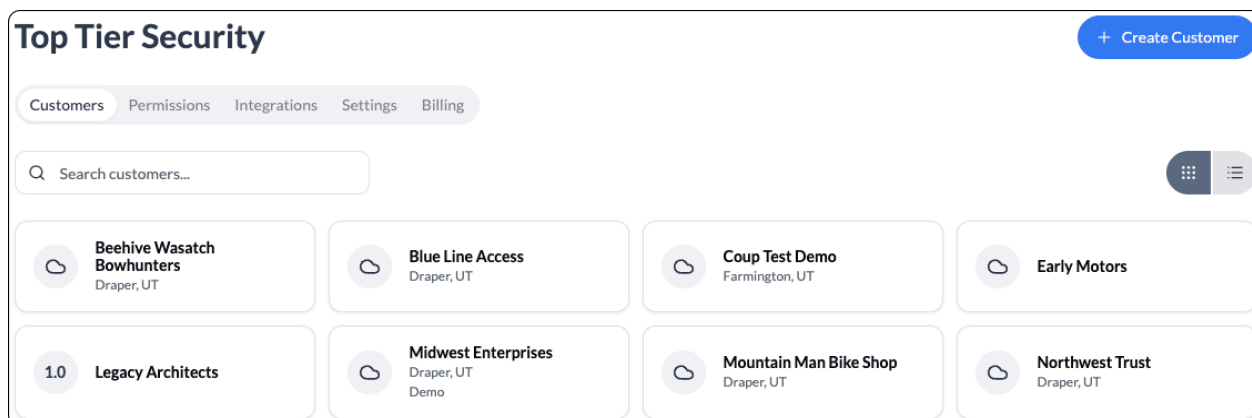
Table of Contents

1.0 Dealer Homepage.....	2
1.1 Accessing a Customer.....	2
1.2 Add a New Customer.....	2
1.3 Editing Existing Customers.....	5
1.4 Deleting Customers.....	6
1.5 Adding a Permission.....	7
1.6 Editing or Deleting an Existing Permission.....	9
1.7 Integrations List.....	10
1.8 Adding a Support Contact.....	11
1.9 Billing Dashboard.....	13
2.0 Customer Dashboard.....	19
2.1 People.....	19
2.2 Groups.....	55
2.3 Units.....	82
2.4 System Events.....	86
2.5 Auto Open.....	93
2.6 Elevators.....	109
2.7 Reports.....	112
2.8 Partitions.....	125
2.9 States.....	129
2.10 Live Events.....	161
2.11 Permissions.....	166
2.12 Integrations.....	170
2.13 System Settings.....	172
2.14 Configuration.....	186
3.0 Settings.....	223
3.1 Account Settings.....	224

1.0 Dealer Homepage

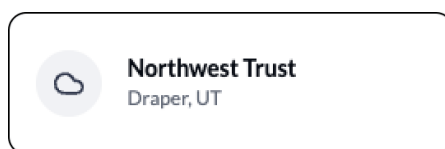
1.0 Dealer Homepage

The Dealer Homepage allows an Installation Partner to view and manage their Customer Accounts (add, edit, or remove).



When an Installation Partner logs in to the PDK.io website or Manage Access in the PDK Access app, they will see the Dealer Homepage for their company.

1.1 Accessing a Customer



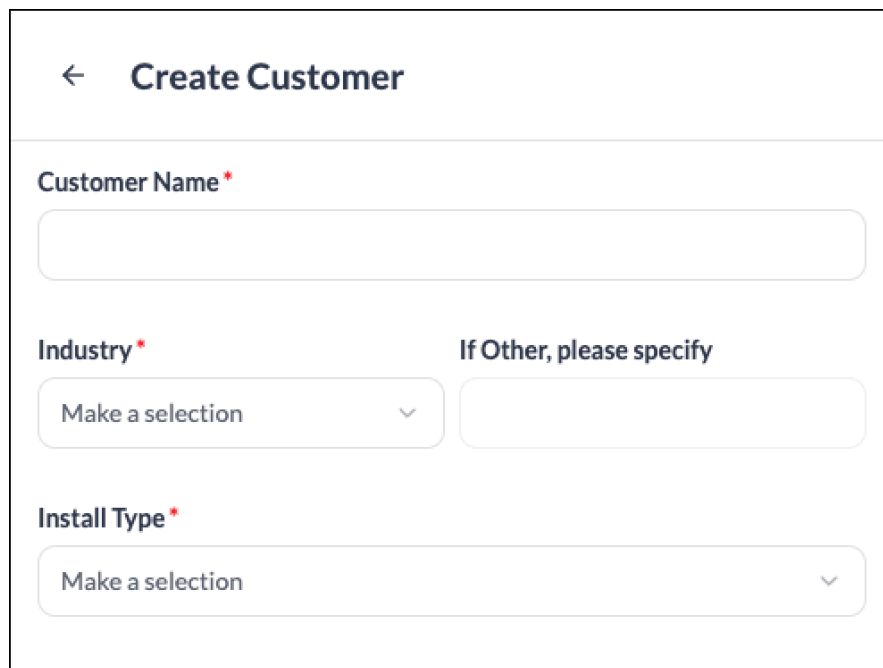
To access a Customer, the Installation Partner simply selects the Customer's name to open the Customer Dashboard. You can also find a Customer by using the search bar located above the Customer list.

1.2 Add a New Customer

To add a new Customer to the Dealer Homepage, select **+ Create Customer**.

+ Create Customer

This opens the **Create Customer** drawer.



The screenshot shows a 'Create Customer' drawer with a back arrow and title. It contains three main sections: 'Customer Name' with a text input field; 'Industry' with a dropdown menu labeled 'Make a selection' and a text input field labeled 'If Other, please specify'; and 'Install Type' with a dropdown menu labeled 'Make a selection'.

Customer Name - Enter the **Customer** account name in this field. This name will be visible to anyone able to access the Customer Dashboard.

Industry and **Install Type** - Enter the Industry type for the **Customer** and select whether this is a **New Install** or **Replacing/Upgrading an Existing PDK System**.

1.0 Dealer Homepage

Street Address *

Apartment/Suite/Building

City *

State/Province/Region *

Zip/Postal Code *

Country *

 Use Current Location as Address

Street Address - Enter the Street Address for the Customer.

Enable issuance of Bluetooth credentials

Users that have been issued a Bluetooth credential can unlock doors by presenting their smartphone to a Bluetooth-enabled reader.

☒

Enable issuance of Mobile App credentials

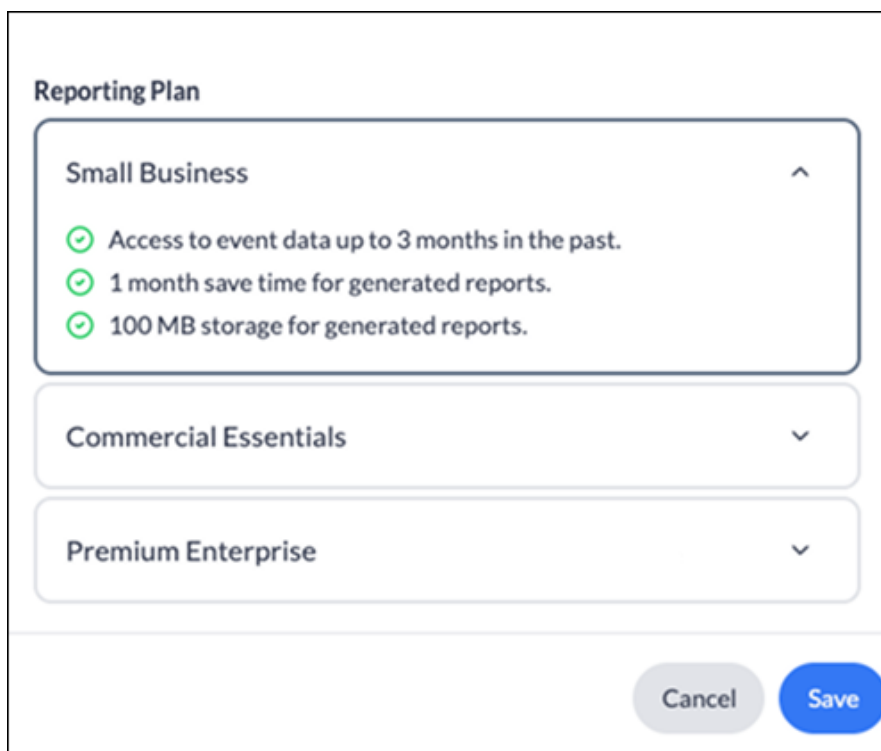
Users that have been issued a Mobile App credential can remotely unlock doors via the PDK app.

☒

Enable issuance of Bluetooth Credentials - Select to enable or disable this feature.

Enable issuance of Mobile App Credentials - Select to enable or disable this feature.

1.0 Dealer Homepage



The image shows a 'Reporting Plan' selection dialog. It has a title 'Reporting Plan' at the top. Below the title are three plan options, each in a rounded rectangle with a dropdown arrow on the right. The first option is 'Small Business' and is highlighted with a blue border. It lists three features with green checkmarks: 'Access to event data up to 3 months in the past.', '1 month save time for generated reports.', and '100 MB storage for generated reports.' The second option is 'Commercial Essentials' and the third is 'Premium Enterprise'. At the bottom right of the dialog are two buttons: a grey 'Cancel' button and a blue 'Save' button.

Reporting Plan

Small Business ^

- ✓ Access to event data up to 3 months in the past.
- ✓ 1 month save time for generated reports.
- ✓ 100 MB storage for generated reports.

Commercial Essentials v

Premium Enterprise v

Cancel Save

Reporting Plan - Select the plan (Small Business, Commercial Essentials, or Premium Enterprise) that will be used for this customer. The Small Business plan is included at no charge for all Customers, but selecting any other available plan requires a yearly fee.

After selecting the features you want to use, select **Save** in the bottom-right corner to complete adding the new Customer to your account and return to the Dealer Homepage.

1.3 Editing Existing Customers

If needed, you can edit Customer details by selecting **System Settings** in the Customer's Dashboard.

Additionally, once a Customer Account has been created, you can configure it as a Demo account by enabling the toggle switch in the **Demo System** section.

1.0 Dealer Homepage

Customer ID

System ID

System Name

Northwest Trust

Description

Industry *

Make a selection

▼

If Other, please specify

Install Type *

Make a selection

▼

[Learn more about customer details](#)

Save Changes

1.4 Deleting Customers

In **System Settings**, you can delete a customer or system under the **System Management** section.

NOTE: Deleting the selected customer permanently deletes all data and makes it unrecoverable; use caution.

1.0 Dealer Homepage

Delete System?

Do you wish to delete this System? This action is permanent and cannot be undone.

In order to delete this System, confirm this action by typing **DELETE Northwest Trust** in the field below.

CancelDelete System

1.5 Adding a Permission

To add a new **Permission** to your **Dealer Account**, in the **Permission** tab in your **Dealer Dashboard**, select the **+ Add Permission** button. Then you can enter the information for the new **Permission**. A **Permission Role** granted at the **Dealer** level provides that Permission Role to all **Customer Accounts** for the Dealer Account.

Home > Top Tier Security

Top Tier Security

+ Add Permission

Customers Permissions Integrations Settings Billing

Search permissions...

Integrator @prodatakey.com

Integrator @prodatakey.com

Admin @prodatakey.com

Reporter @prodatakey.com

In the **Add Permission** dialog, enter the Partner's email address, the Permission level, and the Billing Role (if any) to be assigned to them.

Add Permission

Add a permission to give users specific access and control within the system. Assign the right level to ensure they can manage tasks based on their role.

Email

Role

Billing Role

Cancel

Add

Email - Enter the **Email Address** for the **Permission**.

Role - Select to view the list of **Permission Roles** and select the appropriate **Permission Role** for the Partner.

Billing Role - A **Dealer Partner** can be assigned one of three Billing Roles, as detailed below. This field will only be visible to a **Dealer Partner**.

- **None** - The Dealer Partner will not have access to any Billing information for the Dealer Account.
- **Billing Admin** - The Dealer Partner has full access to all Billing functions for the Dealer Account.
- **Billing Reporter** - The Dealer Partner can review Billing invoices.

1.0 Dealer Homepage

After entering the **User Email** and **Role**, select **Add** to finalize adding the **Permission** to the **Dealer Account**. An invitation email will then be sent to the **User Email** with instructions to activate the **Permission**.

Until the **Permission** has been activated by the **Dealer Partner**, the Partner will be displayed as **(Invitation Pending)** in **Permissions**, rather than the Partner's name.

1.6 Editing or Deleting an Existing Permission

For **Permissions** added to a **Dealer Account**, selecting the user's name opens a drawer displaying the user's details and allows a Partner with a higher **Permission Role** to delete the **User** or edit the **Permission Role**. The **Name**, **Email**, **Phone Number**, **Company Name**, and **Title** will be displayed but cannot be changed.

To delete a **Permission**, select the **Delete Permission** button located in the lower left corner of the drawer.

← Permission

Permissions provide the authorization needed for users to manage systems within an organization. In this context, permissions are pdk.io users, not credential holders within the access control system.

Name

John Doe

Email

@prodatakey.com

Phone Number

Company Name

PDK

Title

PDK

Role

Integrator

Billing Role

Billing Admin

 Delete Permission

Cancel

Save Changes

1.0 Dealer Homepage

1.7 Integrations List

The Integrations tab shows the complete list of **Integrations** that can be activated on Customer Accounts.

Top Tier Security

Customers Permissions **Integrations** Settings Billing

All ▾

All Integrations

PDK integrates with a variety of third-party platforms to give you more flexibility and control. Use this dashboard to decide which integrations are visible to your customers and learn more about how each one works.

 **AEGIX** Visible

Automatically trigger a lockdown when an emergency is initiated from AEGIX.

[Learn More](#)

 **AccessGrid** Visible

Automatically issue Apple Wallet and Google Wallet NFC credentials for compatible AccessGrid readers.

[Learn More](#)

 **AccessIQ** Visible

Synchronize users and allow residents to access common areas from the AccessIQ mobile app.

[Learn More](#)

Admin visibility and configuration settings for each Integration can be adjusted by selecting **Learn More**.

 **AEGIX**

Automatically trigger a lockdown when an emergency is initiated from AEGIX.

☒

Configurable By Admins

Controls whether this integration is configurable by admins.

☒

Visible To Admins

Customers can see this integration on their systems. 

Systems with AEGIX Enabled

Name	
 Northwest Trust	Go to System

1.0 Dealer Homepage

Each Integration will also indicate which Customers it has enabled.

1.8 Adding a Support Contact

Dealers can set a default point of contact for all their Customers and End Users to contact when they need support.

Name*

Provide at least one contact method. All fields are optional as long as one is filled.

Email

Phone Number

Support Button URL

Support Button Label

The URL must begin with "https://" or "http://"

Character Limit: 0/50

Contact Support Form

Allow users to fill out a form and send messages to Support Contact email?

Save

Mobile App Support Contact Setup

This information will be visible to end users in the **PDK Access App**. Please provide at least one contact method:

- **Name** (required)
- **Email Address**
- **Phone Number**
- **Support Button URL**
 - Create a form or survey for users to submit issues, then paste the link here
- **Support Button Label**
 - Customize the label (e.g., "Contact Support")

1.0 Dealer Homepage

NOTE: Admins can override the Dealer’s default **Support Contact** by configuring a customer-specific contact in **System Settings**.

1.9 Billing Dashboard

The Billing Dashboard enables Installation Partners to manage Billing Details, update Payment Methods, and view Invoice History.

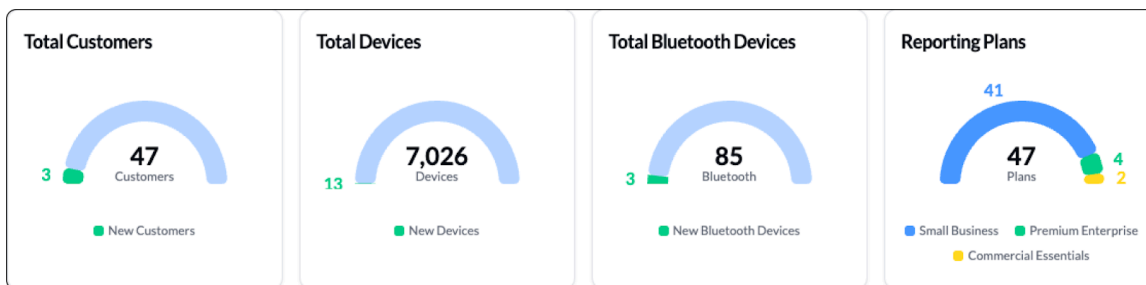


To access the **Billing Dashboard**, navigate to the **Dealer Homepage** and select **Billing**.

Platinum	Partner Status 
Gold	Partner Status 
Certified	Partner Status 
Non-Certified	Partner Status 

1.0 Dealer Homepage

1.9.1 Overview



The **Overview** section gives you a quick snapshot of your account. It shows your **Partner Status** (Platinum, Gold, Certified, or Uncertified) and provides a clear breakdown of your **Customers**, **Devices**, and **Bluetooth Devices**, including **New** and **Total** counts.

You'll also see details about which **Reporting Plans** are being used, such as Small Business, Commercial Essentials, or Premium Enterprise. To help you stay on top of **Billing**, the overview includes your **Recent Invoices** with Customer name, Invoice Number, Invoice Date, Invoice Amount, and Invoice Details. It also highlights **Upcoming Renewals**, so you always know what's coming next.

Recent Invoices		Upcoming Renewals		Month to Date	
Customer Name	Invoice Number	Invoice Date ↑	Invoice Amount	Invoice Details	
Blue Line Access	FED015E5-2497	08/18/2025	\$	-	↓
Early Motors	FED015E5-2510	08/18/2025	\$	3 Doors	↓
RMT Samples	FED015E5-2495	08/10/2025	\$	93 Doors	↓
Midwest Enterprises	FED015E5-2489	08/05/2025	\$	19 Doors	↓
Northwest Trust	FED015E5-2466	08/02/2025	\$	7 Doors	↓

Showing 1 - 5 of 5 invoices

Previous Next

1.0 Dealer Homepage

You can filter **Recent Invoice** data by Month to Date, the Previous 30 days, 60 days, or 90 days, and download it by clicking anywhere on the invoice row. **Upcoming Renewals** display future invoices and can be filtered for the Next 30, 60, or 90 days.

1.9.2 Subscriptions

Customer Name ↓	Renewal Date	Subscription Status	Price per Door	Doors/Devices	Bluetooth Devices	Billing Plan	
Blue Line Access	04/30/2027	Active	\$	7	0	Certified	
Invoice Number	Invoice Date	Invoice Amount	Paid/Unpaid	Payment Method Charged			
0C5F966-0009	04/30/2026	\$	Paid	Visa ••••			

The Subscriptions section makes it easy to view all Customer Subscriptions along with their related Invoice data. Here you can **Search** for a Customer and **Download** a Summary of *all* Customer Invoices. You can also sort the table columns in ascending or descending order by Customer Name, Renewal Date, Price per Door, number of Doors or Devices, Bluetooth Devices, or Billing Plan.

At the individual **Customer level**, click the **Download** button to download all invoices for that Customer. To view specific Invoice details, click the arrow icon to expand the record. Each expanded Invoice includes a downloadable PDF of the **Invoice** and its **payment receipt**, along with the invoice status: **Paid** or **Unpaid**.

NOTES:

- When a new Customer Account is registered, the system automatically generates a complimentary five-day trial invoice. The system does not send this invoice to the Installation Partner.
- If a Dealer is not following standard pricing, the **Billing Plan** will display as **Custom**.

1.9.3 Info

Billing Contact Information

 **Billing Contact Information**  Edit

No Billing Contact Info
There is no billing contact info associated with your account.

 **Payment Information**  Add Payment Method

 Mastercard
**** 

Update your **Billing Contact details** and manage **Payment methods**.

 **Edit Billing Contact Info**

Contact Name

Email

Phone

Address

City

Postal Code

State

Country

1.0 Dealer Homepage

Manage your **Billing Contact** details here, including:

- **Contact Name**
- **Email**
- **Phone Number**
- **Billing Address**

Payment Information

Add Payment Method

 Card

 Google Pay

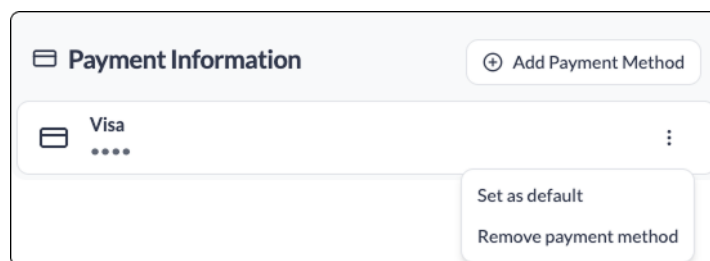
CancelSave

Add and manage **Payment Methods**:

- **Card**
- **Google Pay**

NOTE: You can set a Payment Method as the **Default** or **Remove It**.

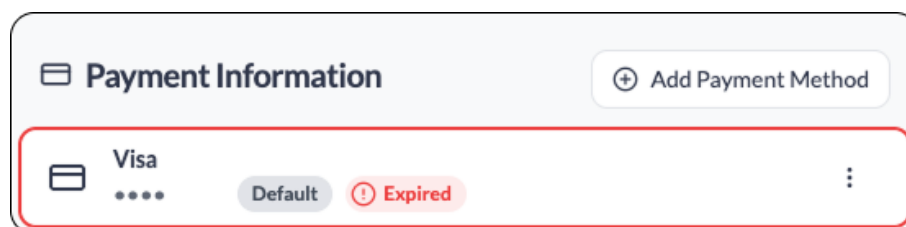
1.0 Dealer Homepage



Expired Payment Methods

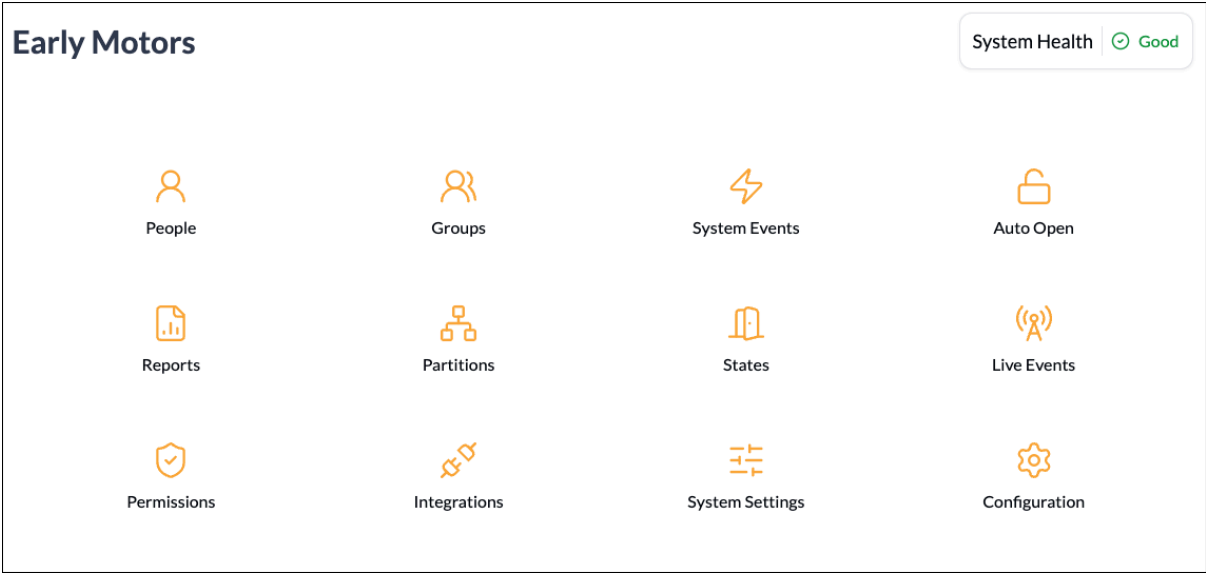


If your Default payment method has expired, you will see a notification at the top of your **Dealer Homepage**. You will also see expired payments in the **Payment Information** section.



2.0 Customer Dashboard

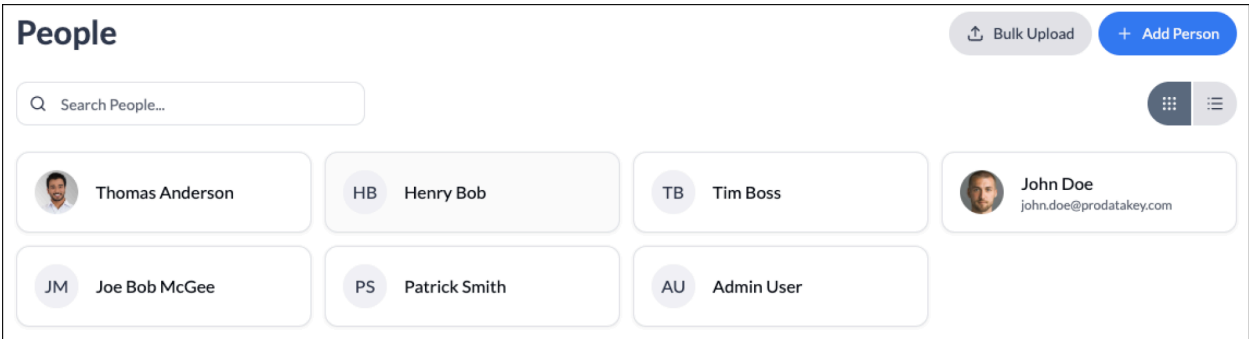
When opening a Customer, the main window, the **Customer Dashboard**, is displayed.



In the upper-right corner of the **Customer Dashboard**, an indicator shows the current **System and Health** status. Selecting the **System and Health** status opens the **System and Health** page.

Selecting each icon takes you to a different page in the software, where you can configure various parts of the system.

2.1 People



2.0 Customer Dashboard

After adding one or more People to the Cloud Node system, they will be listed in alphanumeric order. You can also find a Person using the search bar above the People list.

2.1.1 Adding A Single Person

To add a new Person to the Customer Account, select + **Add Person** in the **People** window. This opens a drawer where you can enter the new **Person's** information.

When creating a new Person on a Customer Account, you are required to enter the **First Name** and **Last Name** of the Person. All other fields are optional.

Add Person

Add a person to the system and set their credentials, access rights, and more.

First Name *	Last Name *
Email Address	Active Date
Expire Date	
	+ Add Custom Field
Access Status ⓘ	
☒ Enabled ☐ Disabled	

Partition - If the **Person** will be assigned to a specific partition, select the **Partition** dropdown to select a listed Partition. The Partition field appears only if partitions beyond the **Default Partition** have been created.

First Name - Enter the first name of the Person.

Last Name - Enter the last name of the Person.

2.0 Customer Dashboard

Email Address - Enter an email address for the person to use **Digital Credentials**.

Active Date - Select to open a calendar for when the Person's credentials will automatically become active.

Expire Date - Select to open a calendar for when the Person's credentials will automatically become inactive.

Custom Field - If Custom Fields are used, you can create or manage them here.

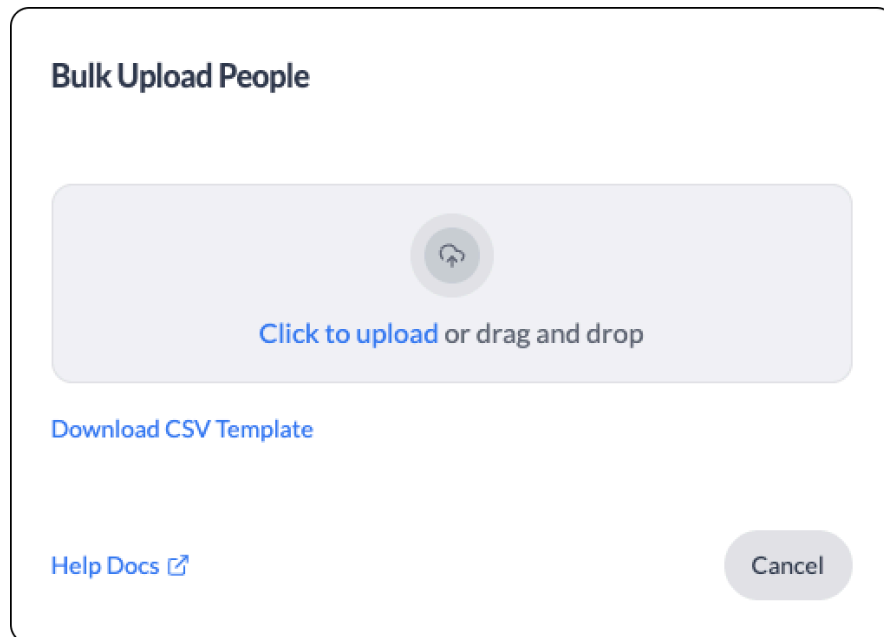
Access Status - This setting lets you set whether the Person is active (Enabled) or inactive (Disabled) upon creation.

2.1.2 Bulk Uploading Users

The **Bulk Upload** feature allows you to add, edit, or remove multiple users at once in your Customer Account by uploading a CSV file.

 Bulk Upload

When you select **Bulk Upload**, a dialog box opens, allowing you to upload your CSV file. A downloadable template file is also available to help you get started.



2.0 Customer Dashboard

To download the template, select **Download CSV Template**. This file, named **import-people-template.csv**, is a CSV (comma-separated values) spreadsheet. After you populate the template, select or drag and drop the file. Select the appropriate Partition to import the records.

Bulk Upload People

 Bulk Upload.csv
56 B

Partition
Default

☒ Allow import to update or overwrite records

[Help Docs](#) 

Cancel Upload

To update existing records, check the **Allow import to update or overwrite records** box. This enables the system to modify, replace, or delete existing People during the import.

After you upload the file, a progress screen will appear. If there are any errors in your file, you'll be shown which rows were skipped. The system will generate a downloadable CSV error report that explains the issues for each failed row.

 Bulk Upload.CSV
365 B
Imported at 8/5/2026, 12:56:27 PM by Jane Doe
2 people added, 0 people updated, 0 people deleted
2 rows skipped  [Download issues file](#)

Dismiss Go to People

2.0 Customer Dashboard

NOTE: The Bulk Import function is ideal when you need to add a large number of People and their credentials at once. If a Group specified in the import file does not already exist on the Customer Account, it will be created automatically, and the listed individuals will be added to that group.

2.1.3 Editing the Details of a Person

To edit the **Details** of a **Person** on a **Customer Account**, first select the **Name** of the **Person** in the **People** window. This will display a drawer with information about the **Person**. Select the field that needs to be updated, then select **Save** after the necessary changes have been made.

←

JD

John Doe

Enabled

↗

First Name *

John

Last Name *

Doe

Email Address

john@prodatakey.com

Active Date

09/01/2026, 00:00:00

×

Expire Date

+

Add Custom Field

Access Status ⓘ

Enabled

Disabled

Cancel

Save

2.1.4 Adding a Credential to a Person

This section of the drawer displays existing **Credentials** and lets you add new **Credentials** to the Person. Each existing Credential appears as an individual item in the Credentials section of the drawer menu. When adding a new **Credential** to a **Person**, **Cards**, or **PINs** are always available. You can select **Digital Credentials** only if you have previously entered an email address for the Person.

Add Credential

☐ Card

☐ PIN

☐ Duress PIN

☐ Digital ⓘ

Cancel

Submit

To add a **Credential** to the selected **Person**, select **+ Add Credential** and then select the type of **Credential**.

- **Card** - When adding a **Card Credential** to a **Person**, the **Credential** number associated with the physical **Credential** must be entered. Additionally, you can enter a Facility Code if Facility Codes are used on the Customer Account, and you can also enter an optional **Description** for the **Credential**.

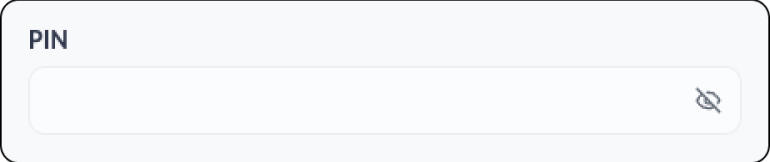
Card Number ⓘ

Facility Code (optional)

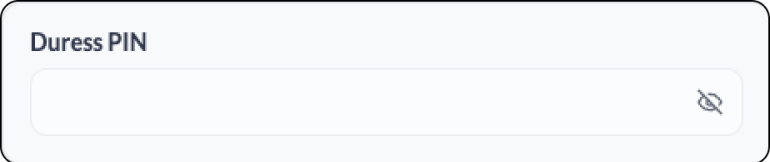
Description (optional)

2.0 Customer Dashboard

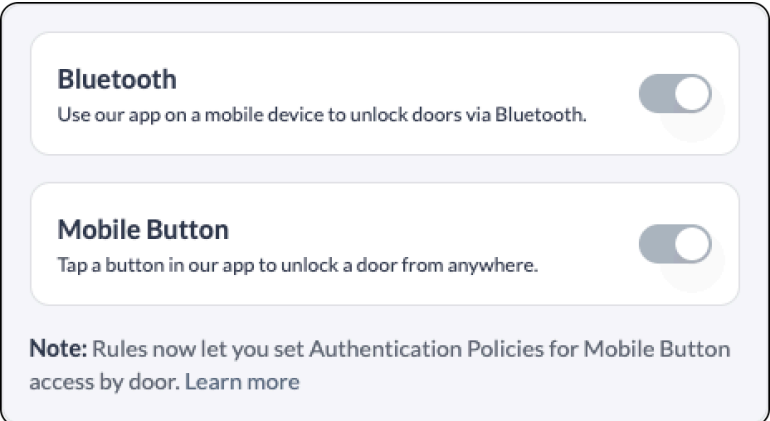
- **PIN** - When adding a **PIN** to a **Person**, if the Customer Account includes any keypad readers, enter a unique PIN

A light gray rounded rectangular box containing the label "PIN" in bold at the top left. Below the label is a white input field with a light gray border. To the right of the input field is a small circular icon with a diagonal slash through it, indicating a password or PIN field.

- **Duress PIN** - When adding a **Duress PIN** to a **Person**, if the Customer Account includes any keypad readers, enter a unique Duress PIN

A light gray rounded rectangular box containing the label "Duress PIN" in bold at the top left. Below the label is a white input field with a light gray border. To the right of the input field is a small circular icon with a diagonal slash through it, indicating a password or PIN field.

- **Digital** - When adding a Digital Credential to a Person, the option to add Bluetooth and/or Mobile Button Credentials is available. **Bluetooth** is used with PDK Red-series readers that support Bluetooth. The **Mobile Button** allows a PDK Access App user to open a door/device, regardless of reader type.

A light gray rounded rectangular panel containing two toggle switches. The first toggle is labeled "Bluetooth" in bold, with the text "Use our app on a mobile device to unlock doors via Bluetooth." below it. The second toggle is labeled "Mobile Button" in bold, with the text "Tap a button in our app to unlock a door from anywhere." below it. At the bottom of the panel is a **Note:** "Rules now let you set Authentication Policies for Mobile Button access by door. Learn more".

Bluetooth

Use our app on a mobile device to unlock doors via Bluetooth.

Mobile Button

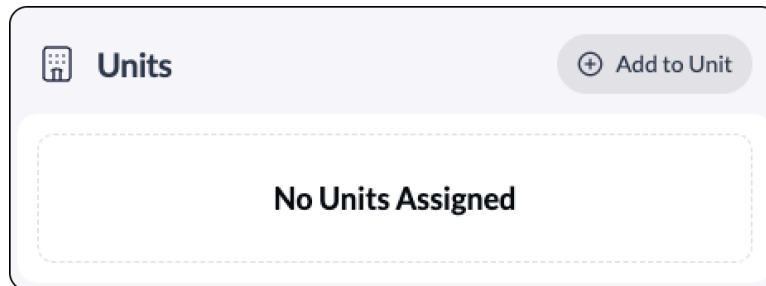
Tap a button in our app to unlock a door from anywhere.

Note: Rules now let you set Authentication Policies for Mobile Button access by door. [Learn more](#)

2.0 Customer Dashboard

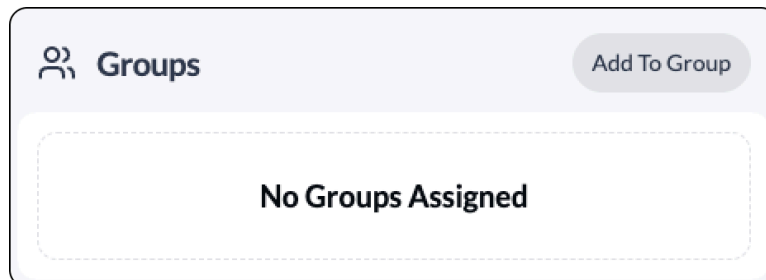
To delete a Credential that was added to a Person, select the garbage can icon located to the right of the Credential details. A pop-up dialog box will then appear, prompting the user to confirm the deletion of the Credential.

2.1.5 Adding a Person to a Unit



To add a Person to a residential Unit, select **+ Add to Unit**.

2.1.6 Adding a Person to a Group



To add a Person to a Group for a shared ruleset, select **+ Add to Group**

2.1.7 Adding a Rule to a Person

Add Rule

Access

Elevator

Event

Anti-Passback

Schedule

Always

Devices

No Devices

Edit Devices

Action

Allow

Deny

Primary Authentication Policy

Select one or more credential types. Secondary Policy is available only with Card or Bluetooth.

☐ Card or Bluetooth

☐ PIN

☐ Mobile Button

Cancel

Submit

To create a **Rule** (**Access**, **Event**, **Elevator**, or **Anti-Passback**) that applies only to the selected **Person**, select + **Add Rule**.

Editing an Access Rule

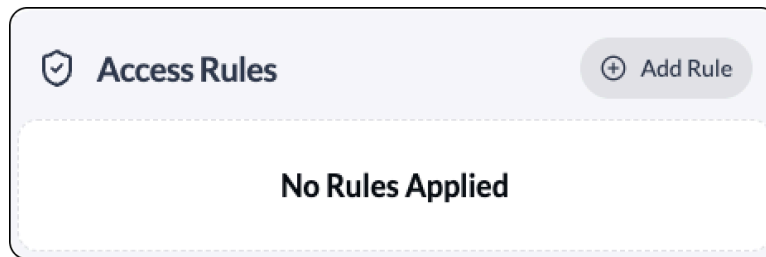
After you create an **Access Rule**, selecting its name opens a drawer where you can edit the details above.

Deleting an Access Rule

To delete an existing **Access Rule**, open the **Access Rule** drawer and select **Delete Rule** in the lower-left corner.

Access Rules

To create an **Access Rule**, select **+ Add Rules** in the **Access Rules** section of the drawer. This can be created for a **Person** or a **Group**.



By default, the **Access** tab will be selected.



Select the **Schedule** field and choose the appropriate option (**Always**, **Recurring**, **Single Date**). Each **Schedule** option will be outlined separately below.

After configuring the **Access Rule** as detailed below, select **Submit** in the lower right corner of the drawer to save the new **Access Rule**.

Creating an Always (24-hour) Access Rule

← Add Rule

Access Elevator Event Anti-Passback

Schedule

Always

Devices

No Devices

Edit Devices

Action

Allow Deny

Primary Authentication Policy

Select one or more credential types. Secondary Policy is available only with Card or Bluetooth.

☐ Card or Bluetooth ⓘ

☐ PIN

☐ Mobile Button

Cancel

Submit

Schedule - The rule will always be processed.

Schedule

Always

Devices - Select the **Devices** to include in the **Access Rule** by selecting **Edit Devices**.



The screenshot shows a rectangular box with a light gray background. Inside the box, the word "Devices" is displayed in a bold, dark gray font. Below it, the text "No Devices" is shown in a lighter gray font. In the bottom right corner of the box, there is a rounded rectangular button with a light gray background and the text "Edit Devices" in a dark gray font.

Action - The **Action** option specifies whether the **Access Rule** allows or denies access to the **Doors/Devices** it contains.

Allow - Will **Allow** access to the specified **Door/Devices** for the **Person**. This is the default state for this option.

Deny - Will **Deny** access to the specified **Door/Devices** for the **Person**.



The image shows two side-by-side rectangular boxes, each representing the "Action" toggle switch. Each box has a title "Action" at the top. Below the title is a horizontal toggle switch. The left box shows the "Allow" option selected, with the "Allow" button highlighted in dark blue and the "Deny" button in light gray. The right box shows the "Deny" option selected, with the "Deny" button highlighted in dark blue and the "Allow" button in light gray.

Authentication Policy - The **Authentication Policy** determines which Credential types are required to gain access.

Primary Authentication Policy
Select one or more credential types. Secondary Policy is available only with Card or Bluetooth.

☐ Card or Bluetooth ⓘ 

☐ PIN 

☐ Mobile Button 

Secondary Authentication Policy
This option is available when Card or Bluetooth is selected as the Primary Authentication Policy. When enabled, the user must enter a PIN after presenting the Primary Credential.

☐ PIN 

Primary Authentication Options:

You must select at least one **Primary Authentication Policy**:

- **Card or Bluetooth:** Requires a physical card or a Bluetooth credential via the PDK Access App.
- **PIN:** Requires entering a PIN on a reader keypad.
- **Mobile Button:** Requires tapping the Door name in the PDK Access App.

Secondary Authentication Policy (Optional):

The **Secondary Authentication Policy** adds an extra layer of security.

- **PIN:** If the **Primary Authentication Policy** is set to **Card or Bluetooth**, you can require a **PIN** as a second step. The user must scan their credential *and then* enter their PIN.

Important Note: If an **Authentication Policy** is set for the **Device** in **Configuration**, it may conflict with the selected **Authentication Policy** and cause credentials to function improperly. We recommend setting this during **Access Rule** creation.

Adding a Recurring Access Rule

←

Add Rule

Access

Elevator

Event

Anti-Passback

Schedule

Recurring

Days

S

M

T

W

T

F

S

Begin

🕒 00:00:00

End

🕒 24:00:00

Devices

No Devices

Edit Devices

Action

Allow

Deny

Primary Authentication Policy

Select one or more credential types. Secondary Policy is available only with Card or Bluetooth.

☐ Card or Bluetooth ⓘ

☐ PIN

☐ Mobile Button

Cancel

Submit

2.0 Customer Dashboard

Schedule - The rule will be processed only during the selected time frame each week.

Days - Select the days of the week the rule will be processed. By default, Monday-Friday are selected.

Begin - Select the specified time (in 24H format) when the **Access Rule** will begin.

End - Select the specified time (in 24H format) when the **Access Rule** will end.



The screenshot shows a configuration panel titled "Schedule". At the top, there is a dropdown menu set to "Recurring". Below this, under the heading "Days", there are seven circular buttons labeled S, M, T, W, T, F, and S. The buttons for M, T, W, T, and F are filled with a dark blue color, while the S buttons are white with a grey border. Under the heading "Begin", there is a text input field with a clock icon on the left and the value "00:00:00". Below that, under the heading "End", there is another text input field with a clock icon on the left and the value "24:00:00".

Devices - Select the **Devices** to include in the **Access Rule** by selecting **Edit Devices**.



The screenshot shows a configuration panel titled "Devices". Below the title, the text "No Devices" is displayed. In the bottom right corner, there is a rounded rectangular button with the text "Edit Devices".

Action - The **Action** option specifies whether the **Access Rule** allows or denies access to the **Doors/Devices** it contains.

Allow - Will **Allow** access to the specified **Door/Devices** for the **Person**. This is the default state for this option.

Deny - Will **Deny** access to the specified **Door/Devices** for the **Person**.



Authentication Policy - The **Authentication Policy** determines which Credential types are required to gain access.

Primary Authentication Policy
Select one or more credential types. Secondary Policy is available only with Card or Bluetooth.

☐ Card or Bluetooth ⓘ 

☐ PIN 

☐ Mobile Button 

Secondary Authentication Policy
This option is available when Card or Bluetooth is selected as the Primary Authentication Policy. When enabled, the user must enter a PIN after presenting the Primary Credential.

☐ PIN 

Primary Authentication Options:

You must select at least one **Primary Authentication Policy**:

- **Card or Bluetooth:** Requires a physical card or a Bluetooth credential via the PDK Access App.
- **PIN:** Requires entering a PIN on a reader keypad.
- **Mobile Button:** Requires tapping the Door name in the PDK Access App.

Secondary Authentication Policy (Optional):

The **Secondary Authentication Policy** adds an extra layer of security.

- **PIN:** If the **Primary Authentication Policy** is set to **Card or Bluetooth**, you can require a **PIN** as a second step. The user must scan their credential *and then* enter their PIN.

2.0 Customer Dashboard

Important Note: If an **Authentication Policy** is set for the **Device** in **Configuration**, it may conflict with the selected **Authentication Policy** and cause credentials to function improperly. It is recommended to set this during **Access Rule** creation.

Creating a Single Date Access Rule

Add Rule

Access

Elevator

Event

Anti-Passback

Schedule

Single Date

Date

Select a date

Begin

00:00:00

End

24:00:00

Devices

No Devices

Edit Devices

Action

Allow

Deny

Primary Authentication Policy

Select one or more credential types. Secondary Policy is available only with Card or Bluetooth.

☐ Card or Bluetooth

☐ PIN

☐ Mobile Button

Cancel

Submit

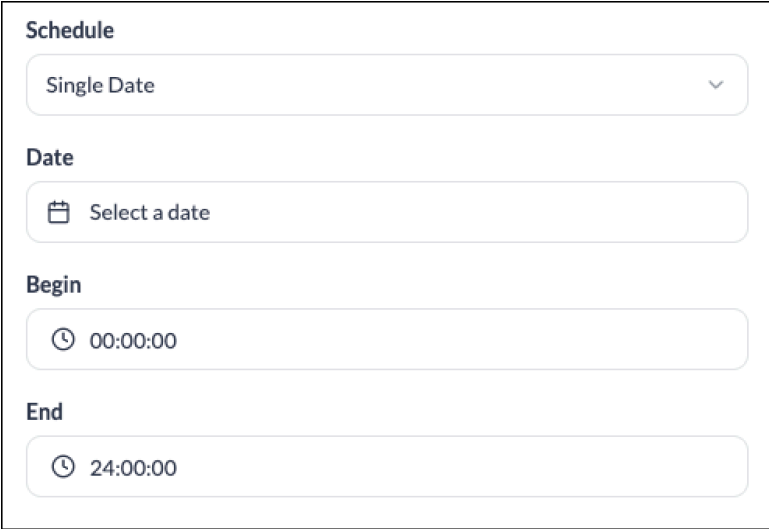
2.0 Customer Dashboard

Schedule - The rule will only be processed for the specified timeframe on a **Single Day**.

Date - Select the date when the rule will be processed.

Begin - Select the specified time (in 24H format) when the **Access Rule** will begin.

End - Select the specified time (in 24H format) when the **Access Rule** will end.



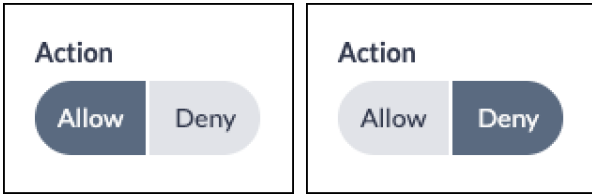
The screenshot shows a configuration form for an Access Rule. It contains four sections: 'Schedule' with a dropdown menu set to 'Single Date'; 'Date' with a calendar icon and the text 'Select a date'; 'Begin' with a clock icon and the time '00:00:00'; and 'End' with a clock icon and the time '24:00:00'.

Devices - Select the **Devices** to include in the **Access Rule** by selecting **Edit Devices**.

Action - The **Action** option specifies whether the **Access Rule** allows or denies access to the **Doors/Devices** it contains.

Allow - Will **Allow** access to the specified **Door/Devices** for the **Person**

Deny - Will **Deny** access to the specified **Door/Devices** for the **Person**.



The image shows two side-by-side screenshots of the 'Action' toggle switch. In the left screenshot, the 'Allow' button is dark blue and the 'Deny' button is light gray. In the right screenshot, the 'Allow' button is light gray and the 'Deny' button is dark blue.

Authentication Policy - The **Authentication Policy** determines which Credential types are required to gain access.

Primary Authentication Policy
Select one or more credential types. Secondary Policy is available only with Card or Bluetooth.

☐ Card or Bluetooth ⓘ 

☐ PIN 

☐ Mobile Button 

Secondary Authentication Policy
This option is available when Card or Bluetooth is selected as the Primary Authentication Policy. When enabled, the user must enter a PIN after presenting the Primary Credential.

☐ PIN 

Primary Authentication Options:

You must select at least one **Primary Authentication Policy**:

- **Card or Bluetooth:** Requires a physical card or a Bluetooth credential via the PDK Access App.
- **PIN:** Requires entering a PIN on a reader keypad.
- **Mobile Button:** Requires tapping the Door name in the PDK Access App.

Secondary Authentication Policy (Optional):

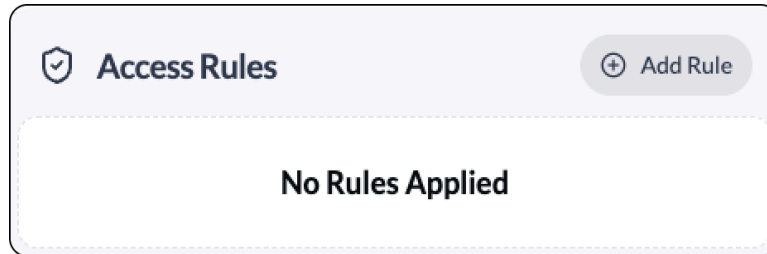
The **Secondary Authentication Policy** adds an extra layer of security.

- **PIN:** If the **Primary Authentication Policy** is set to **Card or Bluetooth**, you can require a **PIN** as a second step. The user must scan their credential *and then* enter their PIN.

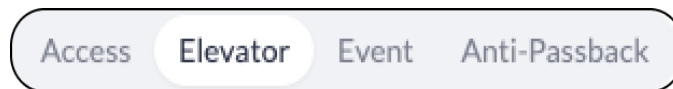
Important Note: If an **Authentication Policy** is set for the **Device** in **Configuration**, it may conflict with the selected **Authentication Policy**, causing **Credentials** to function improperly. It is recommended to set this during **Access Rule** creation.

Elevator Rules

To create an **Access Rule**, select **+ Add Rules** in the **Access Rules** section of the drawer. This can be created for a **Person** or a **Group**.



Select **Elevator**. By default, the **Access** tab will be selected.



Schedule - Select this dropdown to choose the **Schedule Type: Always, Recurring, or Single Date**.

Below is an explanation for each **Schedule** type and how to configure each option.

Always - The rule will always be processed.



Recurring - The rule will be processed only during the selected time frame each week.

Days - Select the days of the week on which the rule will be processed. By default, Monday-Friday are selected.

Begin - Select the specified time (in 24H format) when the **Elevator Rule** will begin.

End - Select the specified time (in 24H format) when the **Elevator Rule** will end.

Schedule

Recurring

Days

S

M

T

W

T

F

S

Begin

🕒 00:00:00

End

🕒 24:00:00

Single Date - The rule will only be processed for the specified timeframe on a single day.

Date - Select the date when the rule will be processed.

Begin - Select the specified time (in 24H format) when the **Elevator Rule** will begin.

End - Select the specified time (in 24H format) when the **Elevator Rule** will end.

Schedule

Single Date

Date

📅 Select a date

Begin

🕒 00:00:00

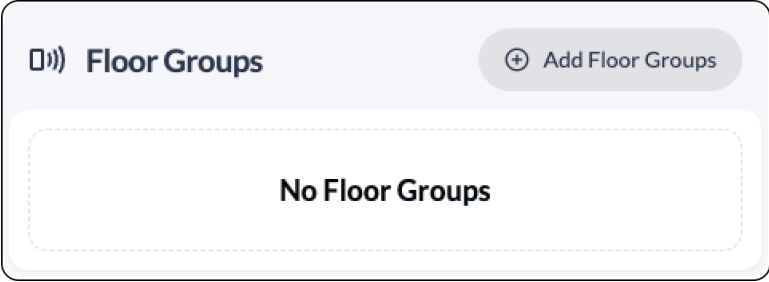
End

🕒 24:00:00

Floor Groups - Select the configured **Elevator Floor Group**.

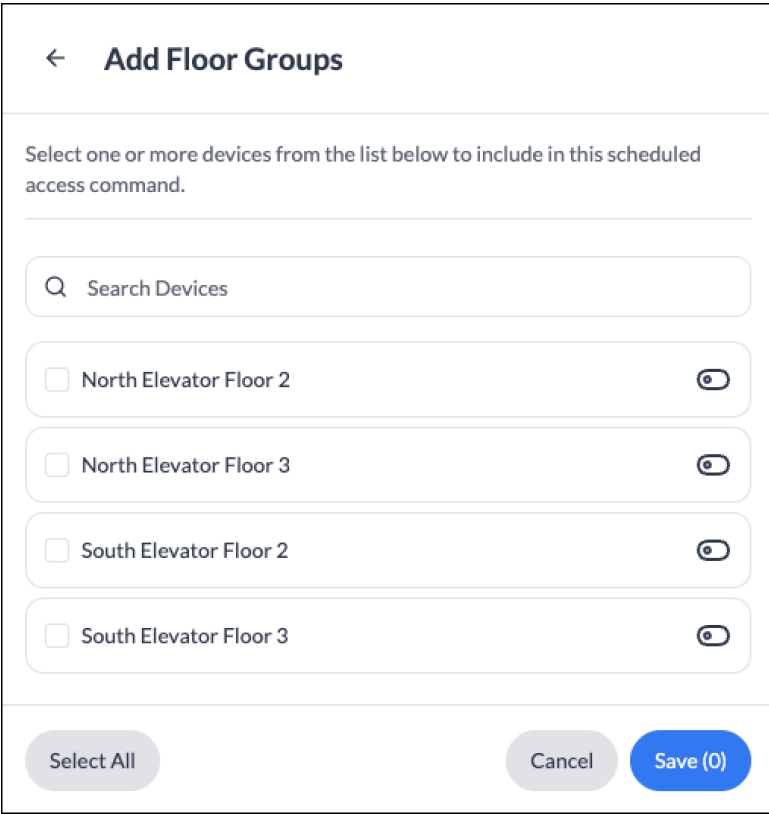
2.0 Customer Dashboard

Select at least one **Floor Group** to save the **Rule**.



The interface shows a header with a list icon and the text "Floor Groups". To the right is a button labeled "Add Floor Groups". Below the header is a large dashed rectangular box containing the text "No Floor Groups".

Select **Edit Floor Groups** to highlight the specified **Floor Groups** and then **Save**.



The dialog has a title bar with a back arrow and the text "Add Floor Groups". Below the title bar is a message: "Select one or more devices from the list below to include in this scheduled access command." Underneath is a search bar with a magnifying glass icon and the placeholder text "Search Devices". Below the search bar is a list of four items, each with a checkbox on the left and a toggle switch on the right:

- ☐ North Elevator Floor 2
- ☐ North Elevator Floor 3
- ☐ South Elevator Floor 2
- ☐ South Elevator Floor 3

At the bottom of the dialog are three buttons: "Select All", "Cancel", and "Save (0)".

Authentication Policy - The **Authentication Policy** determines which Credential types are required to gain access.

Primary Authentication Policy
Select one or more credential types. Secondary Policy is available only with Card or Bluetooth.

☐ Card or Bluetooth ⓘ 

☐ PIN 

☐ Mobile Button 

Secondary Authentication Policy
This option is available when Card or Bluetooth is selected as the Primary Authentication Policy. When enabled, the user must enter a PIN after presenting the Primary Credential.

☐ PIN 

Primary Authentication Options:

You must select at least one **Primary Authentication Policy**:

- **Card or Bluetooth:** Requires a physical card or a Bluetooth credential via the PDK Access App.
- **PIN:** Requires entering a PIN on a reader keypad.
- **Mobile Button:** Requires tapping the Door name in the PDK Access App.

Secondary Authentication Policy (Optional):

The **Secondary Authentication Policy** adds an extra layer of security.

- **PIN:** If the **Primary Authentication Policy** is set to **Card or Bluetooth**, you can require a **PIN** as a second step. The user must scan their credential *and then* enter their PIN.

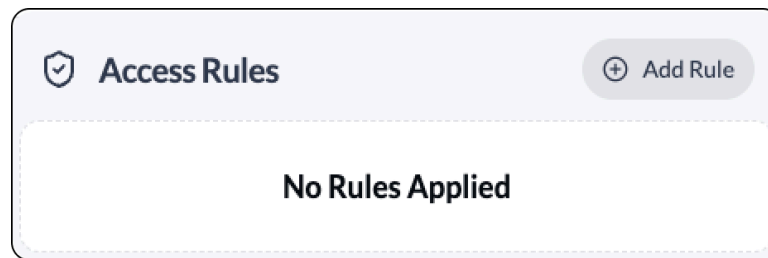
Important Note: If an **Authentication Policy** is set for the **Device** in **Configuration**, it may conflict with the selected **Authentication Policy** and cause Credentials to function improperly. It is recommended to set this during **Access Rule** creation.

After configuring the **Elevator rule**, select **Submit** to save the rule.

Event Rules

Event Rules allow an Action to be processed when a Person performs a specified action on the Cloud Node system.

To create an **Event Rule**, select **+ Add Rules** in the **Access Rules** section of the drawer. This can be created for a **Person** or a **Group**.



Select **Event**. By default, the **Access** tab will be selected.



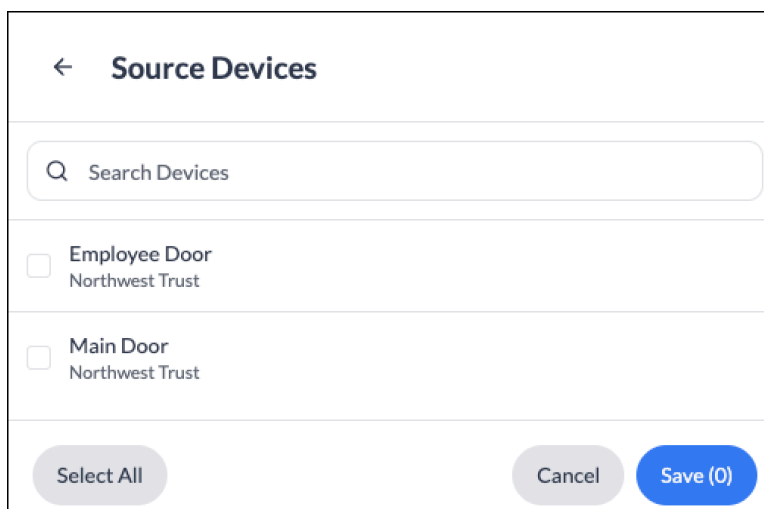
Name - Enter a unique, descriptive name for the **Event** rule.

Trigger - Select the **Trigger** field to select the Event result that will cause the rule to be processed.

Action - Select the **Action** field to select what will occur when the rule is processed.

An Event rule requires both a **Trigger** and an **Action** for the rule to be processed.

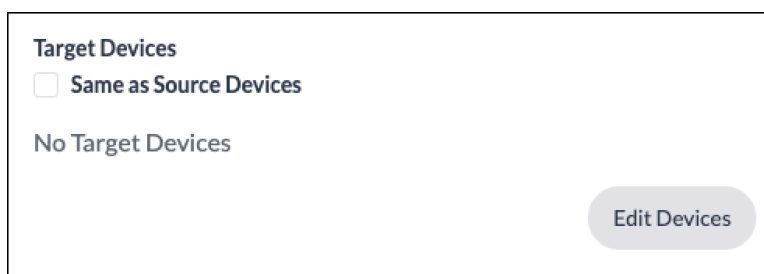
Source Device - Select **Edit Devices** to open the drawer where you can select the **Device** where the selected **Trigger** event will occur. After selecting the chosen **Device**, select **Save**.



The screenshot shows a mobile interface titled "Source Devices" with a back arrow. Below the title is a search bar labeled "Search Devices". There are two list items, each with a checkbox and text: "Employee Door Northwest Trust" and "Main Door Northwest Trust". At the bottom, there are three buttons: "Select All", "Cancel", and "Save (0)".

Target Devices - The **Target Devices** option appears for all **Actions** except **Send Email** or **Push Notification**. Select **Edit Devices** to open the drawer where you can select the **Device** where the configured **Action** event will occur. After selecting the chosen **Device**, select **Save**.

- **Same as Source Devices** - When the **Target Device** is the same as the **Source Device**, select this option by selecting the checkbox.



The screenshot shows a mobile interface titled "Target Devices". It contains a checkbox labeled "Same as Source Devices". Below this, the text "No Target Devices" is displayed. At the bottom right, there is an "Edit Devices" button.

Schedule - Select this dropdown to choose the **Schedule Type**: **Always**, **Recurring**, or **Single Date**.

Below is an explanation of each **Schedule** type and how to configure it

Always - The rule will always be processed.



The screenshot shows a mobile interface with a dropdown menu titled "Schedule". The dropdown is currently set to "Always" and has a downward arrow icon on the right.

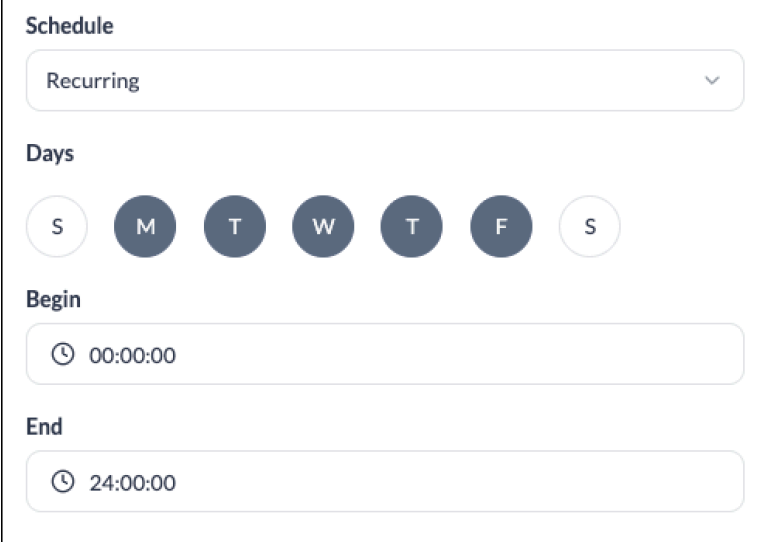
2.0 Customer Dashboard

Recurring - The rule will be processed only during the selected time frame each week.

Days - Select the days of the week the rule will be processed. By default, Monday-Friday are selected.

Begin - Select the specified time (in 24H format) when the **Access Rule** will begin.

End - Select the specified time (in 24H format) when the **Access Rule** will end.



The screenshot shows a 'Schedule' configuration form. At the top, there is a dropdown menu labeled 'Schedule' with 'Recurring' selected. Below this is a 'Days' section with seven circular buttons labeled S, M, T, W, T, F, and S. The buttons for M, T, W, T, and F are dark blue, while the S buttons are light gray. Below the days are two time selection fields. The first is labeled 'Begin' and shows a clock icon followed by '00:00:00'. The second is labeled 'End' and shows a clock icon followed by '24:00:00'.

Single Date - The rule will only be processed for the specified timeframe on a **Single Day**.

Date - Select the date when the rule will be processed.

Begin - Select the specified time (in 24H format) when the **Access Rule** will begin.

End - Select the specified time (in 24H format) when the **Access Rule** will end.

2.0 Customer Dashboard

Schedule

Single Date

Date

 Select a date

Begin

 00:00:00

End

 24:00:00

After configuring the **Event** rule, select **Submit** to save the rule.

Event Triggers

- **When Allowed** - This rule will be processed when a 'Credential Input' event produces an 'Access Allowed' result.
- **When Denied (Explicit)** - This rule processes when a Credential entry is denied because the door/device is in a Do Not Disturb state.
- **When Denied (No Rules)** - This rule processes when a Credential entry is denied because no Allow rule is configured for the timeframe when the credential was processed.
- **Always (Valid Credentials)** - This rule processes when any Credential is entered into the system, regardless of whether access is allowed or denied.
- **On Multiswipe Allow (# Swipe)** - This rule processes when a physical Credential is scanned a set number of times (2, 3, or 4) in rapid succession on a reader.
- **On Duress** - This rule processes when a Duress PIN is entered on a keypad reader.
- **On Anti-Passback Violation** - This rule processes when an Anti-Passback rule triggers a violation for the Person.

Event Actions

- **Send Email** - Selecting this action will allow an email or SMS text message to be sent to the specified email address(es) (or phone numbers) using the pre-configured email template.

- **Send Push Notification** - This action will send a Push Notification to a user with a configured Permission used to log in to Manage Access in the PDK Access App. Push Notifications will be displayed in the same manner as other app notifications on the mobile device.
- **Do Not Disturb** - This action toggles the Target door/device into the 'Do Not Disturb' state (if not in this state) or out of the 'Do Not Disturb' state (if in this state). While in the **Do Not Disturb** state, the door/device will be locked and access attempts will be rejected until the Do Not Disturb state is toggled/canceled.
- **Force Toggle** - This action toggles the current state of the relay for the Target door/device and maintains this new state until another Force Toggle command is sent. For example, if the Target door/device is unlocked/activated, a 'Force Toggle' command will lock/deactivate the door/device, and then further normal access attempts will be rejected until another Force Toggle command is sent.
- **Force Open** - This action sets the relay for the Target door/device to an unlocked/activated state and will remain in this state until a Force Toggle command is sent.
- **Force Close** - This action sets the relay for the Target door/device to a locked/deactivated state and will remain in this state until a Force Toggle command is sent.
- **Lockdown On** - This action toggles the Target door/device into a 'Do Not Disturb' state. While in the **Do Not Disturb** state, the door/device will be locked and access attempts will be rejected until the Do Not Disturb state is toggled/canceled.
- **Lockdown Off** - This action clears the 'Do Not Disturb' state on the door/device and returns it to its default state.
- **Open** - This action will unlock/activate the Target door/device until another command locks/deactivates the door/device, such as Close, Delay Close, and Open/Close.
- **Close** - This action will lock/deactivate the Target door/device until another command that will lock/deactivate the door/device, such as Open, Delay Close, and Open/Close.
- **Open/Close** - This action causes the Target door/device to unlock/activate, then lock/deactivate after the listed Dwell time.
- **Sound Piezo (OSDP Readers Only)** - This action will activate the Piezo speaker in a Red-reader that uses OSDP wiring.
- **Silence Piezo (OSDP Readers Only)** - This action deactivates the Piezo speaker in a Red reader that uses OSDP wiring.

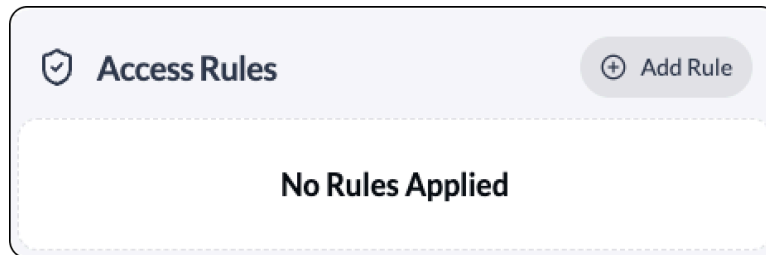
Anti-Passback Rules

Anti-Passback Rules define a specific sequence in which Credentials must be used and are most commonly used in areas with defined exits and entrances. While an Anti-Passback rule is active,

2.0 Customer Dashboard

the system requires that, for every allowed Credential entry by a Person at a designated entry device, there be a corresponding allowed Credential entry at an exit device before the Person can use their Credential at an entry device without an Anti-Passback Violation.

To create an **Anti-Passback Rule**, select **+ Add Rules** in the **Access Rules** section of the drawer. This can be created for a **Person** or a **Group**.



Select **Anti-Passback**. By default, the **Access** tab will be selected.



Schedule - Select this dropdown to choose the **Schedule Type: Always, Recurring, or Single Date**.

Below is an explanation for each **Schedule** type and how to configure each option.

Always - The rule will always be processed.



Recurring - The rule will be processed only during the selected time frame each week.

Days - Select the days of the week on which the rule will be processed. By default, Monday-Friday are selected.

Begin - Select the specified time (in 24H format) when the **Elevator Rule** will begin.

End - Select the specified time (in 24H format) when the **Elevator Rule** will end.

2.0 Customer Dashboard

Schedule

Recurring

Days

S

M

T

W

T

F

S

Begin

🕒 00:00:00

End

🕒 24:00:00

Single Date - The rule will only be processed for the specified timeframe on a single day.

Date - Select the date when the rule will be processed.

Begin - Select the specified time (in 24H format) when the **Elevator Rule** will begin.

End - Select the specified time (in 24H format) when the **Elevator Rule** will end.

Schedule

Single Date

Date

📅 Select a date

Begin

🕒 00:00:00

End

🕒 24:00:00

2.0 Customer Dashboard

Entry Devices - Select at least one Door or Device to function as an **Entry Device**; it will record that the Person has entered and that the Person needs to exit at an **Exit Device** to prevent an **Anti-Passback Violation**.

Select the **Devices** to include as the **Entry Device** by selecting **Edit Devices**.

A rectangular box representing a user interface for selecting entry devices. Inside the box, the text "Entry Devices" is displayed in a bold, dark font, and "No Entry Devices" is displayed below it in a lighter, gray font. In the bottom right corner of the box, there is a rounded rectangular button with the text "Edit Devices" in a dark font.

Exit Devices - Select at least one door or device to function as an **Exit Device**; it will record that the Person has 'exited' and that their credential can be scanned at an **Entry Device** without causing an **Anti-Passback Violation**.

Select the **Devices** to include as the **Exit Device** by selecting **Edit Devices**.

A rectangular box representing a user interface for selecting exit devices. Inside the box, the text "Exit Devices" is displayed in a bold, dark font, and "No Exit Devices" is displayed below it in a lighter, gray font. In the bottom right corner of the box, there is a rounded rectangular button with the text "Edit Devices" in a dark font.

NOTE: **Entry** and **Exit Devices** must be unique **Devices**.

Re-entry - The **Re-Entry** option specifies the behavior when an Anti-Passback rule violation occurs

Deny - When set to **Deny**, the Anti-Passback rule will consider any Credential entry by the violating Credential as occurring during a "**Deny Explicit**" state on the selected **Entry Devices**. This prevents the violating Credential from accessing any **Entry Device** listed in the rule and generates an Anti-Passback Violation event.

Allow - When set to **Allow**, the **Anti-Passback** rule allows access to the listed **Entry Devices**, but generates an **Anti-Passback Violation** event.

2.0 Customer Dashboard

Violation Expiration - The **Violation Expiration** option specifies the duration for which an Anti-Passback rule violation will persist for a violating Credential. Select this dropdown to choose the Violation Expiration: **Never**, **1 Hour**, **24 Hours**, or **Custom**.

Never - Anti-passback restrictions generated by this rule will remain active for the person until a Credential for that Person is used on an **Exit Device** or the restriction for the Person is cleared.



A screenshot of a web form titled "Violation Expiration". It features a dropdown menu with the word "Never" selected. A small downward arrow is visible on the right side of the dropdown box.

1 Hour - Anti-passback restrictions generated by this rule will remain active for the person until a Credential for that Person is used on an **Exit Device**, the restriction for the Person is cleared, or one hour passes.



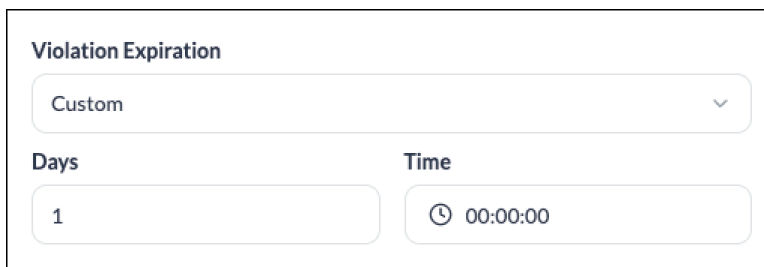
A screenshot of a web form titled "Violation Expiration". It features a dropdown menu with the text "1 Hour" selected. A small downward arrow is visible on the right side of the dropdown box.

24 Hours - Anti-passback restrictions generated by this rule will remain active for the person until a Credential for that Person is used on an **Exit Device**, the restriction for the Person is cleared, or twenty-four (24) hours pass.



A screenshot of a web form titled "Violation Expiration". It features a dropdown menu with the text "24 Hours" selected. A small downward arrow is visible on the right side of the dropdown box.

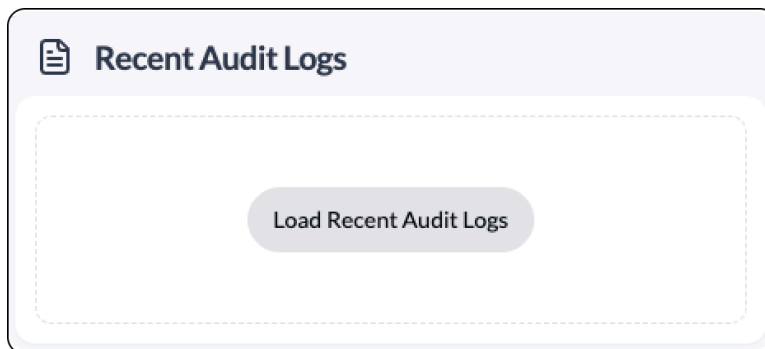
Custom - Anti-passback restrictions generated by this rule will remain active for the Person until a Credential for the Person is used on an **Exit Device**, the restriction for the Person is cleared, or the configured time has passed.



A screenshot of a web form titled "Violation Expiration". The dropdown menu has "Custom" selected. Below the dropdown, there are two input fields: "Days" with the value "1" and "Time" with a clock icon and the value "00:00:00".

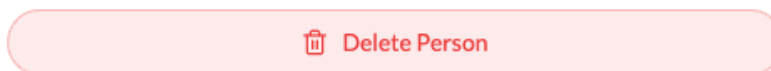
After configuring the **Anti-Passback rule**, select the **Submit** button to save the rule.

2.1.8 Recent Audit Logs



The **Recent Audit Log** only shows the 50 most recent events for the User. If you want additional logged entries, use the Reports function to view *all* logged events and modifications for a specific timeframe, by device name, specific People, etc.

2.1.9 Deleting a Person



To delete a Person, select **Delete Person** at the bottom of the Person record.

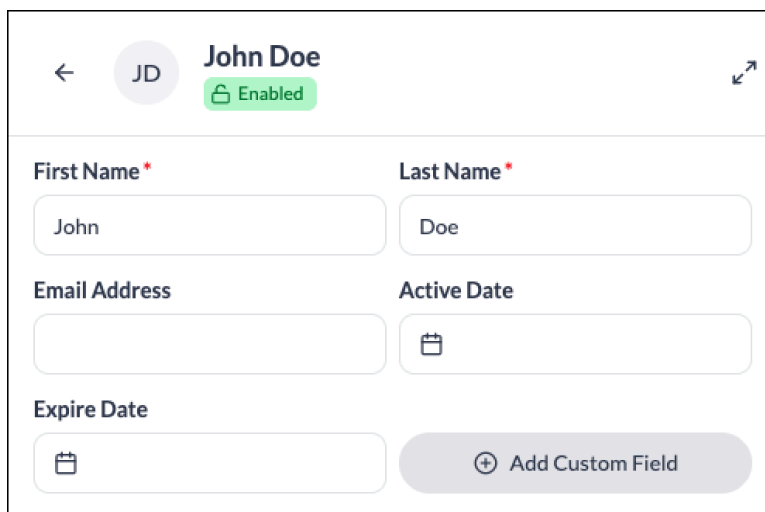
2.1.10 Adding a Photo to a Person



A picture or image can be added to a **Person's** details. This picture will be displayed alongside events featuring them in **Live Events**.

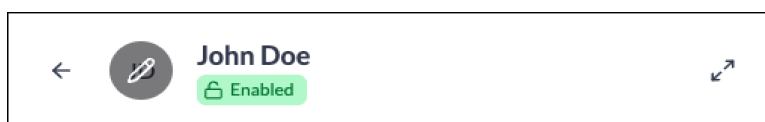
To add a photo to a person on a Customer Account, select the **Name** of the **Person** in the **People** window. This will display a drawer with their information.

2.0 Customer Dashboard



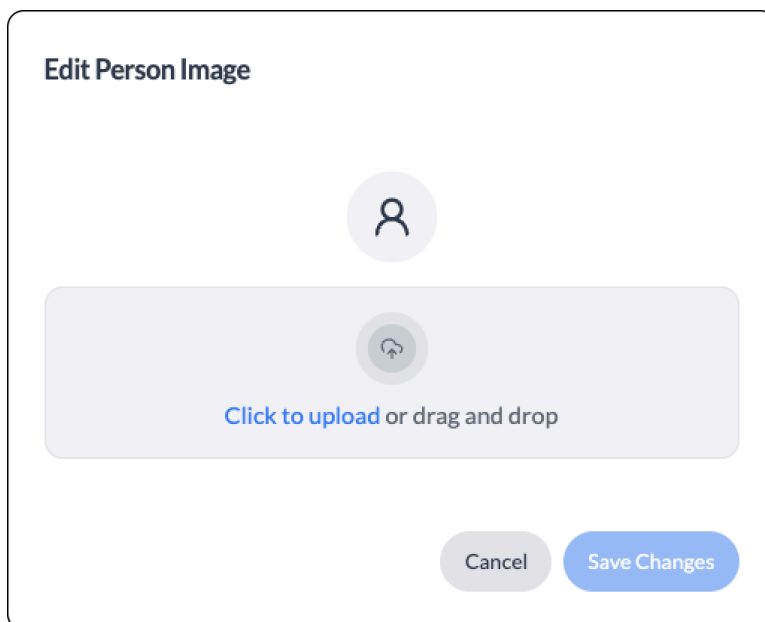
A user profile card for John Doe. At the top left is a back arrow and a circular avatar with initials 'JD'. To the right of the avatar is the name 'John Doe' and a green 'Enabled' status tag. At the top right is a full-screen icon. Below the header are two rows of form fields: 'First Name*' with 'John' and 'Last Name*' with 'Doe'. The next row has 'Email Address' (empty) and 'Active Date' (calendar icon). The bottom row has 'Expire Date' (calendar icon) and a grey button labeled '+ Add Custom Field'.

Hover over the user's initials to see a **pencil icon** to edit.



The same user profile card as above, but the circular avatar now contains a pencil icon, indicating it is editable.

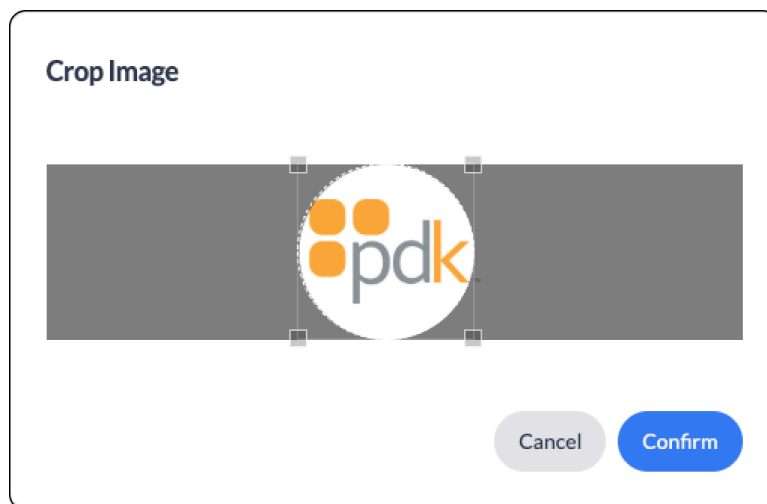
Select **Click to upload or drag and drop** the photo from your device.



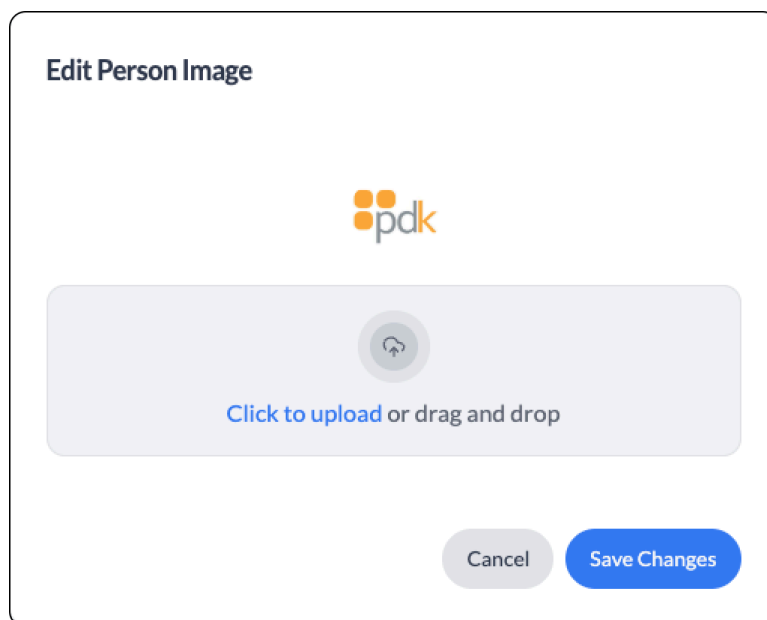
A modal dialog titled 'Edit Person Image'. It features a circular avatar with a person icon. Below the avatar is a large light-grey rectangular area containing a circular upload icon and the text 'Click to upload or drag and drop'. At the bottom right are two buttons: 'Cancel' and 'Save Changes'.

2.0 Customer Dashboard

Adjust the circle's size and position to crop the photo as needed. Then select **Confirm** to save the image.

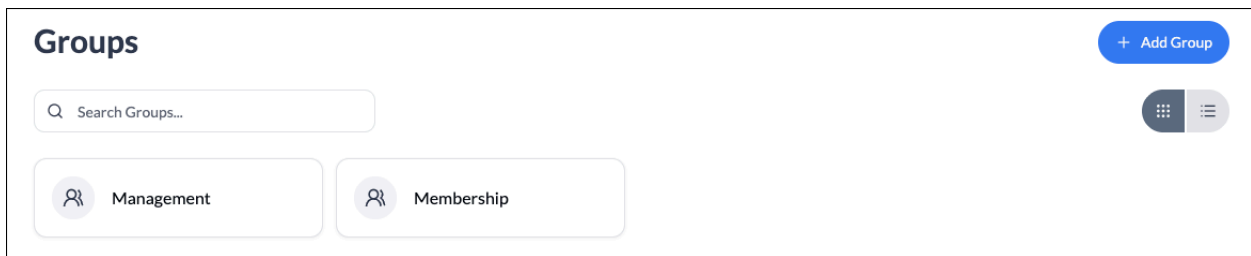


Select **Save Changes**.



2.2 Groups

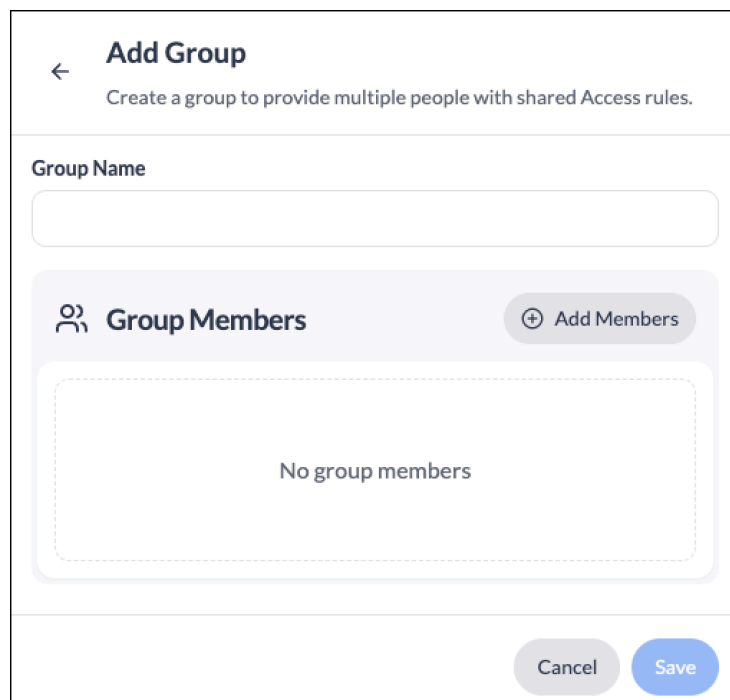
Selecting the **Groups** icon on the **Customer Dashboard** opens the **Groups** window. Using **Groups** allows a User with appropriate **Permissions** to provide a set of shared Access rules. By using a **Group** to manage **Access Rules** instead of assigning **Access Rules** directly to each Person on the Customer Account, any changes, such as creating new rules, updating existing rules, and removing rules, can be made to just the Group instead of having to make the change for each Person. You can also find a Group by using the search bar located above the Group list.



The screenshot shows the 'Groups' window. At the top left is the title 'Groups'. To the right is a blue '+ Add Group' button. Below the title is a search bar with the placeholder text 'Search Groups...'. At the bottom, there are two tabs: 'Management' (selected) and 'Membership'. The 'Management' tab shows a list of groups, currently empty.

2.2.1 Adding a New Group

To create a new **Group**, first select the **+ Add Group** button in the **Groups** window.

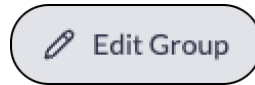


The screenshot shows the 'Add Group' form. At the top is a back arrow and the title 'Add Group'. Below the title is a subtitle: 'Create a group to provide multiple people with shared Access rules.' The form has a 'Group Name' input field. Below that is a section titled 'Group Members' with a '+ Add Members' button. The members list is currently empty, showing 'No group members'. At the bottom right are 'Cancel' and 'Save' buttons.

2.0 Customer Dashboard

After entering the **Group Name** for the new **Group** and adding Group Members, select the **Save** button in the lower-right corner of the window.

2.2.2 Edit Group



After a **Group** has been created, selecting the **Group's** name opens the Group's window. This menu displays the details of the Group and allows the following items to be done:

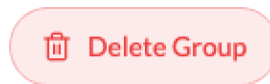
- Edit the Group name and Partition
- Delete the Group
- Adding/Editing/Deleting Access Rules
- Adding/Removing People from the Group
- Review recent events regarding People in the Group

To edit an existing **Group**, select the **Edit Group** button in the bottom right of the menu for the **Group**.

Group Name - Displays the Group's current name. Selecting this field lets you change the Group Name.

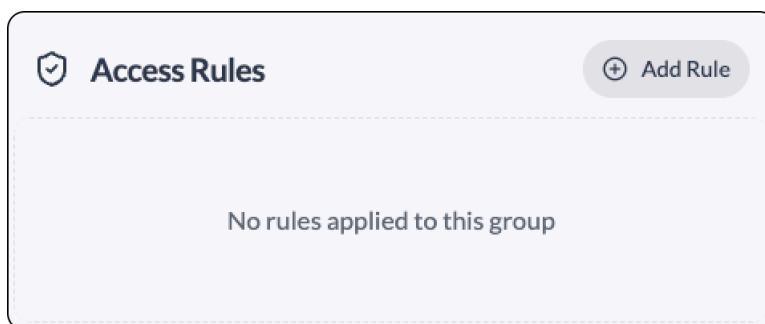
Partition - This feature lets you add the **Group** to a specific **Partition**, so designated Managers can manage it. This option is available only if you have created Partitions beyond the Default.

2.2.3 Delete Group



To delete a **Group** from the **Customer Account**, select **Delete Group**. This opens a dialog box warning you that this action will delete the selected Group and remove any Access Rules currently in place. This will not change the People or Devices assigned to the group.

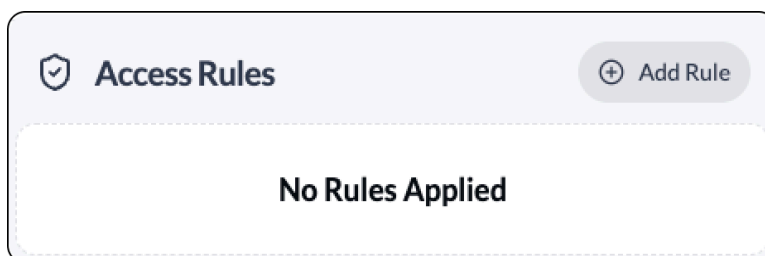
2.2.4 Adding a Rule to a Group



Selecting the + **Add Rules** button adds Rules (**Access**, **Elevator**, **Event**, or **Anti-Passback**) to the Group.

Access Rules

To create an **Access Rule**, select + **Add Rules** in the **Access Rules** section of the drawer. This can be created for a **Person** or a **Group**.



By default, the **Access** tab will be selected.



Select the **Schedule** field and choose the appropriate option (**Always**, **Recurring**, **Single Date**). Each **Schedule** option will be outlined separately below.

After configuring the **Access Rule** as detailed below, select **Submit** in the lower right corner of the drawer to save the new **Access Rule**.

Creating an Always (24-hour) Access Rule

←

Add Rule

Access

Elevator

Event

Anti-Passback

Schedule

Always

▼

Devices

No Devices

Edit Devices

Action

Allow

Deny

Primary Authentication Policy

Select one or more credential types. Secondary Policy is available only with Card or Bluetooth.

☐ Card or Bluetooth ⓘ

☐ PIN

☐ Mobile Button

Cancel

Submit

Schedule - The rule will always be processed.

Schedule

Always

▼

2.0 Customer Dashboard

Devices - Select the **Devices** to include in the **Access Rule** by selecting **Edit Devices**.

Devices

No Devices

Edit Devices

Action - The **Action** option specifies whether the **Access Rule** allows or denies access to the **Doors/Devices** it contains.

Allow - Will **Allow** access to the specified **Door/Devices** for the members of the **Group** that the rule is present in. This is the default state for this option.

Deny - Will **Deny** access to the specified **Door/Devices** for the members of the **Group** that the rule is present in.

Action

Allow Deny

Action

Allow Deny

Authentication Policy - The **Authentication Policy** determines which Credential types are required to gain access.

Primary Authentication Policy

Select one or more credential types. Secondary Policy is available only with Card or Bluetooth.

☐ Card or Bluetooth ⓘ

☐ PIN

☐ Mobile Button

Secondary Authentication Policy

This option is available when Card or Bluetooth is selected as the Primary Authentication Policy. When enabled, the user must enter a PIN after presenting the Primary Credential.

☐ PIN

2.0 Customer Dashboard

Primary Authentication Options:

You must select at least one **Primary Authentication Policy**:

- **Card or Bluetooth:** Requires a physical card or a Bluetooth credential via the PDK Access App.
- **PIN:** Requires entering a PIN on a reader keypad.
- **Mobile Button:** Requires tapping the Door name in the PDK Access App.

Secondary Authentication Policy (Optional):

The **Secondary Authentication Policy** adds an extra layer of security.

- **PIN:** If the **Primary Authentication Policy** is set to **Card or Bluetooth**, you can require a **PIN** as a second step. The user must scan their credential *and then* enter their PIN.

Important Note: If an **Authentication Policy** is set for the **Device** in **Configuration**, it may conflict with the selected **Authentication Policy** and cause credentials to function improperly. It is recommended to set this during **Access Rule** creation.

Adding a Recurring Access Rule

Add Rule

Access

Elevator

Event

Anti-Passback

Schedule

Recurring

Days

S

M

T

W

T

F

S

Begin

00:00:00

End

24:00:00

Devices

No Devices

Edit Devices

Action

Allow

Deny

Primary Authentication Policy

Select one or more credential types. Secondary Policy is available only with Card or Bluetooth.

☐ Card or Bluetooth

☐ PIN

☐ Mobile Button

Cancel

Submit

Schedule - The rule will be processed only during the selected time frame each week.

2.0 Customer Dashboard

Days - Select the days of the week the rule will be processed. By default, Monday-Friday are selected.

Begin - Select the specified time (in 24H format) when the **Access Rule** will begin.

End - Select the specified time (in 24H format) when the **Access Rule** will end.

Schedule

Recurring

Days

S

M

T

W

T

F

S

Begin

🕒 00:00:00

End

🕒 24:00:00

Devices - Select the **Devices** to include in the **Access Rule** by selecting **Edit Devices**.

Devices
No Devices

Edit Devices

Action - The **Action** option specifies whether the **Access Rule** allows or denies access to the **Doors/Devices** it contains.

Allow - Will **Allow** access to the specified **Door/Devices** for the members of the **Group** that the rule is present in. This is the default state for this option.

Deny - Will **Deny** access to the specified **Door/Devices** for the members of the **Group** that the rule is present in.

2.0 Customer Dashboard

Action	Action
Allow Deny	Allow Deny

Authentication Policy - The **Authentication Policy** determines which Credential types are required to gain access.

Primary Authentication Policy
Select one or more credential types. Secondary Policy is available only with Card or Bluetooth.

☐ Card or Bluetooth ⓘ

☐ PIN

☐ Mobile Button

Secondary Authentication Policy
This option is available when Card or Bluetooth is selected as the Primary Authentication Policy. When enabled, the user must enter a PIN after presenting the Primary Credential.

☐ PIN

Primary Authentication Options:

You must select at least one **Primary Authentication Policy**:

- **Card or Bluetooth:** Requires a physical card or a Bluetooth credential via the PDK Access App.
- **PIN:** Requires entering a PIN on a reader keypad.
- **Mobile Button:** Requires tapping the Door name in the PDK Access App.

Secondary Authentication Policy (Optional):

The **Secondary Authentication Policy** adds an extra layer of security.

2.0 Customer Dashboard

- **PIN:** If the **Primary Authentication Policy** is set to **Card or Bluetooth**, you can require a **PIN** as a second step. The user must scan their credential *and then* enter their PIN.

Important Note: If an **Authentication Policy** is set for the **Device** in **Configuration**, it may conflict with the selected **Authentication Policy** and cause credentials to function improperly. It is recommended to set this during **Access Rule** creation.

Creating a Single Date Access Rule

Add Rule

Access

Elevator

Event

Anti-Passback

Schedule

Single Date

Date

Select a date

Begin

00:00:00

End

24:00:00

Devices

No Devices

Edit Devices

Action

Allow

Deny

Primary Authentication Policy

Select one or more credential types. Secondary Policy is available only with Card or Bluetooth.

☐ Card or Bluetooth

☐ PIN

☐ Mobile Button

Cancel

Submit

2.0 Customer Dashboard

Schedule - The rule will only be processed for the specified timeframe on a **Single Day**.

Date - Select the date when the rule will be processed.

Begin - Select the specified time (in 24H format) when the **Access Rule** will begin.

End - Select the specified time (in 24H format) when the **Access Rule** will end.



The screenshot shows a configuration form for an Access Rule. The 'Schedule' section is highlighted. It contains a dropdown menu set to 'Single Date'. Below this, the 'Date' field is empty with a calendar icon and the text 'Select a date'. The 'Begin' time is set to '00:00:00' and the 'End' time is set to '24:00:00', both with clock icons.

Devices - Select the **Devices** to include in the **Access Rule** by selecting **Edit Devices**.

Action - The **Action** option specifies whether the **Access Rule** allows or denies access to the **Doors/Devices** it contains.

Allow - Will **Allow** access to the specified **Door/Devices** for the members of the **Group** that the rule is present in. This is the default state for this option.

Deny - Will **Deny** access to the specified **Door/Devices** for the members of the **Group** that the rule is present in.



The image shows two side-by-side screenshots of the 'Action' toggle switch. In the left screenshot, the 'Allow' button is dark blue and the 'Deny' button is light gray. In the right screenshot, the 'Allow' button is light gray and the 'Deny' button is dark blue.

Authentication Policy - The **Authentication Policy** determines which Credential types are required to gain access.

Primary Authentication Policy
Select one or more credential types. Secondary Policy is available only with Card or Bluetooth.

☐ Card or Bluetooth ⓘ 

☐ PIN 

☐ Mobile Button 

Secondary Authentication Policy
This option is available when Card or Bluetooth is selected as the Primary Authentication Policy. When enabled, the user must enter a PIN after presenting the Primary Credential.

☐ PIN 

Primary Authentication Options:

You must select at least one **Primary Authentication Policy**:

- **Card or Bluetooth:** Requires a physical card or a Bluetooth credential via the PDK Access App.
- **PIN:** Requires entering a PIN on a reader keypad.
- **Mobile Button:** Requires tapping the Door name in the PDK Access App.

Secondary Authentication Policy (Optional):

The **Secondary Authentication Policy** adds an extra layer of security.

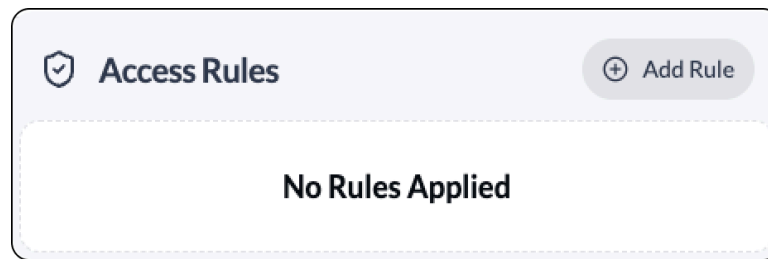
- **PIN:** If the **Primary Authentication Policy** is set to **Card or Bluetooth**, you can require a **PIN** as a second step. The user must scan their credential *and then* enter their PIN.

Important Note: If an **Authentication Policy** is set for the **Device** in **Configuration**, it may conflict with the selected **Authentication Policy**, causing **Credentials** to function improperly. It is recommended to set this during **Access Rule** creation.

Elevator Rules

2.0 Customer Dashboard

To create an **Access Rule**, select **+ Add Rules** in the **Access Rules** section of the drawer. This can be created for a **Person** or a **Group**.



Select **Elevator**. By default, the **Access** tab will be selected.



Schedule - Select this dropdown to choose the **Schedule Type: Always, Recurring, or Single Date**.

Below is an explanation for each **Schedule** type and how to configure each option.

Always - The rule will always be processed.



Recurring - The rule will be processed only during the selected time frame each week.

Days - Select the days of the week on which the rule will be processed. By default, Monday-Friday are selected.

Begin - Select the specified time (in 24H format) when the **Elevator Rule** will begin.

End - Select the specified time (in 24H format) when the **Elevator Rule** will end.

2.0 Customer Dashboard

Schedule

Recurring

Days

S

M

T

W

T

F

S

Begin

🕒 00:00:00

End

🕒 24:00:00

Single Date - The rule will only be processed for the specified timeframe on a single day.

Date - Select the date when the rule will be processed.

Begin - Select the specified time (in 24H format) when the **Elevator Rule** will begin.

End - Select the specified time (in 24H format) when the **Elevator Rule** will end.

Schedule

Single Date

Date

📅 Select a date

Begin

🕒 00:00:00

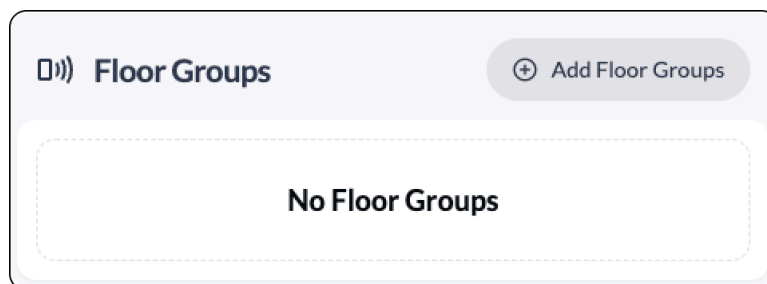
End

🕒 24:00:00

Floor Groups - Select the configured **Elevator Floor Group**.

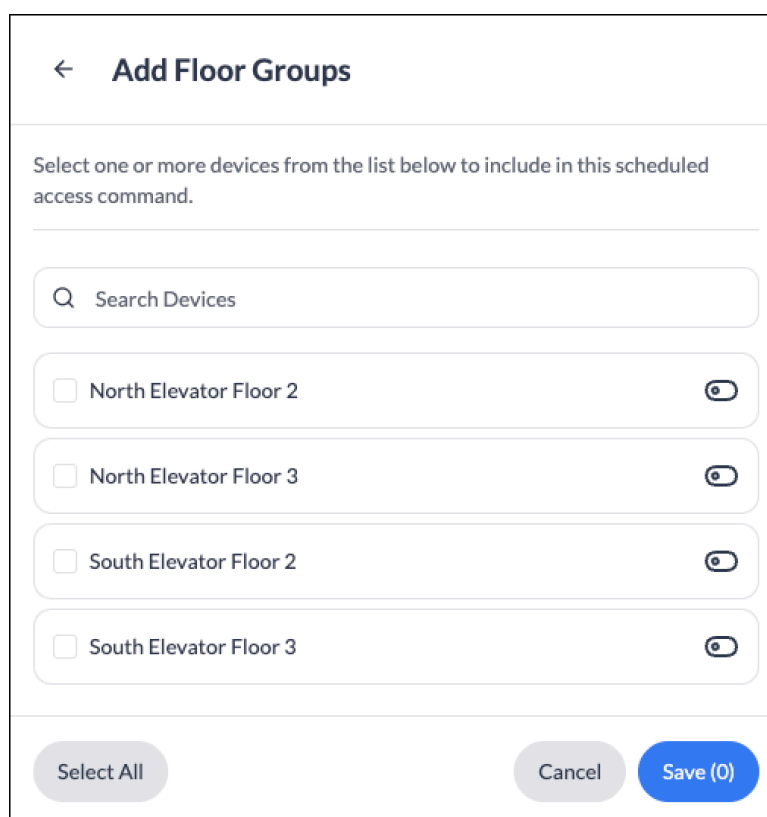
2.0 Customer Dashboard

Select at least one **Floor Group** to save the **Rule**.



The screenshot shows a modal window titled "Floor Groups" with a close button (X) in the top left corner. In the top right corner, there is a button labeled "Add Floor Groups" with a plus icon. The main area of the modal contains a dashed rectangular box with the text "No Floor Groups" centered inside it.

Select **Edit Floor Groups** to highlight the specified **Floor Groups** and then **Save**.



The screenshot shows a modal window titled "Add Floor Groups" with a back arrow in the top left corner. Below the title, there is a text instruction: "Select one or more devices from the list below to include in this scheduled access command." Below this instruction is a search bar with a magnifying glass icon and the placeholder text "Search Devices". Below the search bar is a list of four items, each consisting of a checkbox, a text label, and a toggle switch on the right:

- ☐ North Elevator Floor 2
- ☐ North Elevator Floor 3
- ☐ South Elevator Floor 2
- ☐ South Elevator Floor 3

At the bottom of the modal, there are three buttons: "Select All" (light gray), "Cancel" (light gray), and "Save (0)" (blue).

Authentication Policy - The **Authentication Policy** determines which Credential types are required to gain access.

Primary Authentication Policy
Select one or more credential types. Secondary Policy is available only with Card or Bluetooth.

☐ Card or Bluetooth ⓘ 

☐ PIN 

☐ Mobile Button 

Secondary Authentication Policy
This option is available when Card or Bluetooth is selected as the Primary Authentication Policy. When enabled, the user must enter a PIN after presenting the Primary Credential.

☐ PIN 

Primary Authentication Options:

You must select at least one **Primary Authentication Policy**:

- **Card or Bluetooth:** Requires a physical card or a Bluetooth credential via the PDK Access App.
- **PIN:** Requires entering a PIN on a reader keypad.
- **Mobile Button:** Requires tapping the Door name in the PDK Access App.

Secondary Authentication Policy (Optional):

The **Secondary Authentication Policy** adds an extra layer of security.

- **PIN:** If the **Primary Authentication Policy** is set to **Card or Bluetooth**, you can require a **PIN** as a second step. The user must scan their credential *and then* enter their PIN.

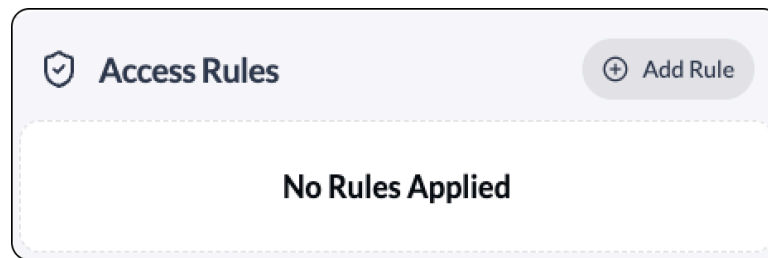
Important Note: If an **Authentication Policy** is set for the **Device** in **Configuration**, it may conflict with the selected **Authentication Policy** and cause Credentials to function improperly. It is recommended to set this during **Access Rule** creation.

After configuring the **Elevator rule**, select **Submit** to save the rule.

Event Rules

Event Rules allow an Action to be processed when a Person performs a specified action on the Cloud Node system.

To create an **Event Rule**, select + **Add Rules** in the **Access Rules** section of the drawer. This can be created for a **Person** or a **Group**.



Select **Event**. By default, the **Access** tab will be selected.



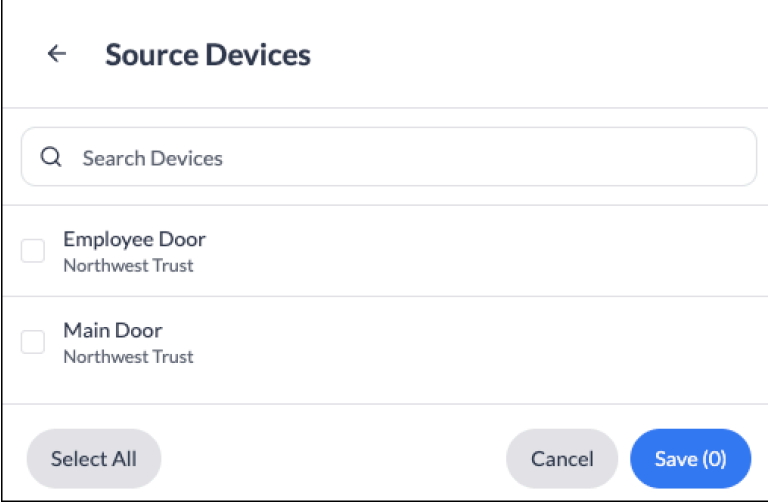
Name - Enter a unique, descriptive name for the **Event** rule.

Trigger - Select the **Trigger** field to select the Event result that will cause the rule to be processed.

Action - Select the **Action** field to select what will occur when the rule is processed.

An Event rule requires both a **Trigger** and an **Action** for the rule to be processed.

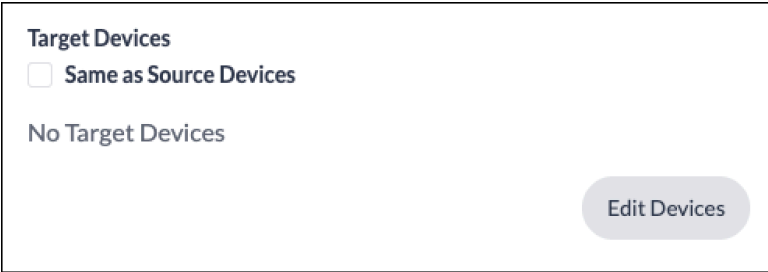
Source Device - Select **Edit Devices** to open the drawer where you can select the **Device** where the selected **Trigger** event will occur. After selecting the chosen **Device**, select **Save**.



The screenshot shows a mobile interface titled "Source Devices" with a back arrow. Below the title is a search bar labeled "Search Devices". There are two device entries, each with a checkbox: "Employee Door Northwest Trust" and "Main Door Northwest Trust". At the bottom, there are three buttons: "Select All", "Cancel", and "Save (0)".

Target Devices - The **Target Devices** option appears for all **Actions** except **Send Email** or **Push Notification**. Select **Edit Devices** to open the drawer where you can select the **Device** where the configured **Action** event will occur. After selecting the chosen **Device**, select **Save**.

- **Same as Source Devices** - When the **Target Device** is the same as the **Source Device**, select this option by selecting the checkbox.



The screenshot shows a mobile interface titled "Target Devices". It contains a checkbox labeled "Same as Source Devices". Below this is the text "No Target Devices". At the bottom right, there is an "Edit Devices" button.

Schedule - Select this dropdown to choose the **Schedule Type**: **Always**, **Recurring**, or **Single Date**.

Below is an explanation of each **Schedule** type and how to configure it

Always - The rule will always be processed.



The screenshot shows a mobile interface with a dropdown menu titled "Schedule". The dropdown is currently set to "Always" and has a downward arrow icon on the right.

2.0 Customer Dashboard

Recurring - The rule will be processed only during the selected time frame each week.

Days - Select the days of the week the rule will be processed. By default, Monday-Friday are selected.

Begin - Select the specified time (in 24H format) when the **Access Rule** will begin.

End - Select the specified time (in 24H format) when the **Access Rule** will end.

The screenshot shows a 'Schedule' configuration form. At the top, there is a dropdown menu labeled 'Schedule' with 'Recurring' selected. Below this is a 'Days' section with seven circular buttons labeled S, M, T, W, T, F, and S. The buttons for M, T, W, T, and F are dark blue, while the buttons for S and S are light gray. Below the days section is a 'Begin' section with a time input field showing '00:00:00'. At the bottom is an 'End' section with a time input field showing '24:00:00'.

Single Date - The rule will only be processed for the specified timeframe on a **Single Day**.

Date - Select the date when the rule will be processed.

Begin - Select the specified time (in 24H format) when the **Access Rule** will begin.

End - Select the specified time (in 24H format) when the **Access Rule** will end.

2.0 Customer Dashboard

Schedule

Single Date ▾

Date

 Select a date

Begin

 00:00:00

End

 24:00:00

After configuring the **Event** rule, select **Submit** to save the rule.

Event Triggers

- **When Allowed** - This rule will be processed when a 'Credential Input' event produces an 'Access Allowed' result.
- **When Denied (Explicit)** - This rule processes when a Credential entry is denied because the door/device is in a Do Not Disturb state.
- **When Denied (No Rules)** - This rule processes when a Credential entry is denied because no Allow rule is configured for the timeframe when the credential was processed.
- **Always (Valid Credentials)** - This rule processes when any Credential is entered into the system, regardless of whether access is allowed or denied.
- **On Multiswipe Allow (# Swipe)** - This rule processes when a physical Credential is scanned a set number of times (2, 3, or 4) in rapid succession on a reader.
- **On Duress** - This rule processes when a Duress PIN is entered on a keypad reader.
- **On Anti-passback Violation** - This rule processes when an Anti-Passback rule triggers a violation for the Person.

Event Actions

- **Send Email** - Selecting this action will allow an email or SMS text message to be sent to the specified email address(es) (or phone numbers) using the pre-configured email template.

- **Send Push Notification** - This action will send a Push Notification to a user with a configured Permission used to log in to Manage Access in the PDK Access App. Push Notifications will be displayed in the same manner as other app notifications on the mobile device.
- **Do Not Disturb** - This action toggles the Target door/device into the 'Do Not Disturb' state (if not in this state) or out of the 'Do Not Disturb' state (if in this state). While in the **Do Not Disturb** state, the door/device will be locked and access attempts will be rejected until the Do Not Disturb state is toggled/canceled.
- **Force Toggle** - This action toggles the current state of the relay for the Target door/device and maintains this new state until another Force Toggle command is sent. For example, if the Target door/device is unlocked/activated, a 'Force Toggle' command will lock/deactivate the door/device, and then further normal access attempts will be rejected until another Force Toggle command is sent.
- **Force Open** - This action sets the relay for the Target door/device to an unlocked/activated state and will remain in this state until a Force Toggle command is sent.
- **Force Close** - This action sets the relay for the Target door/device to a locked/deactivated state and will remain in this state until a Force Toggle command is sent.
- **Lockdown On** - This action toggles the Target door/device into a 'Do Not Disturb' state. While in the **Do Not Disturb** state, the door/device will be locked and access attempts will be rejected until the Do Not Disturb state is toggled/canceled.
- **Lockdown Off** - This action clears the 'Do Not Disturb' state on the door/device and returns it to its default state.
- **Open** - This action will unlock/activate the Target door/device until another command locks/deactivates the door/device, such as Close, Delay Close, and Open/Close.
- **Close** - This action will lock/deactivate the Target door/device until another command that will lock/deactivate the door/device, such as Open, Delay Close, and Open/Close.
- **Open/Close** - This action causes the Target door/device to unlock/activate, then lock/deactivate after the listed Dwell time.
- **Sound Piezo (OSDP Readers Only)** - This action will activate the Piezo speaker in a Red-reader that uses OSDP wiring
- **Silence Piezo (OSDP Readers Only)** - This action will deactivate the Piezo speaker in a Red-reader that uses OSDP wiring

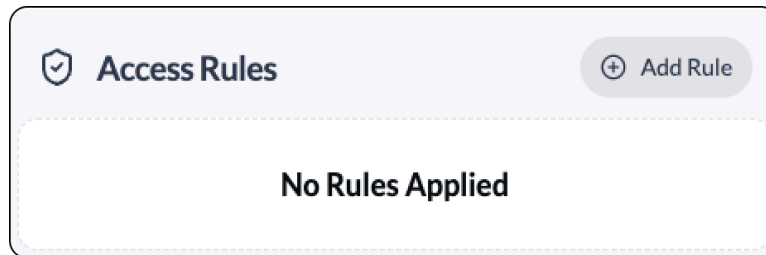
Anti-Passback Rules

Anti-Passback Rules define a specific sequence in which Credentials must be used and are most commonly used in areas with defined exits and entrances. While an Anti-Passback rule is active,

2.0 Customer Dashboard

the system requires that, for every allowed Credential entry by a Person at a designated entry device, there be a corresponding allowed Credential entry at an exit device before the Person can use their Credential at an entry device without an Anti-Passback Violation.

To create an **Anti-Passback Rule**, select **+ Add Rules** in the **Access Rules** section of the drawer. This can be created for a **Person** or a **Group**.



Select **Anti-Passback**. By default, the **Access** tab will be selected.



Schedule - Select this dropdown to choose the **Schedule Type: Always, Recurring, or Single Date**.

Below is an explanation for each **Schedule** type and how to configure each option.

Always - The rule will always be processed.



Recurring - The rule will be processed only during the selected time frame each week.

Days - Select the days of the week on which the rule will be processed. By default, Monday-Friday are selected.

Begin - Select the specified time (in 24H format) when the **Anti-Passback Rule** will begin.

End - Select the specified time (in 24H format) when the **Anti-Passback Rule** will end.

2.0 Customer Dashboard

Schedule

Recurring

Days

S

M

T

W

T

F

S

Begin

🕒 00:00:00

End

🕒 24:00:00

Single Date - The rule will only be processed for the specified timeframe on a single day.

Date - Select the date when the rule will be processed.

Begin - Select the specified time (in 24H format) when the **Anti-Passback Rule** will begin.

End - Select the specified time (in 24H format) when the **Anti-Passback Rule** will end.

Schedule

Single Date

Date

📅 Select a date

Begin

🕒 00:00:00

End

🕒 24:00:00

2.0 Customer Dashboard

Entry Devices - Select at least one Door or Device to function as an **Entry Device**; it will record that the Person has entered and that the Person must exit at an **Exit Device** to prevent an **Anti-Passback Violation**.

Select the **Devices** to include as the **Entry Device** by selecting **Edit Devices**.

A rectangular box representing a user interface for selecting entry devices. Inside the box, the text "Entry Devices" is displayed in a bold font, and "No Entry Devices" is displayed below it in a lighter font. In the bottom right corner of the box, there is a rounded rectangular button with the text "Edit Devices".

Exit Devices - Select at least one door or device to function as an **Exit Device**; it will record that the Person has 'exited' and that their credential can be scanned at an **Entry Device** without causing an **Anti-Passback Violation**.

Select the **Devices** to include as the **Exit Device** by selecting **Edit Devices**.

A rectangular box representing a user interface for selecting exit devices. Inside the box, the text "Exit Devices" is displayed in a bold font, and "No Exit Devices" is displayed below it in a lighter font. In the bottom right corner of the box, there is a rounded rectangular button with the text "Edit Devices".

NOTE: **Entry** and **Exit Devices** must be unique **Devices**.

Re-entry - The **Re-Entry** option specifies the behavior when an Anti-Passback rule violation occurs

Deny - When set to **Deny**, the Anti-Passback rule will consider any Credential entry by the violating Credential as occurring during a "**Deny Explicit**" state on the selected **Entry Devices**. This prevents the violating Credential from accessing any **Entry Device** listed in the rule and generates an Anti-Passback Violation event.

Allow - When set to **Allow**, the **Anti-Passback** rule allows access to the listed **Entry Devices**, but generates an **Anti-Passback Violation** event.

2.0 Customer Dashboard

Violation Expiration - The **Violation Expiration** option specifies the duration for which an Anti-Passback rule violation will persist for a violating Credential. Select this dropdown to choose the Violation Expiration: **Never**, **1 Hour**, **24 Hours**, or **Custom**.

Never - Anti-passback restrictions generated by this rule will remain active for the person until a Credential for that Person is used on an **Exit Device** or the restriction for the Person is cleared.



A screenshot of a web form titled "Violation Expiration". It features a single dropdown menu with the text "Never" selected and a downward-pointing arrow on the right side.

1 Hour - Anti-passback restrictions generated by this rule will remain active for the person until a Credential for that Person is used on an **Exit Device**, the restriction for the Person is cleared, or one hour passes.



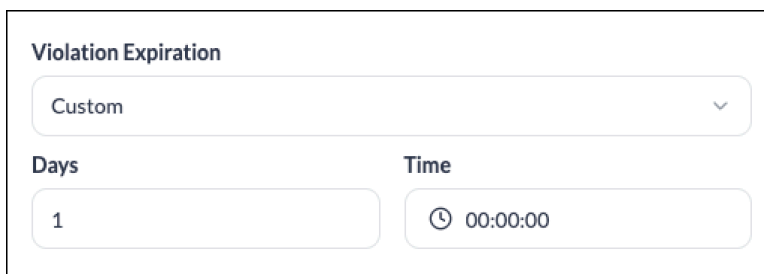
A screenshot of a web form titled "Violation Expiration". It features a single dropdown menu with the text "1 Hour" selected and a downward-pointing arrow on the right side.

24 Hours - Anti-passback restrictions generated by this rule will remain active for the person until a Credential for that Person is used on an **Exit Device**, the restriction for the Person is cleared, or twenty-four (24) hours pass.



A screenshot of a web form titled "Violation Expiration". It features a single dropdown menu with the text "24 Hours" selected and a downward-pointing arrow on the right side.

Custom - Anti-passback restrictions generated by this rule will remain active for the Person until a Credential for the Person is used on an **Exit Device**, the restriction for the Person is cleared, or the configured time has passed.

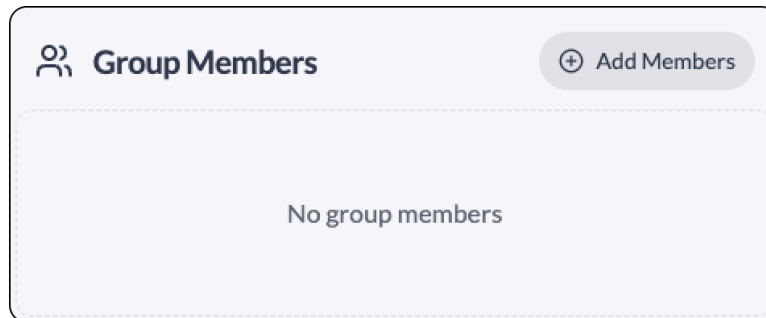


A screenshot of a web form titled "Violation Expiration". The "Custom" option is selected in the dropdown menu. Below the dropdown, there are two input fields: "Days" with the value "1" and "Time" with a clock icon and the value "00:00:00".

2.0 Customer Dashboard

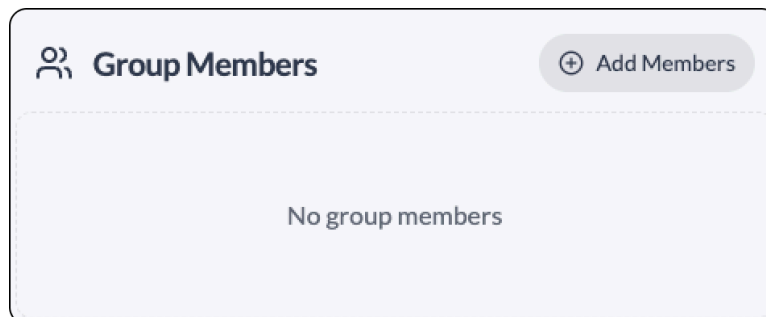
After configuring the **Anti-Passback rule**, select the **Submit** button to save the rule.

2.2.5 Group Members



Selecting **+ Add Members** allows you to add one or more Person(s) to the Group. Place a checkmark next to the People on the Cloud Node System to be added to the Group, then select **Save**. A Person can be a member of multiple Groups on a Customer Account.

2.2.6 Recent Audit Logs



The **Recent Audit Logs** list activity and changes, such as commands sent via the PDK Access App or the PDK.io website, as well as additions, modifications, and updates to access control devices, people, groups, and rules, along with details about those events and changes.

NOTE: The **Recent Audit Log** only shows the 50 most recent events for the Group. If you need additional logged entries, use the Reports function to view *all* logged events and modifications for a specific timeframe, by device name, specific People, etc.

2.3 Units

Units + Add Unit

Search Units...

All 6 Total Units 4 Units Occupied 2 Units Vacant

Unit Number	Status	Residents	Devices
101	Occupied	4	2
102	Occupied	1	1
103	Occupied	2	0
104	Vacant	0	0
105	Occupied	2	3
106	Vacant	0	0

Units are designed for Residential Properties, such as apartment complexes. They allow Admins or Managers to efficiently manage resident access without creating manual **Access Rules** for each apartment. You can also find a Unit by using the search bar located above the Unit list.

Residents assigned to a **Unit** automatically receive 24/7 mobile access to their Unit door.

NOTES:

- **Hardware Support:** Currently, **Red Wireless Locks** are the only hardware supported for Unit Device assignments.
- **Common Areas:** Access to Standard doors (e.g., gym, lobby, pool) is *not* automatic; those must be created using **People** or **Group Access Rules**

2.3.1 Configuring Units

Enable Units Management

Save Changes

Units Management must be enabled in **System Settings** before the **Units** can be configured. Once enabled, the **Units** icon will appear on the Customer Dashboard.

2.3.2 Creating Units

+ Add Unit

To create a **Unit**, select **+ Add Unit**. Each **Unit** requires a unique name.

←

105

↗

Occupied

👤 Residents

+ Add Resident

JD

Jane Doe

No Digital Credentials

Move-in | 08/12/26, 00:00

Move-out ▼

↗

🗑

pdk

John Doe

No Digital Credentials

Move-in | 08/12/26, 00:00

Move-out ▼

↗

🗑

🔌 Devices

+ Add Device

Back Door

🗑

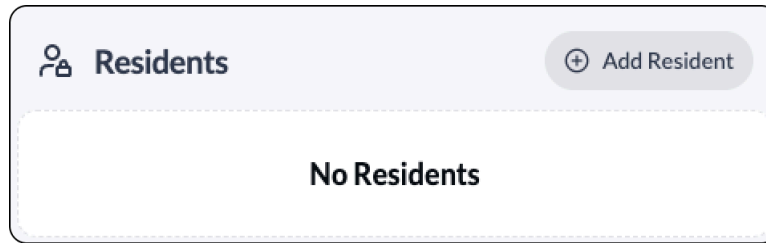
Front Door

🗑

Storage Room

🗑

2.3.3 Assigning Residents to a Unit



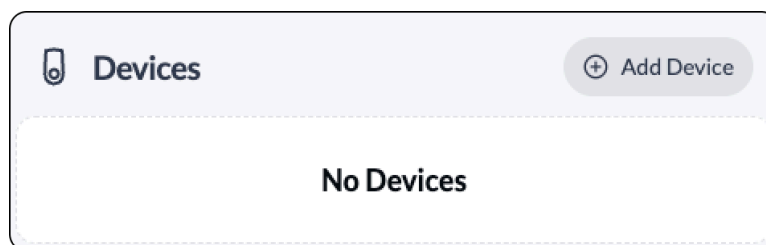
Select users from your **People** list.

- **Move-in:** The Move-in date defaults to the Unit creation date.
- **Move-out:** The Move-out date is not required.
- **No Digital Credential:** Visible if Digital Credentials have not been assigned.

NOTES:

- Move-in/out dates manage Unit residency specifically and are separate from a user's **Active/Expire Dates**.
- Residents must have an email address configured to receive a **Digital Credential** invitation.

2.3.4 Assigning Devices to Units



Select the specific **Red Wireless Lock** to be assigned to the **Unit**.

NOTES:

- A **Device** can only be assigned to one **Unit**.

2.0 Customer Dashboard

- **Units** can be created without assigning a **Device**.

2.3.5 Units List

Units

+ Add Unit

Search Units...

All

6 Total Units

4 Units Occupied

2 Units Vacant

101

Occupied

4 Residents | 2 Devices

102

Occupied

1 Resident | 1 Device

103

Occupied

2 Residents | 0 Devices

104

Vacant

0 Residents | 0 Devices

105

Occupied

2 Residents | 3 Devices

106

Vacant

0 Residents | 0 Devices

Once created, **Units** are searchable and can be filtered by **All**, **Occupied**, or **Vacant**. A list of **Total Units**, **Units Occupied**, and **Units Vacant** is also displayed.

NOTE: The vacancy status for each **Unit** will also be displayed on the **States** page.

Occupied	Vacant
Sales Office - Left - Cylindrical Locked Unit Occupied	Sales Office - Right - Cylindrical Locked Unit Vacant

Copyright © 2026 ProdataKey. All rights reserved.
REV 2.0.0

84

2.3.6 Editing or Deleting a Unit

 Edit Unit

After a **Unit** has been created, selecting the **Unit**'s name opens the Unit's window. Selecting **Edit Unit** allows the name to be changed.

 Delete Unit

To delete a **Unit** from the **Customer Account**, select **Delete Unit**. This opens a dialog box that warns that this action will delete the selected Unit. Before this can be done, all **Residents** and **Devices** must be removed from the Unit.

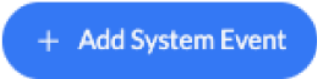
2.4 System Events

System Events					+ Add System Event
Search System Events					
Name	Trigger	Action	Schedule		
Communication Loss	On Comm Loss	Send Email	Always On		
Main Door REX	On Rex Open	Open/Close	Always On		
Unknown Credential	On Credentials Not Found	Send Push Notification	Always On		

System Events are rules that are not linked to the actions of any specific **Person** or **Group** on the **Customer Account**. This includes hardware triggers (DPS, REX, hardware issue/condition, etc.) or general **Credential** activity (any Credential being used, unknown Credentials, Duress PIN use, etc.). The **Integrator**, **Admin**, and **Manager** permission roles can access the **System Events** features. You can also find a **System Event** using the search bar above the **System Event** list.

2.4.1 Creating A System Event

To begin creating a new **System Event** rule, select **+ Add System Event**.

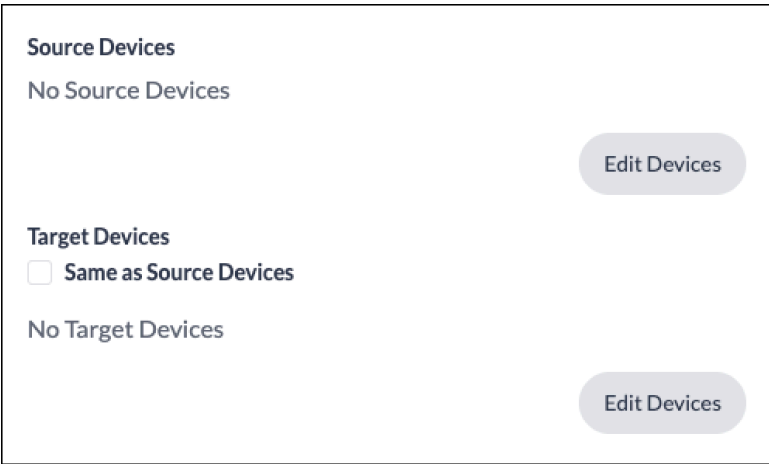
A blue rounded rectangular button with a white plus sign icon followed by the text "Add System Event".

Name - Enter a unique, descriptive name for the **System Event** rule.

Partition - To allow one or more **Managers** assigned to specific **Partitions** to manage the **System Event** rule, select this field. Any previously created **Partitions** appear in the list. The **Partition** field displays only if partitions beyond the default **Partition** have been created.

Trigger - Select this field to select what **Trigger** condition on the **Customer Account** will result in the **System Event** rule being processed.

Action - Select this field to select what **Action** will occur on the **Customer Account** when the **System Event** rule is processed.

A light gray rectangular panel with a thin black border. It contains two sections. The top section is titled "Source Devices" and shows "No Source Devices" with an "Edit Devices" button to its right. The bottom section is titled "Target Devices" and includes a checkbox labeled "Same as Source Devices" which is currently unchecked. Below this is "No Target Devices" with another "Edit Devices" button to its right.

Source Devices
No Source Devices
Edit Devices

Target Devices
☐ Same as Source Devices
No Target Devices
Edit Devices

Source Devices - Select **Edit Devices** to open the drawer where you can select the **Device** where the selected **Trigger** event will occur. After selecting the chosen **Device**, select **Save**.

The screenshot shows a mobile application interface titled "Source Devices" with a back arrow. Below the title is a search bar labeled "Search Devices". There are two device entries, each with a checkbox and text: "Employee Door Northwest Trust" and "Main Door Northwest Trust". At the bottom, there are three buttons: "Select All" (disabled), "Cancel" (disabled), and "Save (0)" (active).

Target Devices - This option appears only when certain **Actions** are selected. The **Same as Source Devices** option is also available. Select **Edit Devices** to open the drawer where you can select the **Device** where the configured **Action** event will occur. After selecting the chosen **Device**, select **Save**.

The screenshot shows a mobile application interface titled "Target Devices" with a back arrow. Below the title is a search bar labeled "Search Devices". There are two device entries, each with a checkbox and text: "Employee Door Northwest Trust" and "Main Door Northwest Trust". At the bottom, there are three buttons: "Select All" (disabled), "Cancel" (disabled), and "Save (0)" (active).

Schedule - Select this dropdown to choose the **Schedule Type: Always, Recurring, or Single Date**.

Below is an explanation of each **Schedule Type** and how to configure it:

Always - The **System Event** rule will always occur, regardless of the day or timeframe.

2.0 Customer Dashboard



A screenshot of a user interface element labeled "Schedule". It features a dropdown menu with the word "Always" selected and a small downward-pointing chevron icon on the right side.

Recurring - The **System Event** rule will be processed only during the selected weekly time frame.



A screenshot of a user interface section titled "Schedule". It contains a dropdown menu with "Recurring" selected. Below this is a "Days" section with seven circular buttons labeled S, M, T, W, T, F, S. The buttons for M, T, W, T, and F are dark blue, while S and S are light gray. Below the days are two time input fields: "Begin" with a clock icon and the value "00:00:00", and "End" with a clock icon and the value "24:00:00".

Days - Select the days of the week the rule will be processed. By default, Monday-Friday are selected.

Begin - Select the specified time (in 24H format) when the **System Event** begins.

End - Select the specified time (in 24H format) when the **System Event** ends.

Single Date - The rule will only be processed for the specified time frame on a single day.

2.0 Customer Dashboard

Schedule

Single Date

Date

 Select a date

Begin

 00:00:00

End

 24:00:00

Date - Select the day the **System Event** will be processed.

Begin - Select the specified time (in 24H format) when the **System Event** begins.

End - Select the specified time (in 24H format) when the **System Event** ends.

2.4.2 Editing a System Event

After a **System Event** has been created, selecting the **System Event's name** will open a drawer where all the details above can be edited.

System Event Triggers

A **Trigger** event must be selected during **System Event** creation. When this **Trigger** event occurs on any selected **Source Device**, the configured **Action** event will occur.

Below is a list of the available **Trigger Events** along with a description of what each **Trigger** means.

- **On Open** - The door position sensor (DPS) is open
 - **On Close** - The door position sensor (DPS) is closed
 - **On Propped** - The door is held or propped open longer than the prop Trigger period
 - **On Forced** - The door is opened without a valid credential read or Request to Exit (REX) input
-

- **On Prop Cleared** - The door position sensor was closed after the prop Trigger was activated
- **All Prop Cleared** - All door-propped alarms have been cleared
- **On Rex Open** - The Request to Exit (REX) input is activated (unlocked). For example, connecting NO on the REX to the PDK REX input (B)
- **On Rex Close** - The Request to Exit (REX) input is deactivated (locked). For example, connecting NC on the REX to the PDK REX input (B)
- **On Credentials Input** - Trigger the event on ANY credential input, either valid or invalid
- **On Credentials Not Found** - Credential input at the reader that is not recognized or not programmed in the system
- **On Comm Loss** - Device communication is lost
- **On Comm Loss Cleared** - Device communication has been re-established
- **On Any Duress** - When a Duress PIN is entered
- **On Input Power Loss** - When primary input power is lost/disconnected
- **On Input Power Recovery** - When primary input power is restored
- **On Overcurrent Detected** - When excess or higher-than-intended current is detected on the indicated Controller
- **On Overcurrent Cleared** - When standard or intended current is detected on the indicated Controller, the detection event is cleared
- **On Underpowered Input Detected** - When insufficient current is detected on the indicated Controller
- **On Underpowered Input Alarm Cleared** - When sufficient current is detected on the indicated Controller, the underpowered detection event is cleared
- **On Low Power Mode On** - When low power mode is detected
- **On Low Power Mode Off** - When low power mode is not detected
- **On Battery Connect** - When expected battery power is detected
- **On Battery Disconnect** - When battery power is lost
- **On Battery Level Change** - When battery level on a Red Wireless Lock has changed
- **On Circuit Breaker On** - A 'Circuit Breaker' event occurred. This is a flood of event logging (40 events in 30 seconds) occurring on either input A or B (DPS or REX), which disables the input for 30 minutes
- **On Circuit Breaker Off** - A 'Circuit Breaker' event ended
- **On Partial Connectivity Detected** - The controller is not responding, but contact with the WiMAC radio is established
- **On Partial Connectivity Cleared** - Communication between the WiMAC radio and controller is restored
- **On Jammed** - When the Red Wireless Deadbolt is jammed
- **On Jammed Cleared** - When the Red Wireless Deadbolt is no longer jammed

System Event Actions

An **Action** event must be selected during **System Event** creation. When a **Trigger** event occurs on any selected **Source Device**, the **Action** event configured will occur.

Below is a list of the available **Action Events** along with a description of what each **Action** means.

- **Send Email** - This action sends an email to the specified email address(es) using the preconfigured email template.
- **Send Push Notification** - This action will send a Push Notification to a user with a configured Permission used to log in to Manage Access in the PDK Access App. Push Notifications will display the same way as other app notifications on the mobile device.
- **Do Not Disturb** - This action toggles the Target door/device into the Do Not Disturb state (if not in this state) or out of the Do Not Disturb state (if in this state). While in the Do Not Disturb state, the door/device will be locked, and access attempts will be rejected until the Do Not Disturb state is toggled/canceled.
- **Force Toggle** - This action toggles the current state of the relay for the Target door/device and maintains this new state until another Force Toggle command is sent. For example, if the Target door/device is unlocked, a Force Toggle command will lock the door/device, and then further normal access attempts will be rejected until another Force Toggle command is sent.
- **Force Open** - This action sets the relay for the Target door/device to an unlocked state and leaves it there until a Force Toggle command is sent.
- **Force Close** - This action sets the relay for the Target door/device to a locked state, which remains until a Force Toggle command is sent.
- **Lockdown On** - This action toggles the Target door/device into a Do Not Disturb state. While in the Do Not Disturb state, the door/device will be locked, and access attempts will be rejected until the Do Not Disturb state is toggled/canceled.
- **Lockdown Off** - This action clears the Do Not Disturb state on the door/device and returns it to its default state.
- **Open** - This action will unlock the Target door/device until another command locks it, such as Close, Delay Close, or Open/Close.
- **Close** - This action locks the Target door/device until another command is issued to unlock it, such as Open, Delay Close, or Open/Close.
- **Open/Close** - This action unlocks the Target Device/Door, then locks it after the listed Dwell and Delay times.
- **Sound Piezo (OSDP Readers Only)** - This action will activate the Piezo speaker in a Red-reader that uses OSDP wiring
- **Silence Piezo (OSDP Readers Only)** - This action will deactivate the Piezo speaker in a Red-reader that uses OSDP wiring

2.4.3 Deleting a System Event

There are two ways to delete a **System Event** rule.

- In the **System Event** window, select the trash can icon next to the **System Event** you want to delete.
- In the existing rule, select **Delete System Event** located in the lower-left corner of the drawer menu.

2.5 Auto Open

An **Auto Open** rule allows a door/device to automatically Open (unlock) and Close (lock) within a specified time frame.

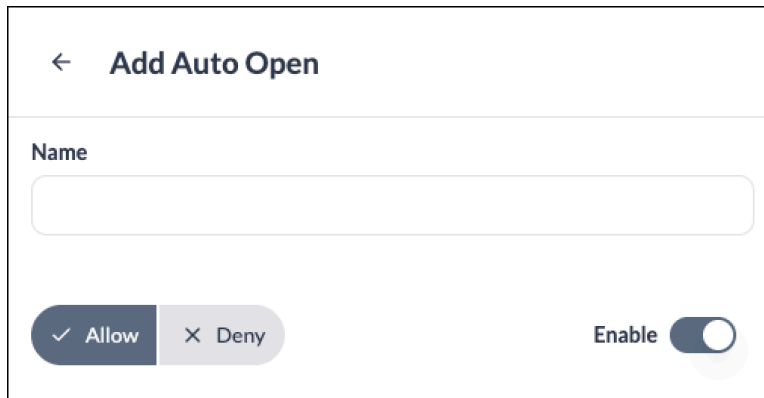
Auto Open rules can also be configured so that doors/devices in existing **Auto Open** schedules do not automatically unlock during specified times, such as holidays, scheduled business closures, or other functions. Specific times, days of the week, and days of the year can be designated to automatically lock and unlock doors, allowing or denying access to a location.

You can locate an **Auto Open** using the search bar above the schedule list, and filter it by categories such as All, Allow, Deny, Active, Expired, Enabled, or Disabled.

Auto Open					+ Add Auto Open	
Search Auto Open		Filter By All ⌵ ⋮ ☰				
Name ⌵	Action	Devices	Schedule	Enable		
 Christmas	✗ Deny	Front Door	00:00 - 24:00 Dec 25th	☒		
 Labor Day	✗ Deny	Front Door	00:00 - 24:00 First Monday in September	☐		
 Monthly Meeting	✓ Allow	Front Door	17:00 - 19:00 Third Thursday	☒		
 Testing	✓ Allow	Front Door	15:18 - 15:20 Weekdays	☒		

2.5.1 Adding an Auto Open Schedule

To create a new **Auto Open** schedule, first select the + **Add Auto Open** button in the **Auto Open** window. This is located above any existing **Auto Open** rules for the **Customer Account**. This will open a drawer where you can enter the information for the new **Auto Open** schedule.



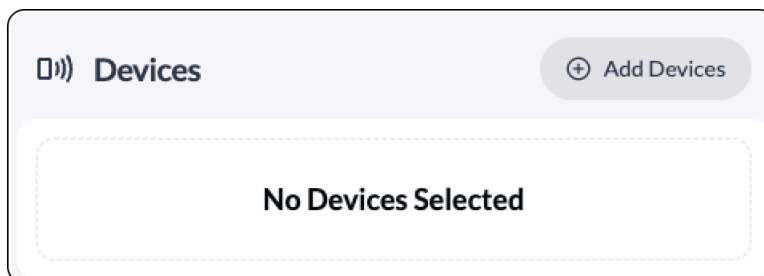
The screenshot shows a drawer titled "Add Auto Open" with a back arrow. It contains a "Name" label above a text input field. At the bottom, there are two radio buttons: "Allow" (selected) and "Deny". To the right of these is an "Enable" toggle switch, which is currently turned on.

Name - Assign a unique descriptive name for the **Auto Open** rule.

Partition - If the **Auto Open** rule is assigned to a specific partition, select it in this Partition field, or use the down arrow to select a listed partition. The **Partition** field appears only if you have created partitions beyond the default **Partition**.

Allow - This enables the **Doors** listed in the **Auto Open** schedule to unlock at the specified date and time. This is the default state for this option.

Enable - Toggle this option to turn the schedule on or off. This toggle is also visible in the main **Auto Open** window, on the right side of each configured schedule.



The screenshot shows a section titled "Devices" with a speaker icon and an "Add Devices" button. Below this is a dashed rectangular box containing the text "No Devices Selected".

Devices - Select the Devices to include in the Auto Open schedule. Select the + **Add Devices** button in the drawer.

 **Add Devices**

Select one or more devices from the list below to include in this scheduled access command.

 Search Devices

☐

Kansas City
3 devices | 0 selected



☐

Omaha
5 devices | 0 selected



☐

St. Paul
1 devices | 0 selected



Next, select the **Devices** to include in the **Auto Open** schedule, then select **Save**. If more than one **Cloud Node** is present in the **Customer Account**, the Doors will be listed under the **Cloud Node** to which they are associated.

Schedule - Select this dropdown to choose the **Schedule Type: Always, Single Date, Daily, Weekly, Monthly, or Yearly**.

 **Schedule**

 Add Schedule

No Schedule

Below is an explanation of each Schedule Type and how to configure it:

Always - The **Auto Open** schedule will always be processed.

← Add Schedule

Schedule

Always

Single Date - The **Auto Open** schedule will be processed once on the selected date.

Schedule

Single Date

Date

📅

Select a Date

Start Time

00:00:00

End Time

24:00:00

+ Add Time

- Delete Time

Date - Select the date you want the schedule to run.

Start Time - Select the specified time (in 24H format) when the **Auto Open** schedule begins.

End Time - Select the specified time (in 24H format) when the **Auto Open** schedule ends.

NOTE: Each schedule can have three different **Start** and **End Times**

Daily - The **Auto Open** schedule will be processed daily.

← Add Schedule

Schedule

Daily

Start Date

Repeat Every

Select a Date

1 Day

▼

▲

Ends

Never

Start Time

End Time

00:00:00

24:00:00

+ Add Time

- Delete Time

Start Date - Select the date you would like the schedule to begin.

Repeat Every - Select how often you would like the schedule to repeat, in days.

Ends - Select when you would like the schedule to stop processing: **Never**, **On a Date**, or **After a Number of Times**.

Start Time - Select the specified time (in 24H format) when the **Auto Open** schedule begins.

End Time - Select the specified time (in 24H format) when the **Auto Open** schedule ends.

NOTE: Each schedule can have three different **Start** and **End Times**

Weekly - The **Auto Open** schedule will be processed weekly.

← Add Schedule

Schedule

Weekly

Days

S

M

T

W

T

F

S

Start Date

Select a Date

Repeat Every

1 Week

▼

▲

Ends

Never

Start Time

⌚ 00:00:00

End Time

⌚ 24:00:00

⊕ Add Time

⊖ Delete Time

Days - Select the days of the week the schedule will be processed. By default, Monday-Friday are selected.

Start Date - Select the date you would like the schedule to begin.

Repeat Every - Select how often you would like the schedule to repeat, in weeks.

Ends - Select when you would like the schedule to stop processing: **Never**, **On a Date**, or **After a Number of Times**.

Start Time - Select the specified time (in 24H format) when the **Auto Open** schedule begins.

End Time - Select the specified time (in 24H format) when the **Auto Open** schedule ends.

NOTE: Each schedule can have three different **Start** and **End Times**

Monthly - The **Auto Open** schedule will be processed monthly.

← Add Schedule

Schedule

Monthly

Date

Relative Day

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

Start Date

Repeat Every

📅 Select a Date

1 Month

▼

▲

Ends

Never

Start Time

End Time

🕒 00:00:00

🕒 24:00:00

⊕ Add Time

⊖ Delete Time

Date Type - Select one of the following:

- **Date** - Select the day(s) of the month the schedule will be processed.
- **Relative Day** - Select the relative day of the month the schedule will be processed if the exact date changes monthly.

Start Date - Select the date you would like the schedule to begin.

Repeat Every - Select how often you would like the schedule to repeat, in months.

2.0 Customer Dashboard

Ends - Select when you would like the schedule to stop processing: **Never**, **On a Date**, or **After a Number of Times**.

Start Time - Select the specified time (in 24H format) when the **Auto Open** schedule begins.

End Time - Select the specified time (in 24H format) when the **Auto Open** schedule ends.

NOTE: Each schedule can have three different **Start** and **End Times**

Yearly - The **Auto Open** schedule will be processed yearly.

The screenshot shows a mobile application interface for adding a schedule. At the top is a header bar with a back arrow and the title 'Add Schedule'. Below this is a 'Schedule' section with a dropdown menu currently set to 'Yearly'. Underneath are two tabs: 'Date' (selected) and 'Relative Day'. The 'Date' tab contains three dropdown menus: 'On the' (set to 'First'), 'Of' (set to 'Monday'), and another dropdown (set to 'January'). Below these is a 'Start Date' section with a date picker icon and the text 'Select a Date'. The 'Ends' section has a dropdown menu set to 'Never'. The 'Start Time' and 'End Time' sections each have a clock icon and a text input field; 'Start Time' is set to '00:00:00' and 'End Time' is set to '24:00:00'. At the bottom are two buttons: 'Add Time' (with a plus icon) and 'Delete Time' (with a minus icon).

Date Type - Select one of the following:

- **Date** - Select the day(s) of the year the schedule will be processed.
- **Relative Day** - Select the relative day of the year on which the schedule will be processed if the exact date changes each year.

Start Date - Select the date you would like the schedule to begin.

2.0 Customer Dashboard

Ends - Select when you would like the schedule to stop processing: **Never**, **On a Date**, or **After a Number of Times**.

Start Time - Select the specified time (in 24H format) when the **Auto Open** schedule begins.

End Time - Select the specified time (in 24H format) when the **Auto Open** schedule ends.

NOTE: Each schedule can have three different **Start** and **End Times**

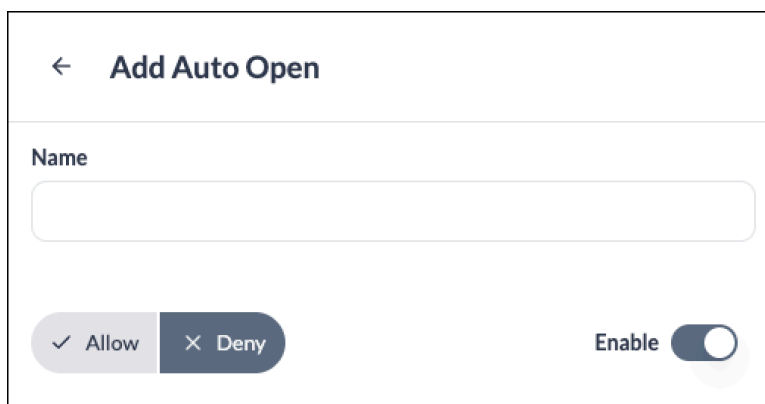
After configuring the **Schedule**, select the **Add** button in the lower-right corner of the drawer.

Select the **Add** button in the lower-right corner of the drawer to save the **Auto Open** schedule.

2.5.2 Adding an Auto Open Deny Schedule (Holiday Closure Schedule)

An **Auto Open Deny** schedule (or holiday closure schedule) overrides normal schedules to prevent doors from automatically unlocking. Use this when a location is closed for holidays or other events.

To create a new **Auto Open Deny** schedule, first select the **+ Add Auto Open** button in the **Auto Open** window. This is located above any existing **Auto Open** schedules for the **Customer Account**. This will open a drawer where you can enter the information for the new **Auto Open Deny** schedule.

The image shows a mobile application drawer titled "Add Auto Open" with a back arrow icon. Below the title is a "Name" label followed by a text input field. At the bottom, there are two buttons: "Allow" with a checkmark icon and "Deny" with an 'X' icon. To the right of these buttons is an "Enable" label and a toggle switch that is currently turned on.

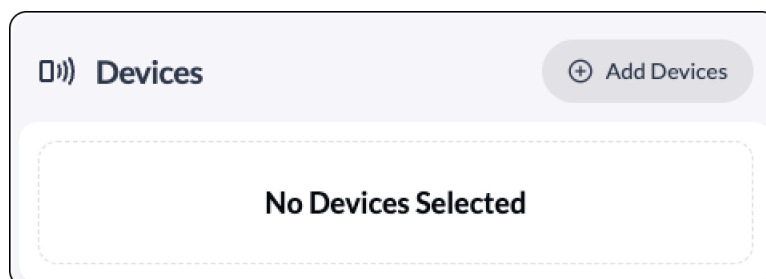
Name - Assign a unique descriptive name for the **Auto Open** rule.

Partition - If the **Auto Open** rule is assigned to a specific partition, select it in this Partition field, or use the down arrow to select a listed partition. The **Partition** field appears only if you have created partitions beyond the default **Partition**.

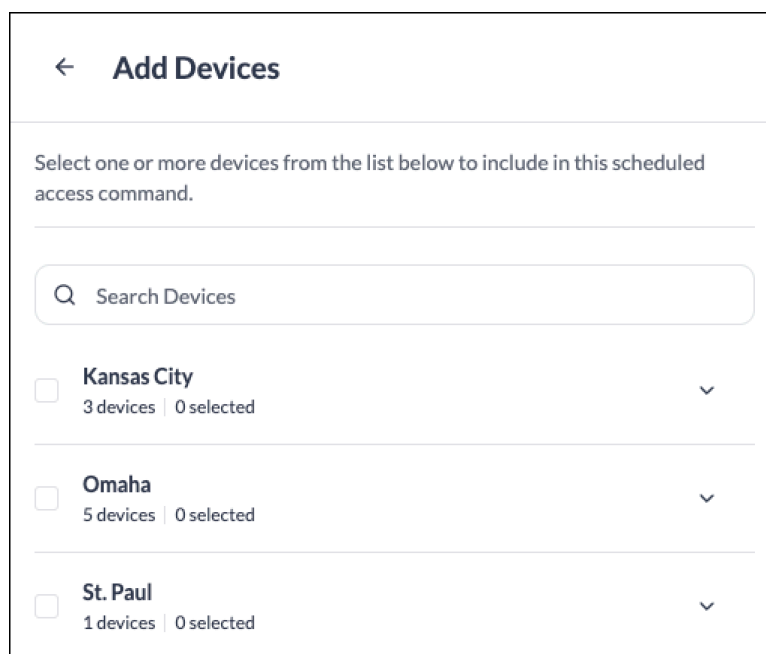
2.0 Customer Dashboard

Deny - This disables **Doors** listed in the **Auto Open** schedule from unlocking at the specified date and time.

Enable - Toggle this option to turn the schedule on or off. This toggle is also visible in the main **Auto Open** window, on the right side of each configured schedule.



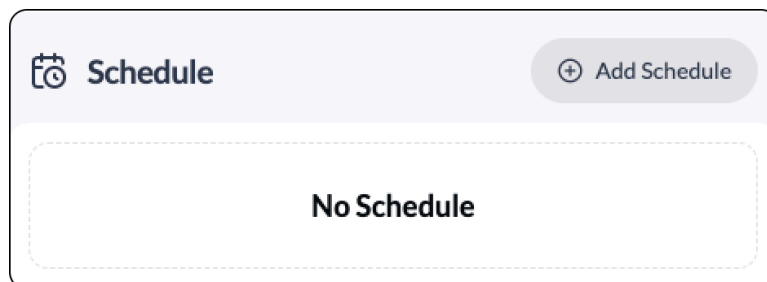
Devices - Select the **Devices** to include in the **Auto Open** schedule. Select the **+ Add Devices** button in the drawer.



Next, select the **Devices** to include in the **Auto Open** schedule, then select **Save**. If more than one **Cloud Node** is present in the **Customer Account**, the **Doors** will be listed under the **Cloud Node** to which they are associated.

2.0 Customer Dashboard

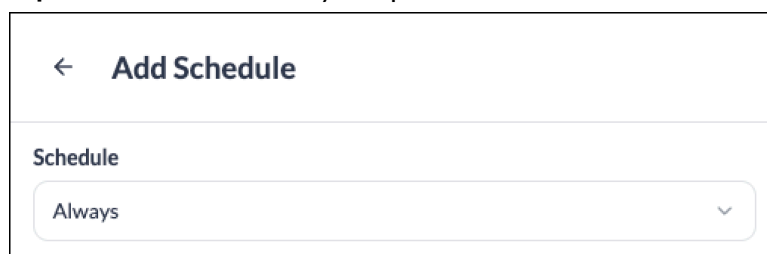
Schedule - Select this dropdown to choose the **Schedule Type: Always, Single Date, Daily, Weekly, Monthly, or Yearly.**



The screenshot shows a card titled "Schedule" with a calendar icon. In the top right corner, there is a button labeled "+ Add Schedule". The main area of the card contains a dashed border and the text "No Schedule".

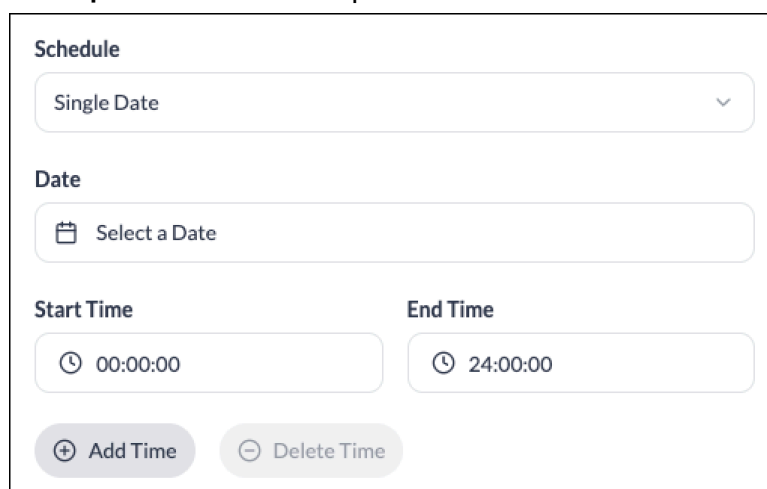
Below is an explanation of each Schedule Type and how to configure it:

Always - The **Auto Open** schedule will always be processed.



The screenshot shows a form titled "Add Schedule" with a back arrow. Under the "Schedule" heading, there is a dropdown menu currently set to "Always".

Single Date - The **Auto Open** schedule will be processed once on the selected date.



The screenshot shows a form titled "Add Schedule" with a back arrow. Under the "Schedule" heading, the dropdown menu is set to "Single Date". Below this, under the "Date" heading, is a date picker labeled "Select a Date". Further down, there are two time pickers: "Start Time" set to "00:00:00" and "End Time" set to "24:00:00". At the bottom, there are two buttons: "+ Add Time" and "- Delete Time".

Date - Select the date you want the schedule to run.

Start Time - Select the specified time (in 24H format) when the **Auto Open** schedule begins.

2.0 Customer Dashboard

End Time - Select the specified time (in 24H format) when the **Auto Open** schedule ends.

NOTE: Each schedule can have three different **Start** and **End Times**

Daily - The **Auto Open** schedule will be processed daily.

The screenshot shows a mobile app interface for adding a schedule. At the top is a back arrow and the title 'Add Schedule'. Below this is a 'Schedule' dropdown menu currently set to 'Daily'. Underneath are two columns: 'Start Date' with a calendar icon and 'Repeat Every' set to '1 Day' with up/down arrows. Below these is an 'Ends' dropdown menu set to 'Never'. At the bottom are two time pickers: 'Start Time' set to '00:00:00' and 'End Time' set to '24:00:00'. At the very bottom are two buttons: '+ Add Time' and '- Delete Time'.

Start Date - Select the date you would like the schedule to begin.

Repeat Every - Select how often you would like the schedule to repeat, in days.

Ends - Select when you would like the schedule to stop processing: **Never**, **On a Date**, or **After a Number of Times**.

Start Time - Select the specified time (in 24H format) when the **Auto Open** schedule begins.

End Time - Select the specified time (in 24H format) when the **Auto Open** schedule ends.

NOTE: Each schedule can have three different **Start** and **End Times**

Weekly - The **Auto Open** schedule will be processed weekly.

← Add Schedule

Schedule

Weekly

Days

S

M

T

W

T

F

S

Start Date

Select a Date

Repeat Every

1 Week

▼

▲

Ends

Never

Start Time

⌚ 00:00:00

End Time

⌚ 24:00:00

⊕ Add Time

⊖ Delete Time

Days - Select the days of the week the schedule will be processed. By default, Monday-Friday are selected.

Start Date - Select the date you would like the schedule to begin.

Repeat Every - Select how often you would like the schedule to repeat, in weeks.

Ends - Select when you would like the schedule to stop processing: **Never**, **On a Date**, or **After a Number of Times**.

Start Time - Select the specified time (in 24H format) when the **Auto Open** schedule begins.

End Time - Select the specified time (in 24H format) when the **Auto Open** schedule ends.

NOTE: Each schedule can have three different **Start** and **End Times**

Monthly - The **Auto Open** schedule will be processed monthly.

← Add Schedule

Schedule

Monthly

Date

Relative Day

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

Start Date

Repeat Every

📅 Select a Date

1 Month

▼

▲

Ends

Never

Start Time

End Time

🕒 00:00:00

🕒 24:00:00

⊕ Add Time

⊖ Delete Time

Date Type - Select one of the following:

- **Date** - Select the day(s) of the month the schedule will be processed.
- **Relative Day** - Select the relative day of the month the schedule will be processed if the exact date changes monthly.

Start Date - Select the date you would like the schedule to begin.

Repeat Every - Select how often you would like the schedule to repeat, in months.

2.0 Customer Dashboard

Ends - Select when you would like the schedule to stop processing: **Never**, **On a Date**, or **After a Number of Times**.

Start Time - Select the specified time (in 24H format) when the **Auto Open** schedule begins.

End Time - Select the specified time (in 24H format) when the **Auto Open** schedule ends.

NOTE: Each schedule can have three different **Start** and **End Times**

Yearly - The **Auto Open** schedule will be processed yearly.

The screenshot shows a mobile application interface for adding a schedule. At the top is a header bar with a back arrow and the title 'Add Schedule'. Below this is a section titled 'Schedule' containing a dropdown menu currently set to 'Yearly'. Underneath are two tabs: 'Date' (which is selected) and 'Relative Day'. The 'On the' section has three dropdowns: 'First', 'Monday', and 'January'. The 'Of' section is empty. Below this is a 'Start Date' section with a date picker icon and the text 'Select a Date'. The 'Ends' section has a dropdown menu set to 'Never'. The 'Start Time' and 'End Time' sections each have a time picker icon and are set to '00:00:00' and '24:00:00' respectively. At the bottom are two buttons: 'Add Time' and 'Delete Time'.

Date Type - Select one of the following:

- **Date** - Select the day(s) of the year the schedule will be processed.
- **Relative Day** - Select the relative day of the year on which the schedule will be processed if the exact date changes each year.

Start Date - Select the date you would like the schedule to begin.

2.0 Customer Dashboard

Ends - Select when you would like the schedule to stop processing: **Never**, **On a Date**, or **After a Number of Times**.

Start Time - Select the specified time (in 24H format) when the **Auto Open** schedule begins.

End Time - Select the specified time (in 24H format) when the **Auto Open** schedule ends.

NOTE: Each schedule can have three different **Start** and **End Times**

After configuring the **Schedule**, select the **Add** button in the lower-right corner of the drawer.

Select the **Add** button in the lower-right corner of the drawer to save the **Auto Open** schedule.

2.5.3 Editing an Auto Open Schedule

After you create an **Auto Open** schedule, selecting its name opens a drawer where you can edit the details above.

2.5.4 Deleting an Auto Open Schedule

There are two ways to delete an **Auto Open Deny** rule.

1. In the **Auto Open** window, select the trash can icon next to the Auto Open schedule you want to delete.
 2. In the existing schedule, select the **Delete Rule** button in the lower-left corner of the drawer.
-

2.6 Elevators

Elevator Floor Groups				+ Add Floor Group
Search Floor Groups				
Name	Cloud Node	Floors	Reader	
North Elevator Floor 2	PDK	North Elevator Floor 2	North Elevator Reader	
North Elevator Floor 3	PDK	North Elevator Floor 3	North Elevator Reader	
South Elevator Floor 2	PDK	South Elevator Floor 2	South Elevator Reader	
South Elevator Floor 3	PDK	South Elevator Floor 3	South Elevator Reader	

Selecting the **Elevators** icon from the **Customer Dashboard** opens the **Elevator Floor Groups** window. **Elevator Floor Groups** group **Elevator Floor Relays** controlled by at least one **Elevator Reader**. **Elevator Floor Groups** allow a **Person** to access designated floors or access them on a set schedule based on an **Access Rule**.

Before **Elevator Floor Groups** can be configured, the following devices must be configured in **Configuration** for the **Customer Account**:

- At least one **Elevator Reader** device.
- At least one **Elevator Floor Relay** device.

Any previously created **Elevator Floor Groups** are listed in alphanumeric order and are searchable.

Once an **Elevator Floor Group** has been created, a rule for the **Elevator Floor Group** will need to be created, either a **Person** or **Group Rule**, in the **Customer Account**.

2.6.1 Adding an Elevator Floor Group

To add an **Elevator Floor Group** to the **Customer Account**, first select the **+ Add Floor Group** button in the **Elevator Floor Groups** window. This opens a drawer where you can enter information for the new **Floor Group**.

← Add Floor Group

Name

Reader

Partition

Cancel Add

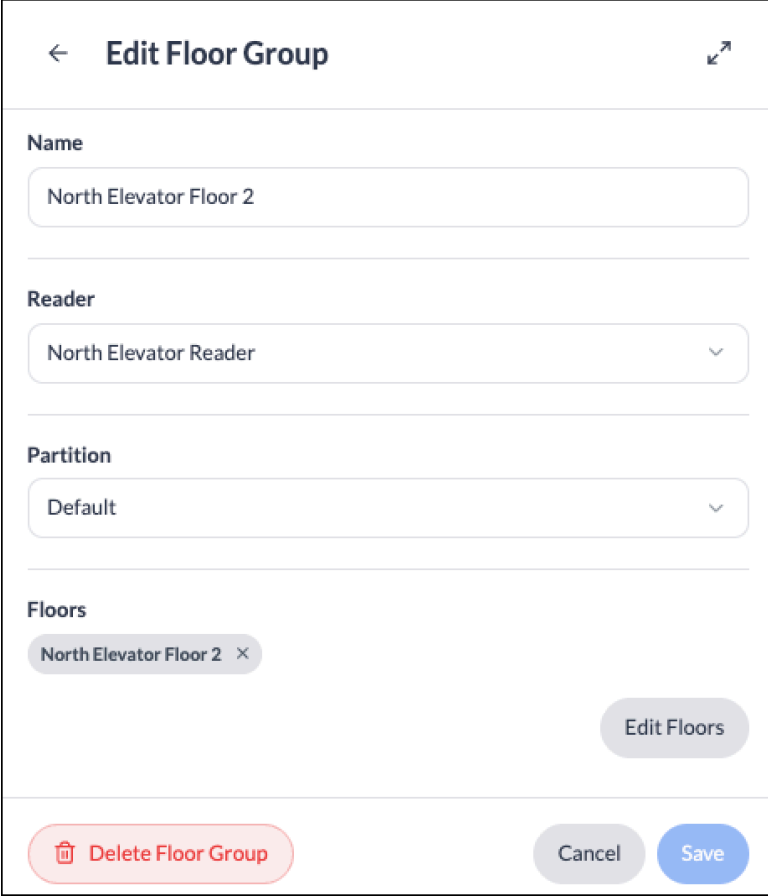
Name - Assign a unique, descriptive name for the **Elevator Floor Group**.

Reader - Select the **Reader** field to select from the configured **Elevator Reader** devices.

Partition - If any additional **Partitions** have been created besides the **Default Partition**, the **Partition** field will be shown. Select the **Partition** field to select a partition from the list.

2.6.2 Editing a Floor Group

After you create an **Elevator Floor Group**, selecting its name displays a drawer where you can edit the **Name**, **Reader**, and **Partition**. In addition, **Elevator Floor Relays**, displayed as **Floors**, must be added to an **Elevator Floor Group** for it to function.



← Edit Floor Group ↗

Name

North Elevator Floor 2

Reader

North Elevator Reader ▾

Partition

Default ▾

Floors

North Elevator Floor 2 ×

Edit Floors

Delete Floor Group Cancel Save

Name - Assign a unique, descriptive name for the **Elevator Floor Group**.

Reader - Select the **Reader** field to select from the configured **Elevator Reader** devices.

Partition - If any additional **Partitions** have been created besides the **Default Partition**, the **Partition** field will be shown. Select the **Partition** field to select a partition from the list.

Floors - Select one or more **Elevator Floor Relay** devices for the floors this **Elevator Floor Group** can access.

2.6.3 Deleting a Floor Group

There are two ways to delete a **Floor Group**.

2.0 Customer Dashboard

1. In the **Floor Group** window, select the trash can icon next to the Floor Group you want to delete.
 2. In the existing Floor Group, select the **Delete Floor Group** button in the lower-left corner of the drawer.
-

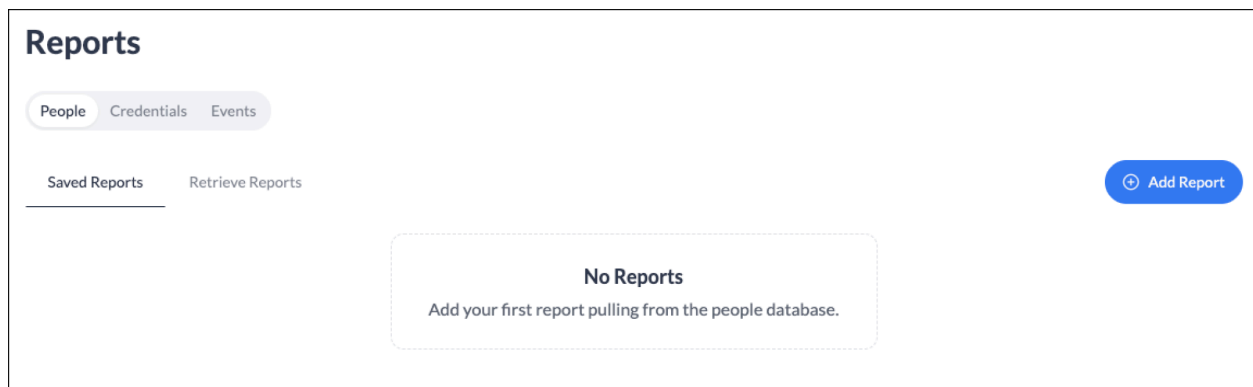
2.7 Reports

Reports allow a user to **Create, Save, Schedule, Retrieve, and Download Reports** that contain details about the **Customer Account**.

To begin, select either **People, Credentials, or Events** depending on the type of **Report** you'd like to create.

2.7.1 People Reports

People Reports allow a user to run **Reports** based on details of the **People** entered into the **Customer Account**.



Adding a People Report

To create a new **People Report**, select the **+ Add Report** button. This is located on the right side of the **People Reports** tab. This opens a drawer where you can enter information for the new **Report**.

When creating a new **People Report**, you must configure several settings.

← **Add Report**

Report Name

Filters

Add Filter

Output

First Name × Last Name ×

Edit Fields

Schedule Report

No schedule ▼

Preview Report

Cancel

Save

Report Name - Enter a descriptive **Name** for the People Report.

Partition - If any additional **Partitions** have been created besides the **Default Partition**, the **Partition** field will be shown.

Filters - Select from the following filter options for the **Report**. After configuring the filters, select **Save**.

First Name - Enter a **First Name** or partial name to filter the People present on the Customer Account. Select the **Condition** of the filter. If the filter must be case-sensitive, toggle **Case Sensitive** on.

2.0 Customer Dashboard

Last Name - Enter a **Last Name** or partial name to filter the People present on the Customer Account. Select the **Condition** of the filter. If the filter must be case-sensitive, toggle **Case Sensitive** on.

Email - Enter an **Email Address** or partial email to filter the People present on the Customer Account. Select the **Condition** of the filter. If the filter must be case-sensitive, toggle **Case Sensitive** on.

Groups - Select which **Groups** to filter on the People present on the Customer Account. Select whether the users are a **Member Of** or **Not Member Of** for the filtered data.

Cards - Enter a **Card Number** or partial card number to filter the People present on the Customer Account. Select between **Equals** or **Does Not Equal** for the filtered data.

Facility Codes - Select which **Facility Codes** were configured for physical Credentials under a Person on the Customer Account to display in the filtered data. Choose between **Equals** or **Does Not Equal** for the filtered data.

Partitions - Select which **Partitions** to filter on the People present on the Customer Account. Select whether the users are a **Member Of** or **Not Member Of** for the filtered data.

Mobile Credentials - Select whether the People present on the Customer Account have different **Mobile Credential** types (**Bluetooth** or **Mobile App**). You can also filter by Credential Status (**Accepted** or **Pending**).

Enabled - Select to view the status of the People present on the Customer Account as either **Enabled** or **Disabled**.

2.0 Customer Dashboard

Output - After selecting the Filters for the **People Report**, the user can choose the details to display when the **Report** is previewed or submitted. The **Output Filters** for a **People Report** are the details on each **Person** on the Customer Account. You can select these **Filter Outputs** by selecting the **Edit Fields** button.

Schedule - Automate Report creation and delivery via email, eliminating the need to generate reports manually each time. Reports can be scheduled to run on a **Daily**, **Weekly**, or **Monthly** basis and sent to one or more **Recipients**.

- **Daily - Report** will be generated **Daily** at the specified time
- **Weekly - Report** will be generated **Weekly** on the specified day and time
- **Monthly - Report** will be generated **Monthly** on the specified date and time
- **No Schedule** - This **Report** will be generated once, at the time of creation

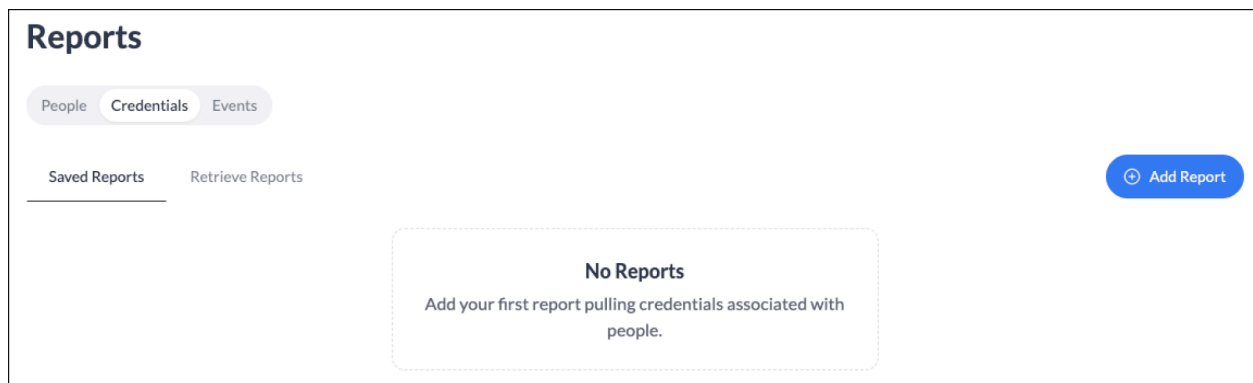
After selecting **Edit Recipients**, a list of potential users will be displayed. To add a user as a **Recipient**, select the email, then **Save**.

The **Report** will not be available to view in the email, but the link will take you to the **Retrieve Report** page. The newest **Report** will be at the top of the page. **Recipients** must have a **PDK.io** login to access the **Report**.

After setting up the **Filters**, **Output**, and **Schedule**, select **Save** or **Preview Report**.

2.7.2 Credential Reports

Credential Reports allow a user to run **Reports** based on the **Credentials** entered on the **Customer Account**.



Adding a Credential Report

To create a new **Credential Report**, select the **+ Add Report** button. This is located on the right side of the **Credential Reports** tab. This opens a drawer where you can enter information for the new **Report**.

When creating a new **Credential Report**, you must configure several settings.

The screenshot shows a drawer titled "Add Report" with a back arrow. It contains several sections: "Report Name" with a text input field; "Filters" with an "Add Filter" button; "Output" with three selected fields ("First Name", "Last Name", "Credential Number") each with a close button, and an "Edit Fields" button; "Schedule Report" with a dropdown menu currently showing "No schedule"; a "Preview Report" button; and at the bottom, "Cancel" and "Save" buttons.

Name - Assign a descriptive **Name** for the **Credential Report**.

Partition - If any additional **Partitions** have been created besides the **Default Partition**, the **Partition** field will be shown.

2.0 Customer Dashboard

Filters - Select the **Filters** field to select the Credential data to be included in the **Credential Report**. Except for **Creation Date** and **Last Scan Date**, you can set these filters to **One Of** or **Not One Of**.

Credential Number or Range - Select specific Credential Number , Credential Number Range , or those that contain certain numbers.
Credential Type - Select between Card , Bluetooth , or Mobile credentials.
Facility Code - Select between any Facility Codes entered on the Customer Account.
Creation Date - Select the Creation Date of the credentials.
Last Scan Date - Select the Last Scan Date of the credentials.
Credential Status - Select the Credential Status . • Enabled - The Person and Credential are active. • Disabled Implicit - The Person is disabled • Pending Redemption - The Bluetooth/Mobile credential invite hasn't been activated/redeemed. • Invitation Expired - The Bluetooth/Mobile invitation that was sent was not activated/redeemed within the allowed period.

Output - After selecting the Filters for the Credential Report, the user can choose the details to display when the **Report** is previewed or submitted. Select these **Filter Outputs** by choosing the **Edit Fields** button.

Schedule - Automate Report creation and delivery via email, eliminating the need to generate reports manually each time. Reports can be scheduled to run on a **Daily**, **Weekly**, or **Monthly** basis and sent to one or more **Recipients**.

- **Daily - Report** will be generated **Daily** at the specified time
- **Weekly - Report** will be generated **Weekly** on the specified day and time
- **Monthly - Report** will be generated **Monthly** on the specified date and time
- **No Schedule** - This **Report** will be generated once, at the time of creation

After selecting **Edit Recipients**, a list of potential users will be displayed. To add a user as a **Recipient**, select the email, then **Save**.

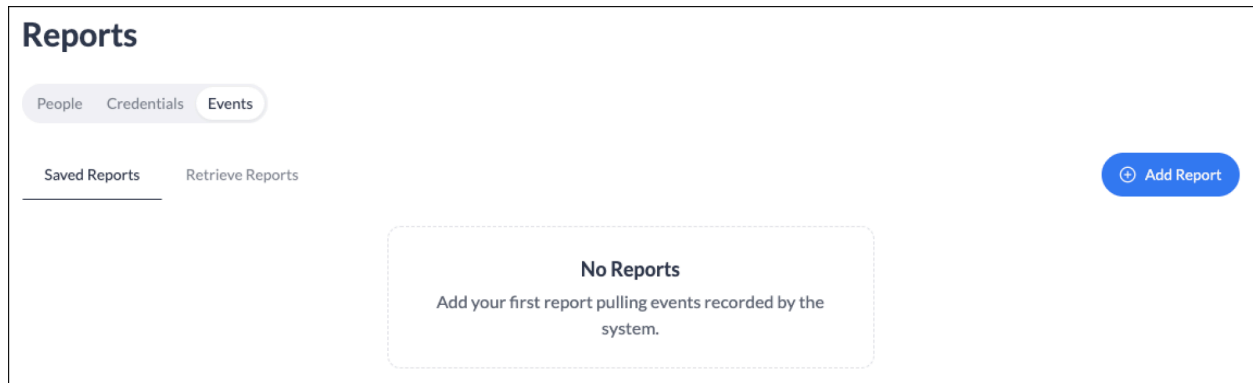
2.0 Customer Dashboard

The **Report** will not be available to view in the email, but the link will take you to the **Retrieve Report** page. The newest **Report** will be at the top of the page. **Recipients** must have a **PDK.io** login to access the **Report**.

After setting up the **Filters**, **Output**, and **Schedule**, select **Save** or **Preview Report**.

2.7.3 Event Reports

Event Reports allow a user to run **Reports** based on the **Events** that have occurred on the **Customer Account**.



Adding an Event Report

To create a new **Event Report**, select the **+ Add Report** button. This is located on the right side of the **Event Reports** tab. This opens a drawer where you can enter information for the new **Event Report**.

When creating a new **Event Report**, you must configure several settings.

← **Add Report**

Report Name

Filters

Occurred
Today

Clear Filter

Edit Filter

Add Filter

Output

Occurred × Info Text × Event × Result × Details ×

☒ Export Details into Columns

Edit Fields

Schedule Report

No schedule ▼

Preview Report

Cancel

Save

Name - Assign a descriptive **Name** for the **Event Report**.

Partition - If any additional **Partitions** have been created besides the **Default Partition**, the **Partition** field will be shown.

2.0 Customer Dashboard

Filters - Select from the following filter options for the **Report**. For all filters except **Occurred**, a user can select whether to include or exclude the selected item(s) (**One Of**, **Not One Of**) from the Report.

Occurred - Select a date or date range.
Events - Select the Event type.
Results - Select the Result type.
Battery Charge Level Change - Select the Battery Charge Level status.
Devices - Select the Device's name.
People - Select the Person's name.
Cards - Select the physical credential number.
Connections - Select the Connection's name.
Groups - Select the Group's name.

Output - After selecting the **Filters** for the **Event Report**, the user can choose the details to display when the **Report** is previewed or submitted. Users can select these **Filter Outputs** by selecting the **Edit Fields** button. When the **Report** is downloaded, you can export the details into separate columns by toggling on **Export Details into Columns**.

Schedule - Automate report creation and email delivery, eliminating the need to generate reports manually each time. Reports can be scheduled to run on a **Daily**, **Weekly**, or **Monthly** basis and sent to one or more **Recipients**.

- **Daily - Report** will be generated **Daily** at the specified time
- **Weekly - Report** will be generated **Weekly** at the specified day and time
- **Monthly - Report** will be generated **Monthly** on the specified date and time
- **No Schedule** - This **Report** will be generated once, at the time of creation

After selecting **Edit Recipients**, a list of potential users will be displayed. To add a user as a **Recipient**, select the email, then **Save**.

The **Report** will not be available to view in the email, but the link will take you to the **Retrieve Report** page. The newest **Report** will be at the top of the page. **Recipients** must have a **PDK.io** login to access the **Report**.

2.0 Customer Dashboard

After setting up the **Filters**, **Output**, and **Schedule**, select **Save** or **Preview Report**.

2.7.4 Previewing or Submitting a Report

Reports

People

Credentials

Events

Saved Reports

Retrieve Reports

Add Report

Name	Scheduled	Last Run	Next Run	
Credential Test Report	-	-	-	
Test	Daily	2026-07-29 11:00:00	2026-07-30 11:00:00	

After selecting the desired **Filters** and **Output** details, the user can **Preview** the selected report. Select the **Preview Report** button. This **Preview** displays up to 50 entries based on the selected **Output filters**. When you change **Filters** or **Output** selections, or when new events occur, select **Preview** again to update the report preview.

Preview Report

Close Preview

Submit

After **Previewing a Report**, select the **Submit** button so you can open the **report** result again later or download it in the **Retrieve Reports** tab. If you Preview and Submit a Report without saving it, the system generates it without a descriptive name. The Report's retrievability period depends on the Reporting Plan.

NOTE: Each **saved report** displays the **Name**, **Schedule**, **Last Run**, and **Next Run**.

2.7.5 Retrieving a Report

Reports

People

Credentials

Events

Saved Reports

Retrieve Reports

 Filters

Submitted		Name	Submitter	Credentials		
		2026-07-30 10:51:46	Expired Invitations	10		
		2026-07-30 10:51:19	Enabled	5004		
		2026-07-30 10:49:25	-	5014		
		2026-07-30 05:00:27	Test	Scheduled	5014	

After a Report is **Submitted**, you can retrieve it later, within the limits of the Reporting Plan for the Customer Account. Any previously **Submitted Reports** will be displayed in the **Retrieve Reports** tab. Selecting the downward arrow icon will allow a user to download the Report (JSON, HTML, or CSV). Selecting the magnifying glass icon next to a Submitted Report lets a user view the Report and when it was submitted.

2.7.6 Scheduling a Report

Users with **Integrator, Admin, Manager, or Reporter-level permissions** can automate the creation and delivery of **Reports** (People, Credentials, or Events) via email, eliminating the need to generate them manually each time. **Reports** can be scheduled to run on a **Daily, Weekly, or Monthly** basis and sent to one or more **Recipients**.

Schedules

- **Daily - Report** will be generated **Daily** at the specified time
- **Weekly - Report** will be generated **Weekly** on the specified day and time
- **Monthly - Report** will be generated **Monthly** on the specified date and time
- **No Schedule** - This **Report** will be generated once, at the time of creation

Recipients

2.0 Customer Dashboard

After selecting **Edit Recipients**, a list of potential users will be displayed. To add a user as a **Recipient**, select the email, then **Save**.

Add Recipients

Select recipients for the scheduled report

Search People

@prodatakey.com

@prodatakey.com

@prodatakey.com

@prodatakey.com

Select All

Cancel

Save (0)

NOTE: The **Report** will not be available to view in the email, but the link will take you to the generated **Report**. **Recipients** must have a **PDK.io** login to access the **Report**.

Saved Reports

Each **Saved Report** will display the **Name**, **Schedule Type**, **Last Run Date**, and **Next Run Date**.

Name	Scheduled	Last Run	Next Run	
Scheduled Report Test	Weekly	2026-01-09 10:32:00	2026-01-16 10:32:00	

Report Delivery

At the previously scheduled date and time, **Recipients** will receive an automated email with a link to the generated **Report**. This email will be sent from **ProdataKey Cloud Systems** (**no-reply@accounts.pdk.io**). The subject line includes the **Report Name** and the scheduled date and time. After selecting **View Report**, you will be redirected to log in to your **PDK.io** account.

Below is an example of a **Scheduled Report** email.

Copyright © 2026 ProdataKey. All rights reserved.
REV 2.0.0

122

Your Daily Report Report from PDK.io – 2026-01-14 19:00:02

ProdataKey Cloud Systems <no-reply@accounts.pdk.io>
to me ▾



Your **Daily Report** Report from PDK.io – **2026-01-14 19:00:02**

Your PDK.io Report for **High Rise Security** is ready to review.

This report was generated automatically based on your schedule preferences in PDK.io. It includes the latest data for the period:

2026-01-14 19:00:02 → 2026-01-14 19:00:03

[View Report](#)

About This Report

People Report: Includes all user records within the customer account, including names, access levels, and contact details.

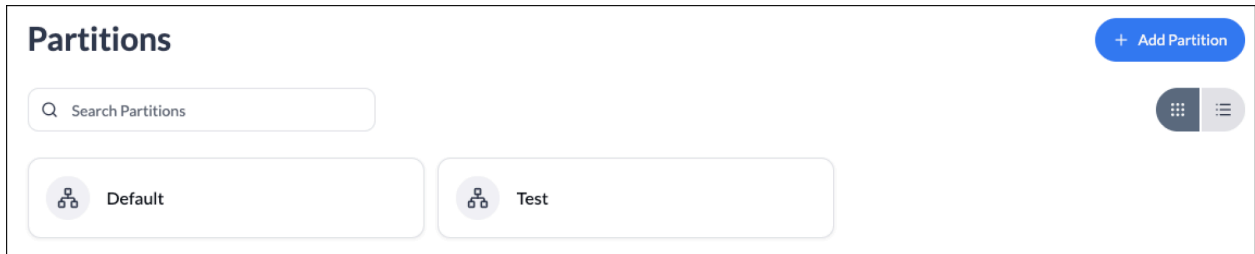
Thank you for using PDK.io!

[Contact PDK](#) | [Manage Report Schedule or Preferences](#)



ProdataKey

2.8 Partitions

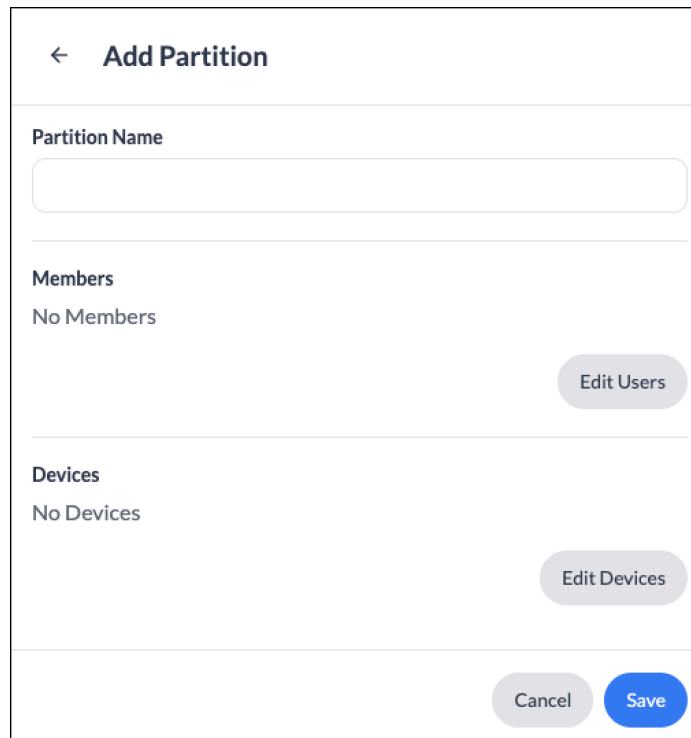


The screenshot shows the 'Partitions' management window. At the top left is the title 'Partitions'. To the right is a blue button labeled '+ Add Partition'. Below the title is a search bar with the placeholder text 'Search Partitions'. At the bottom, there are two partition cards: 'Default' and 'Test', each with a group of three people icon.

Partitions allow a **Manager** or **Reporter** to access only the **People**, **Groups**, and **Rules** to which they are assigned management duties. This is commonly used for one or more floors within a building, a department, individual tenants in a multi-tenant building, or other selected **Doors** on a **Customer Account**. **Permissions** for **Integrator** and **Admin** can grant **Managers** or **Reporters** access to **Partitions**. You can also locate a **Partition** using the search bar above the list of **Partitions**.

2.8.1 Adding a Partition

To create a new **Partition**, first select **+ Add Partition** in the **Partitions** window. This opens a drawer where you can enter the information for the new **Partition**.



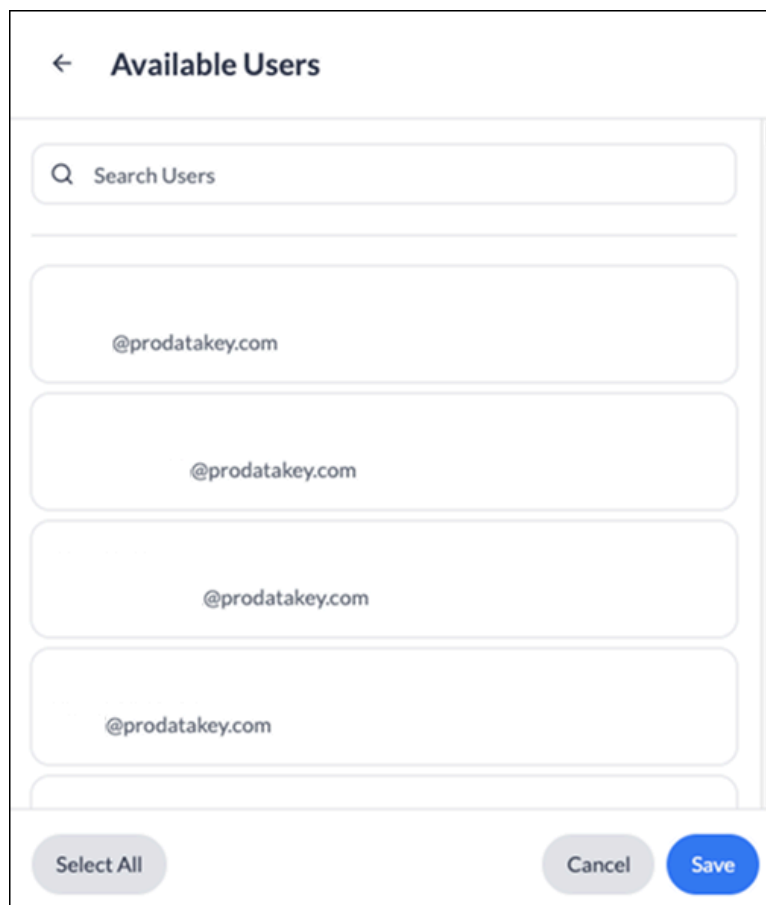
The screenshot shows the 'Add Partition' drawer. At the top left is a back arrow and the title 'Add Partition'. Below the title is a 'Partition Name' label and an empty text input field. Below that is a 'Members' label and the text 'No Members'. To the right of 'No Members' is a button labeled 'Edit Users'. Below that is a 'Devices' label and the text 'No Devices'. To the right of 'No Devices' is a button labeled 'Edit Devices'. At the bottom right are two buttons: 'Cancel' and 'Save'.

2.0 Customer Dashboard

Partition Name - Enter a descriptive name for the **Partition** in this field.

Members - Select the **Edit Users** button to add **users** with **Permissions** for the **Customer Account** to manage the **Partition**. After selecting the **User(s)** and highlighting them, select the **Save** button below the list of **Users** to add them to the new **Partition**, then return to the **Partition** creation drawer.

NOTE: **Integrators** and **Admins** have full access to all information in the **Customer Account**, regardless of **Partition** assignment.



Devices - Select the **Edit Devices** button to add **Devices** to the **Customer Account** for management in the **Partition**. After selecting the **Device(s)** and highlighting them, select the **Save** button below the list of **Devices** to add them to the new **Partition**, then return to the **Partition** creation drawer.

←

Devices

Q

Search Devices

☐

West Lobby
Kansas City

☐

Deliveries
Omaha

☐

Executive Bathroom
Omaha

☐

Executive Parking
Omaha

☐

Front Entrance
Omaha

☐

Studio
Omaha

☐

North Lobby
St. Paul

Select All

Cancel

Save (0)

After naming the new **Partition** and adding managed **Users** and **Devices** to the **Partition**, select the **Save** button in the bottom-right corner of the drawer to complete adding the new **Partition** to the **Customer Account**.

2.8.2 Editing a Partition

After you create a **Partition**, selecting its name displays a drawer menu where you can edit the **Partition Name**, **Members**, **Devices**, and **Custom Fields** (if used). Please note that you cannot rename the **Default Partition**.

←

Edit Partition

Partition Name

Default

Members

No Members

Edit Users

Devices

Kansas City

Delivery Dock × Testing This × West Lobby ×

Omaha

Deliveries × Executive Bathroom × Executive Parking ×

Front Entrance × Studio ×

St. Paul

North Lobby ×

Edit Devices

Custom Fields

↑

↓

+ Add Custom Field

Field ID: Phone Number

Number

Field Visibility | Visible

Required | False

Minimum | 0

Maximum | 10

Decimal Precision | 0

Cancel

Save

2.0 Customer Dashboard

The **Partition Name**, **Members**, and **Devices** fields work the same way as when you initially add the **Partition** to the **Customer Account**.

Custom Fields - To add a custom field to **People** in the **Partition**, select the **Create Custom Field** button to open the Custom Fields window.

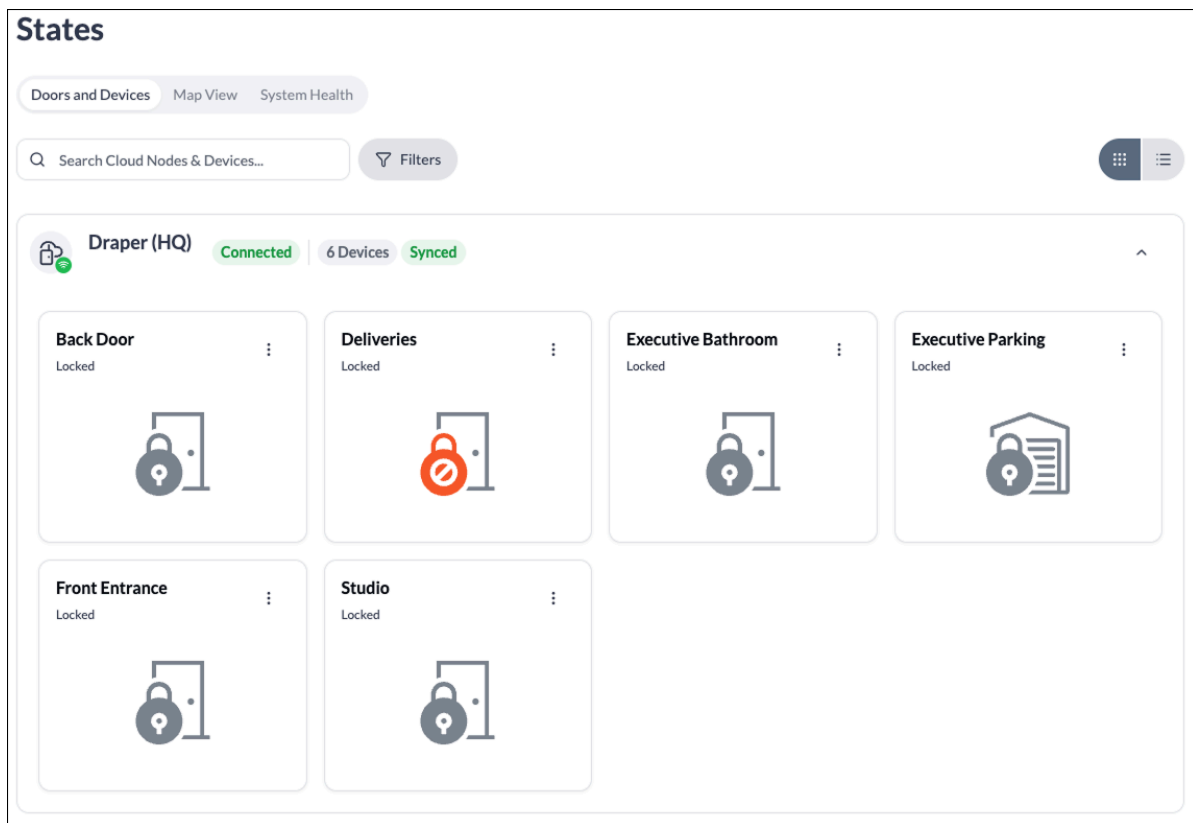
2.8.3 Deleting a Partition

To delete a Partition, select the **Delete Partition** button in the lower-left corner of the drawer.

NOTE: The Default Partition cannot be deleted.

2.9 States

2.9.1 Doors and Devices View



2.0 Customer Dashboard

The **Doors and Devices** view lets you see and control the Doors and Devices on the system. The search field lets you search by Cloud Node or Device names.

How to Filter the Doors and Devices View

Expanding the Filters section allows a Partner to search for and limit which Devices or Doors are displayed.

The screenshot shows a modal dialog titled "Filters" with a back arrow icon. It contains two main sections: "Filters" and "Display Options".

Filters Section:

- Cloud Nodes:** A dropdown menu with a downward arrow.
- Types:** A dropdown menu with a downward arrow.
- Controllers and Hubs:** A dropdown menu with a downward arrow.
- States:** A dropdown menu with a downward arrow.

Display Options Section:

- Name A to Z:** A radio button that is currently selected.
- Name Z to A:** An unselected radio button.
- Group by Type:** A toggle switch that is currently turned off.

Buttons:

- Reset Filters:** A light gray button.
- Cancel:** A light gray button.
- Apply Filters:** A blue button.

- **Cloud Nodes** - This will display Doors and Devices connected to the selected Cloud Node.
- **Types** - This will only display Doors, Elevators, or IO devices of the selected type(s).

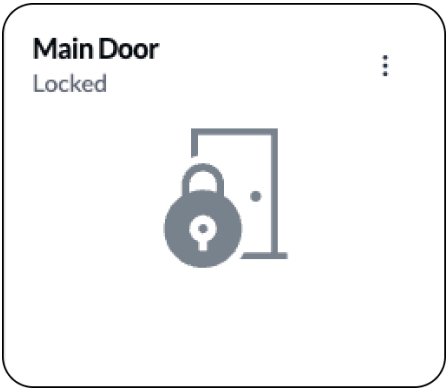
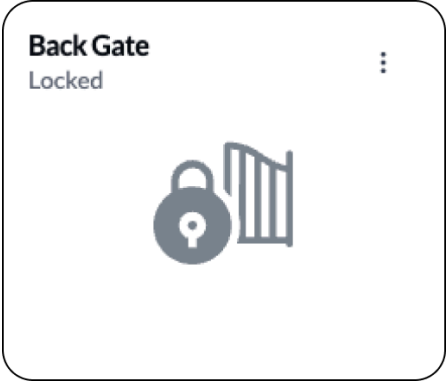
2.0 Customer Dashboard

- **Controllers and Hubs** - This displays only Devices or Doors connected to the selected Controller or Hub on the Customer Account.
 - **States** - This displays Doors and Devices currently in the selected State.
-

Doors and Devices Icons

The **Door and Devices** view displays a list of configured Doors and Devices in alphanumeric order beneath the **Filters** header. Different states or conditions are displayed by different icons.

Below are the Doors or Devices available on a **Customer Account**. These icons are selected in **Configuration**.

Device Type	Name	Icon
Primary Reader	Swinging Door	 The icon shows a rounded rectangle containing the text 'Main Door' in bold and 'Locked' below it. In the top right corner is a three-dot menu icon. In the center is a padlock icon superimposed on a door frame.
Primary Reader	Swinging Gate	 The icon shows a rounded rectangle containing the text 'Back Gate' in bold and 'Locked' below it. In the top right corner is a three-dot menu icon. In the center is a padlock icon superimposed on a gate structure.

2.0 Customer Dashboard

Primary Reader	Roll-up Door	Garage Locked 
IO Device	Swinging Door	Back Door  A B
IO and Premium IO Device	Alarm	Side Door  A B

2.0 Customer Dashboard

IO and Premium IO Device	Fan	Office A B
IO and Premium IO Device	Light	Storage A B
IO and Premium IO Device	Button	Front Desk A B

2.0 Customer Dashboard

IO and Premium IO Device	Sprinkler	Main Office  A B
IO and Premium IO Device	Other	Break Room  A B

Below is a list indicating the state of the Doors or Devices and their corresponding meanings.

	
A closed Door/Gate in a locked state.	An open Door/Gate in a locked state.

2.0 Customer Dashboard

	
A Door/Gate is not communicating and was closed when communications were lost.	A Door/Gate is not communicating and was open when communications were lost.
	
A closed Door/Gate in an Unlocked state.	An open Door/Gate in an Unlocked state.
	
A closed Door/Gate in a 'Do Not Disturb' (DND) state.	An open Door/Gate in a 'Do Not Disturb' (DND) state.
	
A closed Door/Gate that is locked during an 'Auto-Open after First-Allowed' schedule, but no Credential entry has occurred.	An open Door/Gate that is locked during an 'Auto-Open after First-Allowed' schedule, but no Credential entry has occurred.

	
A closed Door/Gate that is unlocked during an Auto-Open schedule.	An open Door/Gate that is unlocked during an Auto-Open schedule.

Doors and Devices Alerts

If there is a problem or potential issue with the state of the door, such as the door being propped, having been forced open, a controller issue occurring, or the Device being toggled into an unlocked state (remaining unlocked until '**Force Toggle**' is again), these conditions will be displayed on the upper left and right areas around the central icon. Below are images showing some of the icons for potential issues.



Doors and Device Actions

Selecting the kabob button (three vertical dots) in the upper right corner of the Door or Device will allow you to access certain **Device Actions**.

Device Actions

Unlock

DND

Force Toggle

Silence Piezo

View Controller Health

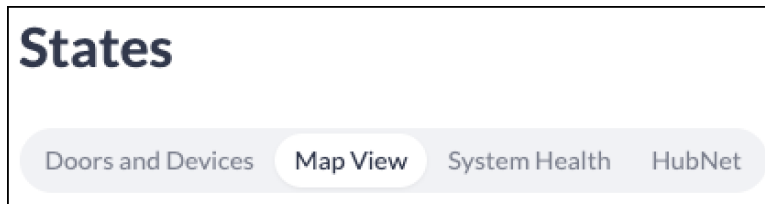
View Device Config

Device Type	Available Actions
Door or Gate	• Unlock or Lock • DND • Force Toggle • Silence Piezo • View Controller Health • View Device Config
Red Wireless Lock	• Unlock or Lock • DND • Force Toggle • Silence Piezo • View Controller Health • View Device Config
IO Device	• View Controller Health • View Device Config
Premium IO Device	• Activate • DND • Force Toggle • Silence Piezo • View Controller Health • View Device Config

2.0 Customer Dashboard

Elevator Reader	• Activate Floor Group • DND • DND Floor • Silence Piezo • View Controller Health • View Device Config
-----------------	--

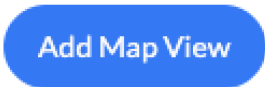
2.9.2 Map View



Map View allows a user with the appropriate Permissions to set up, edit, view, and control **Doors and Devices** in a Customer Account.

To start using **Map View**, a Partner with appropriate Permissions must add an image, such as a blueprint or rendering of the location, to display in the **Map View**.

Adding a Map View

A blue, rounded rectangular button with the text "Add Map View" in white, centered within the button.

Select **Add Map View** in the upper right corner.

← Add Map View

Name

The Name is a fully descriptive name that is displayed on the View Selector.

Short Name

The Short Name is an abbreviated name that is used with Link Icons.

Image

Click to upload or drag and drop
JPG, JPEG, PNG, SVG

Partitions

Default ×

Edit Partitions

Close

Done

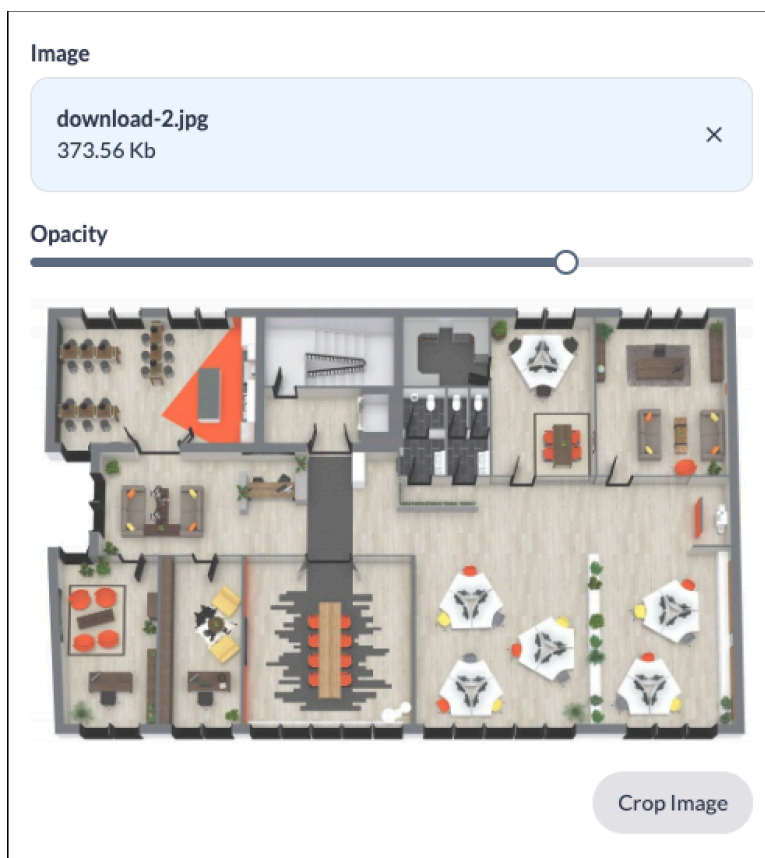
Name - Enter the **Name**, which will be shown in the Map View once setup is complete.

Short Name - Enter the **Short Name**, which will be displayed and used when linking Map Views together.

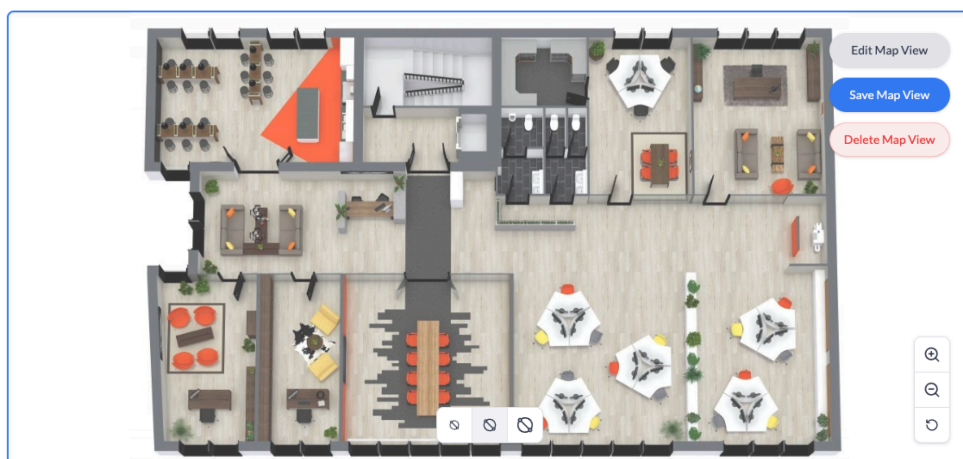
Image - Select **Click to upload** to open a dialog box, then browse to and open the image you want to use. After uploading the image, adjust the image's **Opacity** and **Crop the Selected Image** if needed.

Partitions - Select the **Partition** whose Managers have access to control Doors in the Map View.

2.0 Customer Dashboard



After making any necessary adjustments, select **Done** to save your changes.



Select **Edit Map View** to add **Devices** and **Links**.

2.0 Customer Dashboard

Partitions

Default × NASA × SpaceX ×

Edit Partitions

Devices

Delivery Dock × West Lobby × Deliveries × Executive Parking ×

Front Entrance ×

Edit Devices

Links

Office × Second Floor ×

Edit Links

Delete Map View

CloseDone

Select **Edit Devices**, then select the devices to include on the **Map View**.

← Edit Devices

All Devices

Q

Delivery Dock

Kansas City



Testing This

Kansas City



West Lobby

Kansas City



Deliveries

Omaha



Unselect All

Cancel

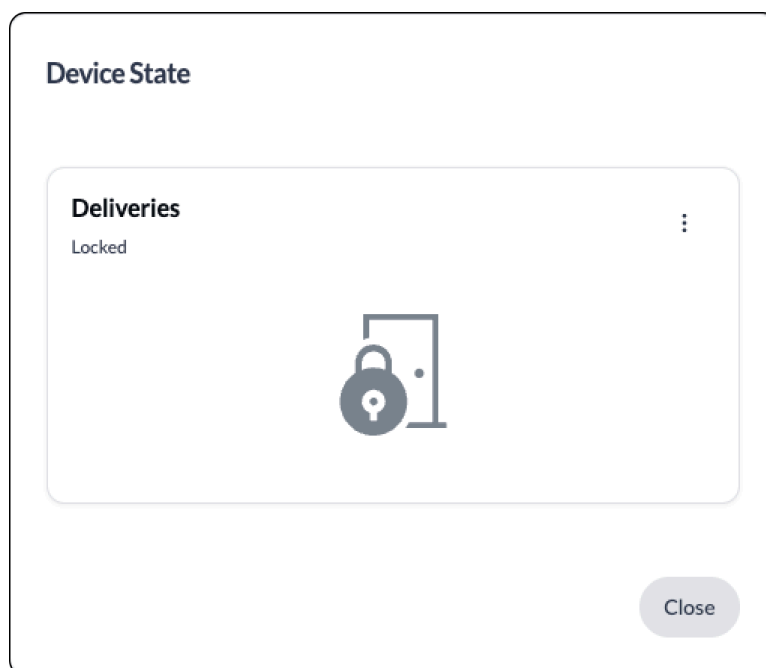
Save

After adding the **Door** or **Device**, you can drag it around the **Map View** to where it is physically located on the image.

2.0 Customer Dashboard



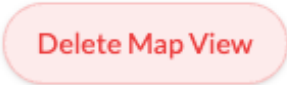
In **Map View**, selecting a Device displays the same **Device Actions** as in the Doors and Devices view.



Editing Map View

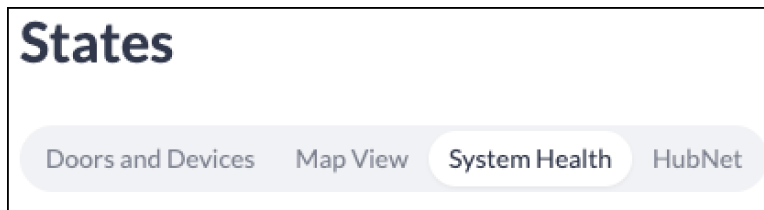
After you create a **Map View**, selecting **Edit Map View** opens a drawer where you can edit the details above.

Deleting a Map View

A red, rounded rectangular button with the text "Delete Map View" in white.

To delete a Map View, select the **Delete Map View** button.

2.9.3 System Health View



The **System Health** window enables users to quickly assess the current condition of the hardware (Cloud Nodes, Connections, and Red Locks) on their Customer Account.

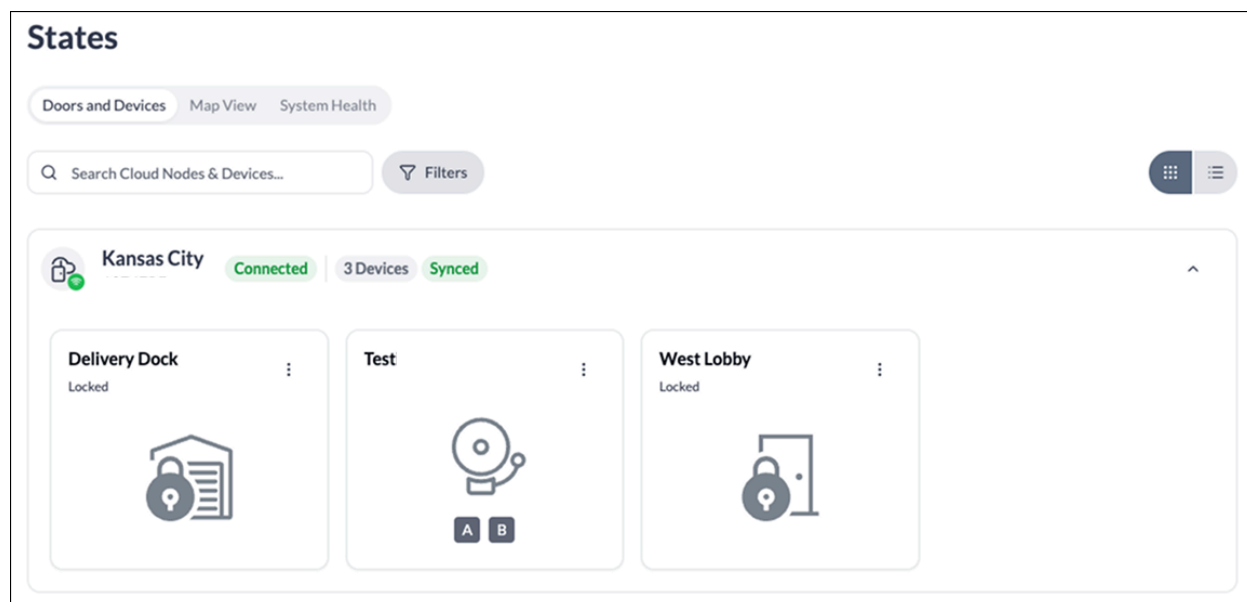
The **System Health** window can be accessed in two different ways, both of which are detailed below:

- Select **System Health** in the upper-right corner of the **Customer Dashboard**, as shown in the image below.

2.0 Customer Dashboard



- In the States window, select **System Health**, as shown in the image below.



In the **System Health** window, all Cloud Nodes, Connections, and Red Locks are displayed by default. Each Cloud Node registered on the system will have its associated hardware listed below it. You can also find a Cloud Node, Connection, or Device using the search bar above the System Health view.

2.0 Customer Dashboard

States

Doors and Devices Map View **System Health**

Filters

Kansas City 2 Devices **Synced**

Device Name	Status	Sync Status	Sync Completed	Software Version
Onboard Controller	Connected	Synced	07/30/2026, 16:34:48	2.4.5
Red 1 Door Controller (R1)	Connected	Synced	07/30/2026, 16:34:48	2.4.5

Omaha 2 Devices **Synced**

Device Name	Status	Sync Status	Sync Completed	Software Version
Onboard Controller	Connected	Synced	07/30/2026, 16:34:48	2.4.5
Red 4 Door Controller (R4)	Connected	Synced	07/30/2026, 16:34:47	2.4.5

Filtering and Table Options

Next to the **Search Cloud Nodes & Devices** section in the **System Health** window, you can use the **Filters** button.

Selecting the **Filters** button opens a drawer where you can choose which filters and table options to apply. After configuring any filters, select **Apply Filters**. To clear all changes and return to the defaults, select **Reset Filters**.

← Filters

Filters

Cloud Nodes

Controllers and Hubs

Status

Sync Status

Connection Types

- **Cloud Nodes** - This filter displays the hardware connected to the selected Cloud Node(s).
- **Controllers and Hubs** - This filter displays hardware for the selected items.
- **Status** - This filter displays the hardware with the selected **Status**.
- **Sync Status** - This filter displays hardware with the selected **Sync Status**.
- **Connection Types** - This filter displays hardware with the selected **Connection Type**.

The **Table Options** let users display different columns in the **Cloud Node** table by toggling each associated section on or off.

Table Options



Status



Sync Status



Sync Completed



Software Version



Connection Type



Battery

- **Status** - Displays the Status, showing the overall status of the hardware.
- **Sync Status** - Displays the Sync Status.
- **Sync Completed** - Displays when the hardware last synced with the Cloud database.
- **Software Version** - Displays the firmware version of the hardware.
- **Connection Type** - Displays the Connection Type for the hardware.
- **Battery** - Displays whether the hardware has a backup battery connected and the corresponding charge percentage.

Status

Each Cloud Node, Connection, and Red Lock added to the Customer Account displays the hardware's current status.

- **Connected** - The hardware is currently connected to the Cloud Database, meaning any changes can be synced to the hardware.

2.0 Customer Dashboard

- **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, Red Connection, and Red Lock will show the current **Sync Status**.

- **Pending** - This status indicates pending changes waiting to sync with the Cloud Node or Controller. This can commonly occur due to pending Cloud Node updates, offline Controllers or Red Locks (which will sync upon re-connection), and other temporary conditions.
- **Syncing** - This status indicates that the hardware 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 hardware is in this Status, please contact **ProdataKey Support**.

NOTE: Certain hardware will never sync to the Cloud database and will display a dash in the **Sync Status** and **Sync Completed** column.

←



Kansas City

Status	Connected
IPv4 Address	
IPv6 Address	
MAC Address	
Serial Number	
Software Version	2.5.4
API Software Version	2.5.4
Sync Status	Synced
Last Synced Time	07/30/2026, 16:34:47

2.0 Customer Dashboard

- **Status** - Displays whether the Cloud Node is Connected to the Cloud database (Online) or Disconnected (Offline)
- **IPv4 Address** - Displays the DHCP or static IPv4 Address
- **IPv6 Address** - Displays the IPv6 Address
- **MAC Address** - Displays the MAC Address for the network adapter in the Cloud Node.
- **Serial Number** - Displays the Serial Number of the Cloud Node
- **Software Version** - Displays the version of software running on the Cloud Node that communicates with the cloud.
- **API Software Version** - Displays the version of software running on the Cloud Node that manages access control activity
- **Sync Status** - Displays the current Sync Status of the Cloud Node to the Cloud database.
- **Last Synced Time** - Displays when the Cloud Node last synced to the Cloud database.

Controller Health Details

  **Red 1 Door Controller (R1)**

Status	Connected
Connection Type	Ethernet
Device Type	Controller
Device Model	Red 1
IPv4 Address	
IPv6 Address	
MAC Address	
Battery Charge	No Battery
Serial Number	
Firmware Version	2.4.5
Sync Status	Synced
Last Synced Time	07/30/2026, 16:34:48
Connection Unstable	No
Power Source	Power over Ethernet (PoE)
Overcurrent	No
Undervoltage	No
Low Power Mode On	No
Input Power On	Yes
Input Current	< 0.05 A
Input Voltage	15.008 V
Peripheral Power On	Yes
Peripheral Current	< 0.05 A
Peripheral Voltage	12.096 V
Radio Timeout	No

Restart Controller

View Config

View State

- **Status** - Displays whether the Controller is Connected to (Online) or Disconnected from (Offline) the Cloud Node.
- **Connection Type** - Displays whether the Controller is an Onboard, Ethernet, or Wireless Controller.
- **Device Type** - For a Controller, this will always be Controller.
- **Device Model** - Displays the Controller model.
- **IPv4 Address** - Displays the DHCP or static IPv4 Address
- **IPv6 Address** - Displays the IPv6 Address
- **MAC Address** - Displays the Controller's MAC Address.
- **Battery Charge** - Displays the estimated charge level of an attached battery (if present) or if no battery is installed.
- **Serial Number** - Displays the Controller's serial number. This is also printed on a sticker on the board.
- **Firmware Version** - Displays the version of the firmware running on Red-series Controllers
- **Sync Status** - Displays the Controller's current sync status to the Cloud database.
- **Last Synced Time** - Displays when the Controller last synced to the Cloud database.
- **Connection Unstable** - Indicates whether the Controller has lost or regained communication repeatedly during a brief period.
- **Power Source** - Displays the Controller's power source.
- **Overcurrent** - Indicates whether the Controller is currently in an Overcurrent state.
- **Undervoltage** - Indicates whether the Controller is receiving sufficient voltage from its power input.
- **Low Power Mode On** - Displays whether the Controller is operating in Low Power Mode. Low Power Mode is when a Controller with a low battery powers off any attached devices (Reader, REX, locking hardware, etc.) to maintain battery life
- **Input Power On** - Displays whether primary external power is connected.
- **Input Current** - Displays the Controller's input power current.
- **Input Voltage** - Displays the Controller's input power voltage.
- **Peripheral Power On** - Indicates whether the Controller is in a State where it supplies power to connected peripheral devices.
- **Peripheral Current** - Displays the current draw for peripherals connected to the Controller.
- **Peripheral Voltage** - Displays the voltage supplied to peripherals connected to the Controller.
- **Radio Timeout** - Displays whether the WiMAC module is in a communication failure.

Hub Health Details

←  Red Hub - Engineering	
Status	Connected
Connection Type	Ethernet
Device Type	Red Hub
IPv4 Address	
IPv6 Address	
MAC Address	
Serial Number	
Firmware Version	1.1.6
Connection Unstable	No
Power Source	Power over Ethernet (PoE)
Input Current	< 0.05 A
Input Voltage	51.792 V
Restart Device Reset Device View Config	

- **Status** - Displays whether the Hub is Connected to (Online) or Disconnected from (Offline) the Cloud Node.
- **Connection Type** - Displays that the Hub is connected via Ethernet.
- **Device Type** - For a Red Hub, this will always be Hub.
- **IPv4 Address** - Displays the IPv4 Address.
- **IPv6 Address** - Displays the IPv6 Address.
- **MAC Address** - Displays the Hub's MAC Address.
- **Serial Number** - Displays the Hub's serial number. This is also printed on a sticker on the back of the Hub.
- **Firmware Version** - Displays the firmware version currently running on the Hub.
- **Connection Unstable** - Indicates if the Hub has repeatedly lost and regained communication within a short period.
- **Power Source** - Displays the Hub's power source.
- **Input Current** - Displays the Hub's input power current.
- **Input Voltage** - Displays the Hub's input power voltage.

Wireless Lock Health Details

  **Sales Office**

Status	Connected
Connection Type	PDK HubNet
Device Type	Wireless Lock
Device Model	SDS
MAC Address	
Battery Charge Level	79%
Serial Number	
Firmware Version	1.1.5
Sync Status	Synced
Last Synced Time	07/31/2026, 09:30:58
Connection Unstable	No
Jammed	No
Input Current	< 0.05 A
Input Voltage	5.779 V

Restart Device

Reset Device

View State

- **Status** - Displays whether the Lock is Connected to (Online) or Disconnected from (Offline) the Hub.
- **Connection Type** - Displays the connection type, which is always **HubNet** for Wireless Locks.
- **Device Type** - For a Lock, this will always be Wireless Lock.
- **Device Model** - Displays the Device Model type. Deadbolt (KMS), Cylindrical (SDS), Interconnected (CLS).
- **MAC Address** - Displays the Lock's MAC Address.

- **Battery Charge Level** - Displays the estimated remaining battery charge.
- **Serial Number** - Displays the Lock's serial number. This is also printed on a sticker on the Lock.
- **Firmware Version** - Displays the firmware version currently running on the Lock.
- **Sync Status** - Displays the current sync state.
- **Last Sync Time** - Displays the most recent time the Controller database synced with the Cloud database.
- **Connection Unstable** - Indicates if the Lock has repeatedly lost and regained communication within a short period.
- **Jammed** - Displays if the Deadbolt is in a Jammed state.
- **Input Current** - Displays the Lock's input power current.
- **Input Voltage** - Displays the Lock's input power voltage.

System Health Actions

View State - Takes the User to a filtered **Doors and Devices** view, showing only the Devices connected to the selected connection.

View Config - Available only to Partners with Integrator Permissions, this takes the User to the **Connection Configuration** page for the selected Connection.

Restart Controller - Available only to Partners with Integrator Permissions, this option restarts the selected Controller, similar to power cycling the Controller.

Restart Device - Available only to Partners with Integrator Permissions, this option restarts the selected Hub or Lock, similar to power cycling.

Reset Device - Available only to Partners with Integrator Permissions, this option resets the selected Hub or Lock, similar to a physical soft reset.

2.9.4 HubNet View

States

Doors and Devices

Map View

System Health

HubNet

This section lets you monitor and search for **HubNet(s)** on your system.

The table displays:

- Wireless Lock Name
- Connected Hub
- Signal Strength

 Draper Locks

Wireless Lock	Hub Connection	Signal Strength
Sales Office - Left - Cylindrical	Red Hub - Engineering	
Mktg Storage Room - Deadbolt	Red Hub - Support	
PM Storage Room Cylindrical	Red Hub - Engineering	
Sales Office - Right - Cylindrical	-	

NOTE: On each page refresh, **HubNet** monitors signal strength and determines the best **Hub** to use when connecting to a **Wireless Lock**.

Signal Details

Signal Details

Signal Quality



RSSI

-44 dBm

Selecting a **Wireless Lock** will open the **Signal Details** view, which includes the **Wireless Lock's** **RSSI** (Received Signal Strength Indicator).

2.0 Customer Dashboard

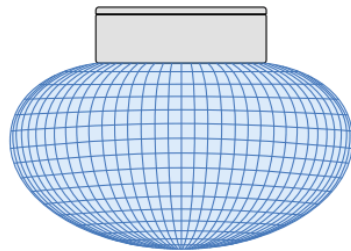
RSSI Range	Quality	Description
-60 dBm or higher	Excellent	Maximum signal strength
-61 dBm to -69 dBm	Good	Strong, reliable connection
-70 dBm to -79 dBm	Fair	Adequate for most uses
-80 dBm or lower	Poor	Weak signal, may drop

Understanding RSSI

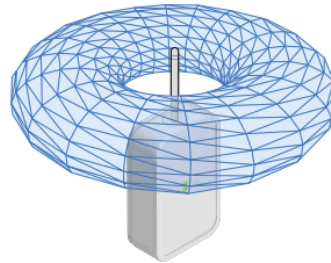
- RSSI (Received Signal Strength Indicator) measures the strength of the radio signal between the Hub and a Wireless Lock, expressed in dBm (decibels relative to one milliwatt).
- Values closer to 0 dBm indicate stronger signals and generally better connection reliability.
- Signal strength is dynamic and *will* change over time.

Range

To ensure optimal signal quality, maintain a clear line of sight between the **Hub** and the outside of the **Wireless Lock**.



internal
antenna



external
antenna

- **Internal Antenna:** up to 70 feet
- **External Antenna:** up to 100 feet

Factors that will reduce range and signal strength include:

- Environmental obstacles (walls, metal, concrete, elevator shaft, etc.)
- Radio signal reflections
- Wireless interference from nearby devices
- The overall health and load of your network

NOTE: Test signal strength with the door open and closed.

If you consistently receive **Poor Signals**, consider relocating the **Hub** to a more central location relative to the **Wireless Locks** or adding additional **Hubs** to enhance coverage.

Wireless Locks with Poor Signal Strength may experience:

- Decreased battery life
- Slower reaction times to remote commands
- Longer Firmware upgrade times

NOTE: If there is no signal and the **Wireless Lock** is within range of the **Hub**, ensure that the correct **Antenna Type** is configured

2.0 Customer Dashboard

Filters

Can filter for **Signal Strength(s)** or **Hub Connection(s)**

Signal Strength ▾

Excellent

Good

Fair

Poor

None

✓

✓

✓

✓

✓

Connection ▾

Red Hub - Engineering

Red Hub - Support

Red Hub - Hall

✓

✓

✓

2.10 Live Events

Live Events will display certain Events that occur on a Customer Account. The displayed Events relate to Credential scans and Hardware Events. All Permission roles have access to the **Live Events** features.

Live Events		
Live Events Debug Mode ▾ Filters		
Time	Location	Result
08/10/2026 15:55:01	Northwest Trust	Auto Open has been enabled on the device Main Door.
08/10/2026 15:48:37	Northwest Trust	Person John Doe has requested access to the device Main Door. Access allowed. Person used card for requesting access.
08/10/2026 15:47:57	Northwest Trust	Unknown card swipe has been detected on the device Main Door.
08/10/2026 15:47:44	Northwest Trust	Person John Doe has requested access to the device Main Door. Access denied because the person is currently not enabled. Person used card for requesting access.

This screen shows any **Events** that occur while the **Live Events** window is open. A user can also filter the display of events, past or future. Until an applicable event occurs, the Live Events window will display **No Live Events**. As events occur, the system displays event information in real time. You can open Live Events in a separate window by selecting the arrow button next to **Filters**.

2.10.1 How to Read Live Events

The **Live Events** View displays easy-to-read information about any Events that occur while the Live Events window is open.

Time - This column displays the local time (as configured for the Cloud Node) when the Event occurred.

Location - This column displays the Cloud Node where the Event occurred.

Result - This column displays details about an Event that occurred. If a photo was uploaded for that person, it will also be displayed.

2.10.2 Debug Mode

A user with **Integrator**-level **permissions** can switch between viewing **Live Events** and **Debug Mode**.

Selecting **Debug Mode** displays the **Debug Mode** view, which shows the raw Event information and can help troubleshoot issues, such as finding a credential number.

2.10.3 Filter Options

Cloud Nodes - Select a **Cloud Node** to include/exclude the selected **Cloud Node(s)** from being displayed. If no **Cloud Nodes** are selected, the **Live Event** view includes all Cloud Nodes.

← Filters

Filters

Cloud Nodes ^

☐ Kansas City

☐ Omaha

☐ St. Paul

Events v

Display Options

Photo Size

Reset Filters

Cancel

Apply Filters

Events - Select an **Event** to include/exclude the selected **Event(s)** from being displayed. If no **Events** are selected, the Live **Event** view includes all **Events**.

The screenshot shows a 'Filters' dialog box with a back arrow and the title 'Filters'. It contains two main sections: 'Cloud Nodes' with a dropdown arrow, and 'Events' with an expand/collapse arrow. Below the 'Events' section is a search bar labeled 'Search...'. A list of event types follows, each with an unchecked checkbox: AutoOpen Enabled, AutoOpen Disabled, Open (DPS), Close (DPS), Request to Exit Open, Request to Exit Closed, Propped Alarm, Propped Alarm Clear, Forced Alarm, Circuit Breaker On, and Circuit Breaker Off. At the bottom, there are three buttons: 'Reset Filters' (light gray), 'Cancel' (light gray), and 'Apply Filters' (blue).

Photo Size - If you add a photo to a Person, it will display during a Credential scan along with the other Event information. The **Photo Size** slider lets you set the size of the photo displayed for the person associated with an event. After adding the user's photo, adjusting the **Photo Size** slider increases or decreases the size of the user's photo shown in Credential scans.

After selecting any filters that need to be applied to the Live Events view, select **Apply Filters** to return to the Live Events view to begin filtering based on the selected filters.

Event Filters

When viewing Live Events, several Events can be displayed. These differ from the Events displayed and available for use with People/Group Rules and System Event Rules. The Live Events feed displays all Events available, or is filtered to show only certain event types. Any Event in Live Events will display the Door/Device where the Event occurred, if applicable.

Event Filter Options

- **Auto Open Enabled** - An Auto Open schedule began on the indicated Door/Device
- **Auto Open Disabled** - An Auto Open schedule ended on the indicated Door/Device
- **Open (DPS)** - A door position sensor (DPS) on the indicated Door/Device was opened.
- **Close (DPS)** - A door position sensor (DPS) on the indicated Door/Device was closed.
- **Request to Exit Open** - A 'Request to Exit' (REX) input on the indicated Door/Device was activated (opened)
- **Request to Exit Closed** - A 'Request to Exit' (REX) input on the indicated Door/Device was deactivated (closed).
- **Propped Alarm** - The door indicated was held or propped open longer than the configured prop trigger time.
- **Propped Alarm Clear** - The door indicated has been closed, ending the Prop Alarm.
- **Forced Alarm** - The indicated door was opened without an authorized Credential being read or a Request to Exit (REX) input being received.
- **Circuit Breaker On** - A 'Circuit Breaker' event occurred in the indicated Door/Device. This is a flood of event logging (40 events in 30 seconds) occurring on either input A or B (DPS or REX), which disables the input for 30 minutes.
- **Circuit Breaker Off** - A previously detected 'Circuit Breaker' logging event on the indicated Door/Device has ended.
- **Partial Connectivity Detected** - The indicated Controller is not responding, but contact with the WiMac radio is established.
- **Partial Connectivity Cleared** - Communication between the WiMac radio and the indicated Controller is restored.
- **All Prop Clear** - The doors indicated have been closed, ending all active Prop Alarms.
- **No Person Associated with Credentials** - A Credential read at the indicated Door or Device was not recognized or was not assigned to a Person on the Customer Account.
- **Access Denied** - A valid credential assigned to a person in the system was used at the indicated Door/Device, and access was denied because no Access Rule was present or a Deny rule was active.
- **Access Allowed** - A credential with a valid Access Rule was read at the indicated Door or Device, unlocking the Door/Device as configured.
- **Communication Loss** - Communication with the indicated Controller was lost.

2.0 Customer Dashboard

- **Communication Loss Clear** - Communication with the indicated Controller was re-established
 - **Overcurrent Detected** - Higher than intended current draw to attached devices (reader, REX, locking hardware, etc.) occurred on the indicated Controller.
 - **Overcurrent Cleared** - Higher than intended current stopped occurring on the indicated Controller.
 - **Undervoltage Detected** - Insufficient amperage from the power supply was detected on the indicated Controller
 - **Undervoltage Cleared** - An insufficient amperage from the power supply event ended on the indicated Controller
 - **Input Power Connected** - Primary input power was connected to the indicated Controller.
 - **Input Power Disconnected** - Primary input power was disconnected or lost for the indicated Controller.
 - **Low Power Mode On** - The indicated Controller entered 'Low Power' mode, where any attached devices (reader, REX, locking hardware, etc.) will be powered off to maintain battery life.
 - **Low Power Mode Off** - The indicated Controller ceased to be in 'Low Power' mode.
 - **Battery Connected** - An external battery was connected to the indicated Controller.
 - **Battery Disconnected** - An external battery was disconnected from the indicated Controller.
 - **Duress PIN Entered** - A duress PIN was entered at the indicated Door/Device.
 - **Card Scan Error** - An invalid card scan (invalid/unknown format or unreadable) was detected at the indicated Door/Device.
 - **Anti-Passback Violation** - An Anti-Passback violation occurred.
 - **Packetized Protocol Error** - Touch io Reader is not paired correctly, and a credential is scanned
-

2.11 Permissions

Permissions within PDK.io are a core feature that specify which functionalities are available to a user at the **Dealer** or **Customer Account** level. Each **Permission Role** (**Integrator**, **Admin**, **Manager**, or **Reporter**) specifies what PDK.io features are available. The previously created Permissions are searchable.

- A **Permission** granted within the **Customer Account** (from the **Customer Dashboard**) provides those functionalities only for that **Customer Account**.

2.0 Customer Dashboard

Partners with **Integrator** or **Admin** Permissions can add **Permissions** (at their Permission level or lower) to other Partners.

2.11.1 Function Availability by Permission Role

Each **Permission Role** specifies which **Customer Account** functions users can access. Each **Permission**, from **Integrator** to **Reporter**, is more limited in scope compared to the previous **Permission Role**. To find a previously added permission, use the search bar above the Permission list.

Integrator - This **Permission** has full access to all **Customer Account** functions.

Admin - This **Permission** can access and manage all **Customer Account** functions except **Configuration**, and has a limited view of **System Settings**. An **Admin** can also issue **Admin** or lower **Permissions** to others.

Manager - This **Permission** can 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** allows viewing **People**, **Groups**, and **States** in read-only mode. **Reporters** can view **Live Events** and submit **Reports**. **Reporters** can only view this information in their assigned **Partition**.

The following table details which functions each Permission level allows.

	Integrator	Admin	Manager	Reporter
People	✓	✓	✓	Read-Only
Groups	✓	✓	✓	Read-Only
System Events	✓	✓	✓	
Auto Open	✓	✓	✓	
Elevators	✓	✓		
Reports	✓	✓	✓	✓
Partitions	✓	✓		
States	✓	✓	✓	Read-Only

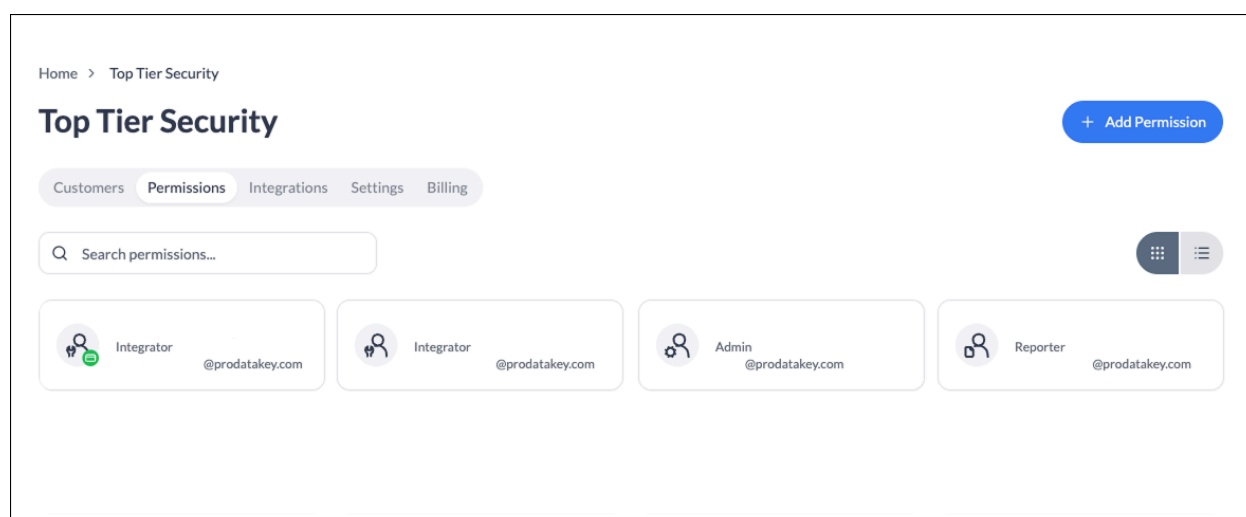
2.0 Customer Dashboard

Live Events	✓	✓		✓
Permissions	✓	✓		
Integrations	✓	✓		
System Settings	✓	Limited View		
Configuration	✓			

Important Note: ProdataKey Technical Support cannot add permissions.

2.11.2 Adding a Permission to a Customer Account

To begin adding a new **Permission** to the Customer Account, select the **+ Add Permission** button in the **Permissions** window. Then you can enter the information for the new **Permission**.



In the **Add Permission** dialogue, enter the email address and the Permission level to be assigned to them.

Add Permission

Add a permission to give users specific access and control within the system. Assign the right level to ensure they can manage tasks based on their role.

Email

Role

Email - Enter the email address of the user for the **Permission**.

Role - Select to view the list of **Permission Roles** and select the appropriate **Permission Role** for the user.

After entering the **User Email** and **Role**, select **Add** to finalize adding the **Permission** to the **Customer Account**. An invitation email will then be sent to the **User Email** with instructions to activate the **Permission**.

Until the user activates the Permission, the user's Permission will be displayed as **(Invitation Pending)**, rather than the user's name.

2.11.3 Editing or Deleting an Existing Permission

For **Permissions** added to a **Customer Account**, selecting the user's name opens a drawer displaying the user's details and allows a Partner with a higher **Permission Role** to delete the **User** or edit the **Permission Role**. The **Name**, **Email**, **Phone Number**, **Company Name**, and **Title** will be displayed but cannot be changed.

2.0 Customer Dashboard

To delete a **Permission**, select the **Delete Permission** button located in the lower left corner of the drawer.

← **Permission**

Permissions provide the authorization needed for users to manage systems within an organization. In this context, permissions are pdk.io users, not credential holders within the access control system.

Name
John Doe

Email
@prodatakey.com

Phone Number

Company Name
PDK

Title
PDK

Role
Integrator

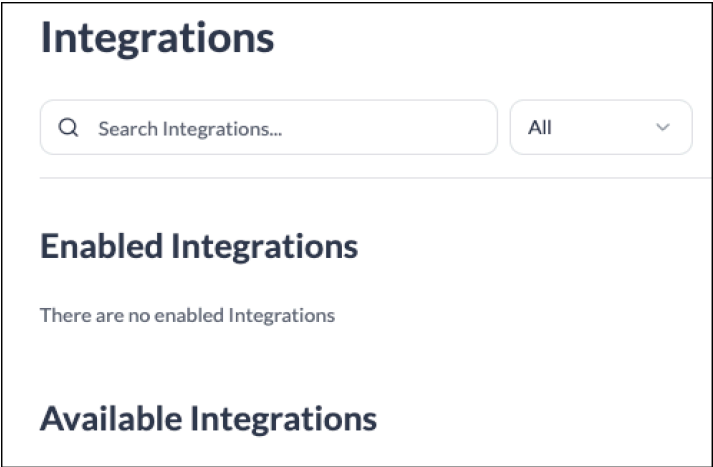
Delete Permission

Cancel

Save Changes

2.12 Integrations

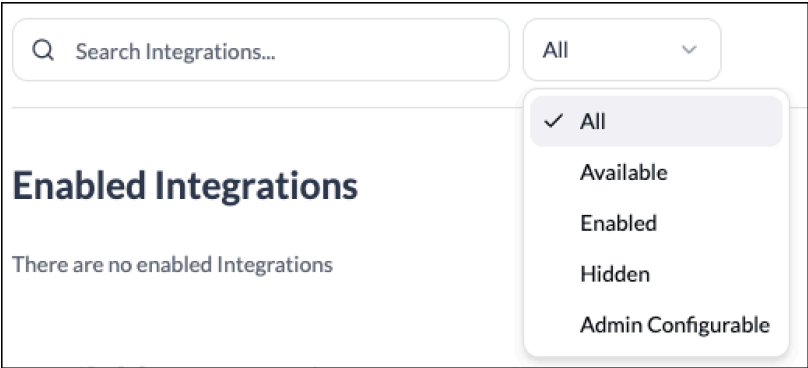
2.12.1 Enabled and Available Integrations



The list of **Enabled and Available Integrations** appears directly under the **Search Integrations** section.

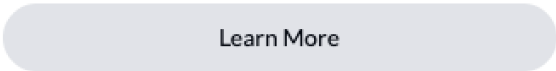
Once an **Integrator enables** an integration, it will be displayed here.

Any **Hidden Integrations** by an Installation Partner appear at the bottom of the list.



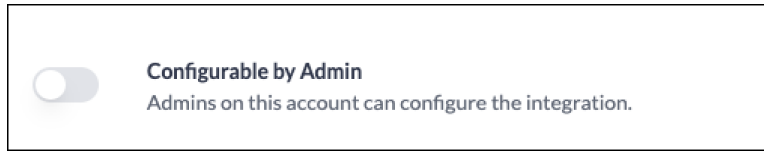
You can filter and search for all Integration types.

2.12.2 Configuration



Select **Learn More** for each **Integration** you want. A drawer will appear with the option to **Enable** the **Integration**. To have your **Admin** configure the **Integration**, select the toggle labeled **Configurable by Admin** (if available).

2.0 Customer Dashboard



NOTE: Not all Integrations are Configurable by Admins.

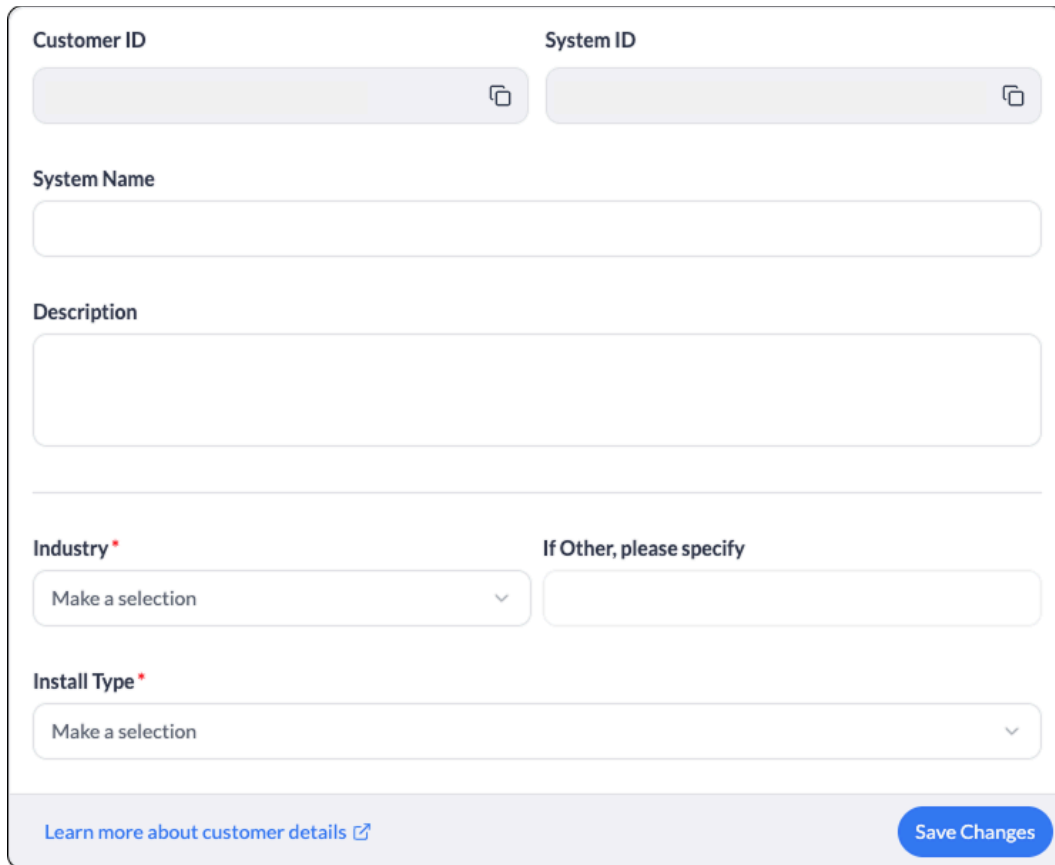


After enabling an Integration, select Manage to edit its configuration.

2.13 System Settings

The **System Settings** window allows a Partner with Integrator access to configure settings for the entire Customer Account. Users with Admin-level permissions have a limited view of System Settings.

2.13.1 Customer Information



The form is titled "Customer Information" and contains several input fields. At the top, there are two fields: "Customer ID" and "System ID", both with copy icons. Below these are "System Name" and "Description" text areas. Further down are two dropdown menus: "Industry" (with a red asterisk) and "Install Type" (with a red asterisk), both showing "Make a selection". To the right of the "Industry" dropdown is a text field labeled "If Other, please specify". At the bottom left is a link "Learn more about customer details" with an external link icon. At the bottom right is a blue "Save Changes" button.

The **Customer Information** section displays the following information:

Customer ID - This shows one of the unique IDs for the **Customer Account**. This is mostly useful for the PDK Support staff.

System ID - This shows one of the unique IDs for the **Customer Account**. This is mostly useful for the PDK Support staff and is used to configure certain **Integrations**.

System Name - This displays the Customer Account name. Only the Dealer Partner with the **Integrator Permission** role in their **Dealer Account** can change this.

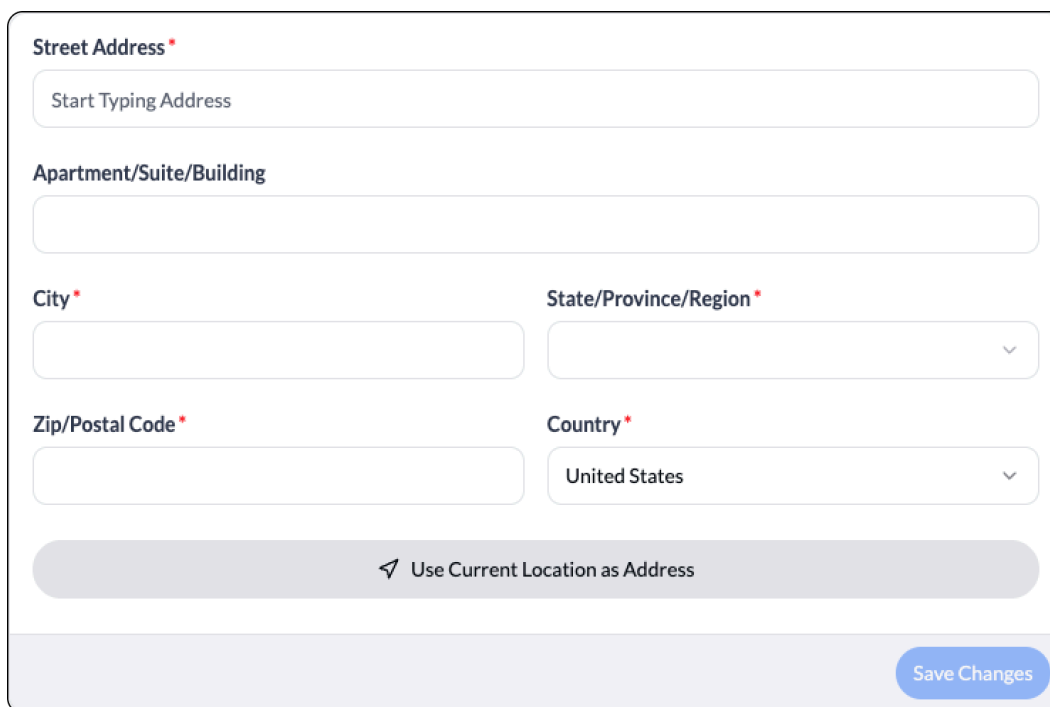
Description - (Optional) Selecting this field allows a Partner to enter a description for the **Customer Account**.

Industry - From the dropdown list, select the **Industry Type** for the Customer Account.

2.0 Customer Dashboard

Install Type - From the dropdown list, select whether the install type is **New Install** or **Replace/Upgrade Existing System to PDK** for the Customer Account.

2.13.2 Location



The form is titled "Location" and contains several input fields and a button. At the top is a "Street Address" field with a red asterisk and a placeholder "Start Typing Address". Below it is an "Apartment/Suite/Building" field. The "City" field has a red asterisk, and the "State/Province/Region" field has a red asterisk and a dropdown arrow. The "Zip/Postal Code" field has a red asterisk, and the "Country" field has a red asterisk and a dropdown arrow showing "United States". At the bottom is a button labeled "Use Current Location as Address" with a location pin icon. A "Save Changes" button is in the bottom right corner.

The use of **Mobile Button digital credentials** can be restricted to a Geofenced boundary. Add your Customer's location address by entering it manually in the **Street Address** field, using your current location, or dragging and dropping a pin.

2.13.3 Adding a Support Contact

Admins can set a direct point of contact for their End Users who need support. By default, the Dealer configures this contact, but you can override it at the Customer level in **System Settings**.

2.0 Customer Dashboard

Name*

Provide at least one contact method. All fields are optional as long as one is filled.

Email



Phone Number



Support Button URL



The URL must begin with "https://" or "http://"

Support Button Label

Character Limit: 0/50

Contact Support Form

Allow users to fill out a form and send messages to Support Contact email?



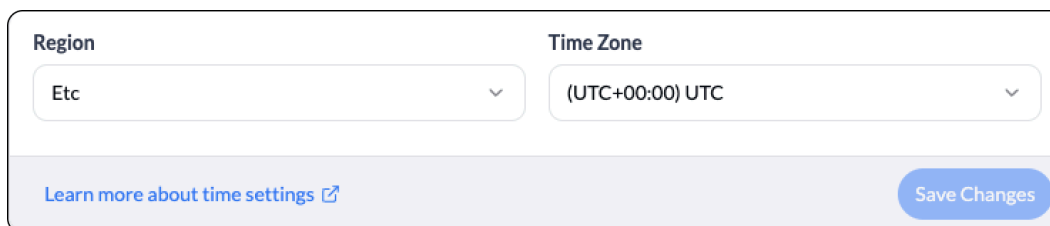
[Learn more about Support Contacts](#) 

Save Changes

This information will be visible to end users in the **PDK Access App**. Please provide at least one contact method:

- **Name** (required)
- **Email Address**
- **Phone Number**
- **Support Button URL**
 - Create a form or survey for users to submit issues, then paste the link here
- **Support Button Label**
 - Customize the label (e.g., "Contact Support")

2.13.4 Time Settings



Region: Etc

Time Zone: (UTC+00:00) UTC

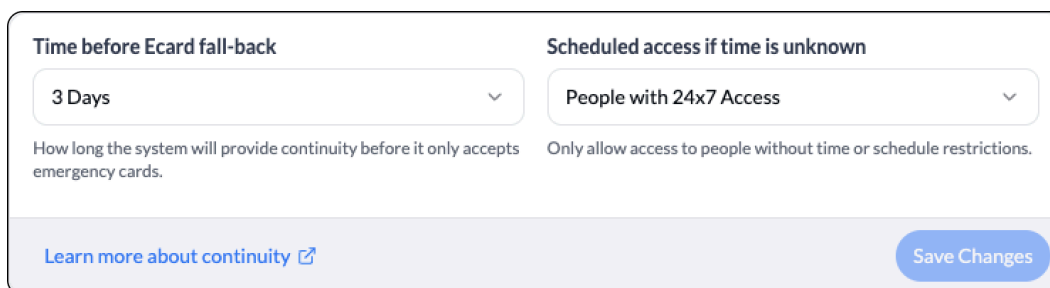
[Learn more about time settings](#)

[Save Changes](#)

Region - Select the **Region** of the World where the Customer Account's default Time Zone is located.

Time Zone - Select the default **Time Zone** for the Customer Account. **Downloaded Reports** will be displayed in this Time Zone. The Time Zone for each Cloud Node is set in Configuration.

2.13.5 Continuity Settings



Time before Ecard fall-back: 3 Days

Scheduled access if time is unknown: People with 24x7 Access

How long the system will provide continuity before it only accepts emergency cards.

Only allow access to people without time or schedule restrictions.

[Learn more about continuity](#)

[Save Changes](#)

Continuity allows a local version of the access database and rules to be retained on Cloud Nodes, Red-series controllers, and Red Wireless Locks. This will allow credentials and schedules to function as expected for a designated period when communication with the Internet or the Cloud Node is lost.

If the Cloud Node loses its connection to the Internet, the local Cloud Node database and attached Controllers and Red Locks will function normally for the **Time before the Ecard fall-back** setting. At that time, the local database will be disabled until the Cloud Node can connect to the Internet and sync again.

If a Red-series Controller is very briefly offline (60 seconds or less), any Events that trigger rules on the Controller will be processed when the Controller reconnects, resulting in a delayed appearance. If the Controller is offline for longer than this, only rules triggering emails will be processed.

2.0 Customer Dashboard

Please note that while a Controller or Red Lock is operating in Continuity mode, the following restrictions will occur:

- Elevator access on the Controller will not function.
- You will be unable to activate doors/devices connected to the Controller or Red Lock from inside the PDK Access app or the States page. Bluetooth and hard credential access are unaffected.
- Any Events that occurred while in Continuity mode will not be available in the Reports dashboard until the Controller or Red Lock reconnects and synchronizes data with the Cloud Node.
- Any emails from Event rules that occur while in Continuity mode will not be processed until reconnection with the Cloud Node is established.

When configuring Continuity, the following settings are available:

Time before Ecard fall-back - This allows you to select the period during which it will operate in Continuity Mode before reverting to using only Ecards.

Schedule access if time is unknown - This setting specifies which People will have access to the connected doors/devices if the Controller or Red Lock cannot validate the current time (for example, if it cannot connect to the internet at all) while operating in Continuity mode. If it can validate the current time, it will operate as expected in Continuity mode.

- **Ecards Only:** The controllers will respond only to Ecards, effectively bypassing Controller Continuity mode.
 - **People with 24x7 Access:** This will only allow people with 24x7 access to the door to use their credentials, while being unable to validate the current time
 - **Ignore Schedules:** All those with access to the door are granted entry regardless of the schedule.
-

2.13.6 Credential Settings

Default Card Formats

Cloud Nodes inherit the default Card Format settings. Add or override Card Formats on each Cloud Node.

 **Standard 26-bit Format**
Do Not Enforce9 - 64 bits

[+ Activate Card Format](#) [Manage Custom Formats](#)

Monthly Credential Resets per User

1

Users can request replacement credentials previously issued. Limit the amount of times this self-help feature can be used.

Enable issuance of Bluetooth credentials
Users that have been issued a Bluetooth credential can unlock doors by presenting their smartphone to a Bluetooth-enabled reader.☒

Enable issuance of Mobile App credentials
Users that have been issued a Mobile App credential can remotely unlock doors via the PDK app.☒

[Learn more about Card Formats](#) [Save Changes](#)

Activate Card Format - Select **Activate Card Format** to select the additional **Card Format(s)** that will be applied to all **Cloud Nodes** in the **Customer Account** by default. This can be changed in the **Card Formats** section of the **Configuration** page.

Manage Custom Formats - Select the **Manage Custom Formats** button to view, add, or edit an existing **Card Format**.

Monthly Credential Resets per User - Selecting this field allows a User to adjust how many times an End-User can request replacement **Digital Credentials** per month before the End-User must contact the site Admin to reset the restrictions on requesting replacement credentials.

Enable issuance of Bluetooth Credentials - Select the toggle switch to enable or disable this feature that allows issuing PDK Access Bluetooth credentials.

Enable issuance of Mobile App Credentials - Select the toggle switch to enable or disable the feature that allows issuing PDK Access Mobile Button credentials.

Activate Card Formats

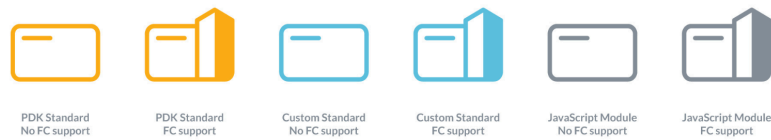
Cloud Nodes can use up to five Card Formats for your physical credentials.

In the Card Formats section of the Configuration page, you can choose from the available Card Formats on the Cloud Node or create a new one.

NOTES:

- Different reader models may send slightly different bit results with the same card.
- Red-series controllers report the bit range correctly, but older controllers (Single IO and Eight IO) may require a larger bit range than Red-series controllers.

CARD FORMAT ICONS



- Yellow Formats are Card Formats created by ProdataKey
- Blue Formats are Card Formats added through the **Formatter defined by the parameters** option described below.
- Grey Formats are Card Formats uploaded through the **Custom Formatter module** option described below.

Selecting an Existing Card Format

Select **+ Active Card Formats**. The **Activate Card Format** drawer will appear, allowing you to create a new Card Format.

Activate Card Format

Card Format

Description

Support Bit Range

Bit range defines packet length for card scans. Using non-overlapping ranges controls card format processing.

Minimum Input Bits

To

Maximum Input Bits

Cancel

Save

After configuring the **Card Format**, select the Save button to add it to the **Cloud Node**.

Edit an Active Card Format

To edit a Card Format, select the Card Format in the list. For the default included Card Formats, you cannot edit the Format. For newly created Card Formats, see the section below on adding a new Card Format.

← 33-bit RS2-HID Format

Num Bits

33

Default Max Input Bits

40

Default Min Input Bits

28

Card Holder ID Bits

27

Card Holder Start Address

4

Num Facility Code Bits

2

Facility Code Start Address

2

Num Bits to Sum for Odd Parity

30

Odd Start Address

2

Num Bits to Sum for Even Parity

30

Even Start Address

1

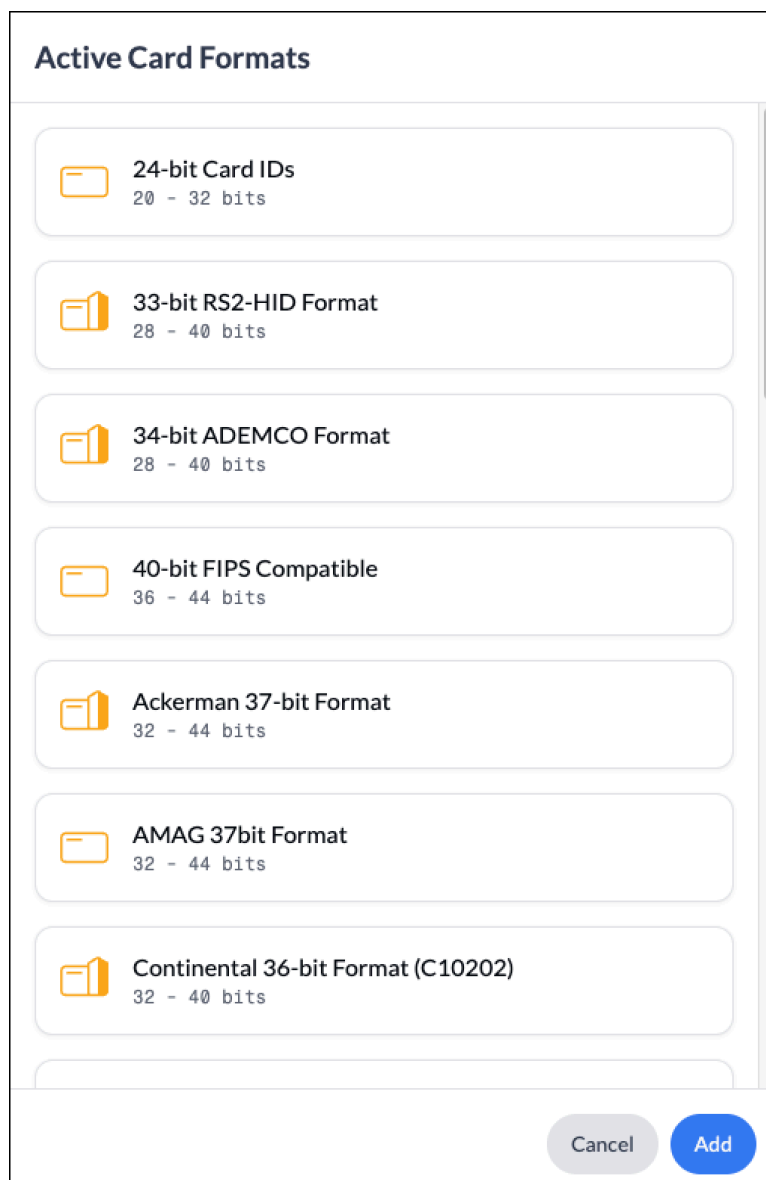
✓ Support Facility Code Processing

✓ Supports Parity

Cancel

Manage Custom Formats

By selecting the Manage Custom Formats button, you are able to add, view format details, or delete User-Defined Card Formats.



Adding a Custom Card Format

Selecting the Add button in the bottom-right corner of the **Active Card Formats** menu opens the **Add Card Format** window.

Add Card Format

Name

Num Bits

Card Holder ID Bits

Card Holder Start Address

Num Facility Code Bits (Optional)

Facility Code Start Address (Optional)

Num Bits to Sum for Even Parity (Optional)

Even Start Address (Optional)

Num Bits to Sum for Odd Parity (Optional)

Odd Start Address (Optional)

Default Min Input Bits

Default Max Input Bits

✖

Support Facility Code Processing

✖

Supports Parity

Upload File

Cancel

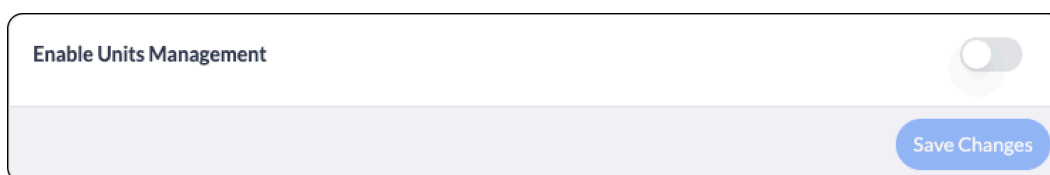
Add

2.0 Customer Dashboard

From this menu, you can either upload a JavaScript module by selecting **Upload File** in the lower-left corner or manually enter the parameters for the Card Format, as explained below.

- **Name** - Enter a unique name for the Card Format
- **Num Bits** - This is the number of bits in the Card Format. Any bit data in the credential scan above this value will be ignored.
- **Cardholder ID Bits** - The number of bits for the card number.
- **Cardholder Start Address** - The bit in the credential scan where the card number begins.
- **Num Facility Code Bits (Optional)** - The number of bits for the Facility Code of the credential.
- **Facility Start Address (Optional)** - The bit in the credential scan where the Facility Code begins.
- **Num Bits to Sum For Even Parity (Optional)** - This is the bit length from the credential scan used to determine even parity.
- **Even Start Address (Optional)** - This is the bit in the credential scan where the even parity bits begin.
- **Num Bits to Start For Odd Parity (Optional)** - This is the bit length from the credential scan used to determine odd parity.
- **Odd Start Address (Optional)** - This is the bit in the credential scan where the odd parity bits begin.
- **Default Min Input Bits** - Enter the minimum bits for the Card Range
- **Default Max Input Bits** - Enter the maximum bits for the Card Range
- **Support Facility Code Processing** - Select if the Facility Code bits are used for this Card Format
- **Supports Parity** - Enforces a secondary check of data from the scanned credential to ensure a misread credential is not processed as valid.

2.13.7 Units Management

A screenshot of a user interface element for 'Units Management'. It features a light gray rectangular box with rounded corners. Inside the box, the text 'Enable Units Management' is displayed in a dark gray font on the left. On the right side of the box, there is a toggle switch that is currently in the 'off' position, indicated by a white circle on a gray track. Below the text and toggle, there is a solid light blue horizontal bar. In the bottom right corner of this bar, there is a blue button with white text that says 'Save Changes'.

Units are designed for Residential Properties, such as apartment complexes. They allow Admins or Managers to efficiently manage resident access without creating manual **Access Rules** for each apartment. Before **Units** can be created, this must be enabled.

2.13.8 Reporting Plan

Reporting Plan

Small Business

✓ Access to event data up to 3 months in the past.

✓ 1 month save time for generated reports.

✓ 100 MB storage for generated reports.

Commercial Essentials

Premium Enterprise

Save Changes

The Reporting feature offers three different pricing plans, each with distinct data retention timeframes, Saved Report storage limits, and Saved Report retention timeframes. An Integrator can change the Reporting Plan.

	Report Retention	Saved Report Storage	Saved Report Retention
Small Business	90 days	100 MB	30 days
Commercial Essentials	1 year	1GB	6 months
Premium Enterprise	5 years	10 GB	2 years

Report Retention - The length of time Report data is saved on the Customer Account.

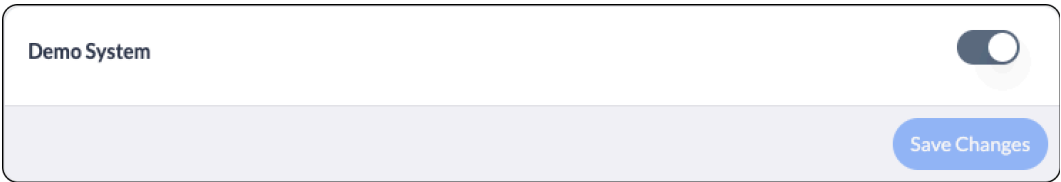
Saved Report Storage - This is the amount of data that Saved Reports can occupy on the Customer Account.

Saved Report Retention - This is the length of time that Saved Reports are retained on the Customer Account.

2.0 Customer Dashboard

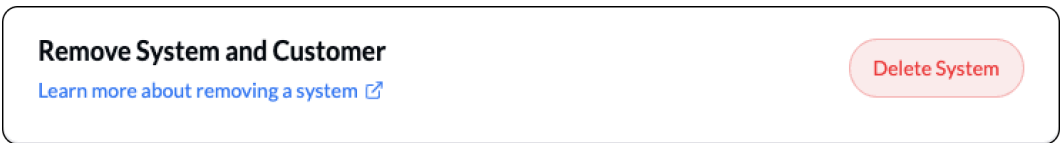
The **Small Business** level is included on all **Customer Accounts** by default. For more information about the different **billing plans**, contact the **ProdataKey** sales staff.

2.13.9 Demo System



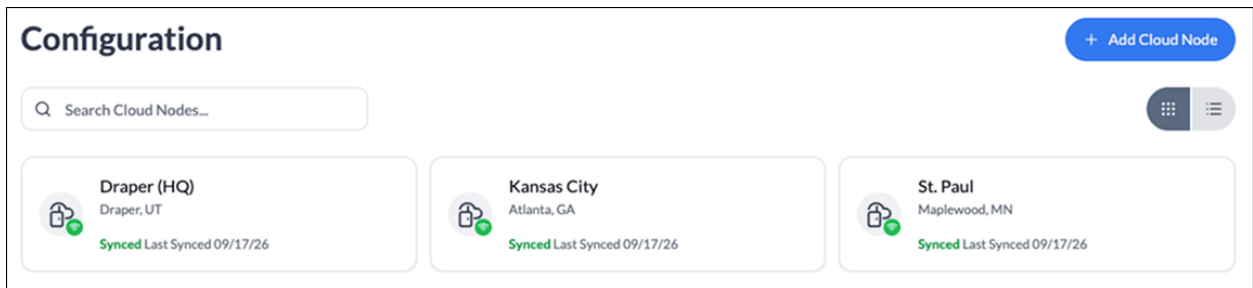
The **Demo System** section (visible only to Dealers with the Integrator Permission role) lets a single **Customer Account** on a **Dealer Account** be configured as a **Customer Account** with a limited number of non-billable **Devices** for the **Installation Partner** to demonstrate the **ProdataKey** software.

2.13.10 System Management



The **System Management** section allows an **Installation Partner** with the **Integrator Permission Role** to permanently delete a **Customer Account** and all associated data from the **Dealer Account**.

2.14 Configuration



2.0 Customer Dashboard

The list of Cloud Nodes on the Customer Account will be displayed here, showing their name, serial number, and last synced date. The list is searchable by name or serial number.

2.14.1 Adding a Cloud Node to the Customer Account

+ Add Cloud Node

Select + Add Cloud Node

Details
Name *

Serial Number

Description

Name - Enter the name for the Cloud Node

Serial Number - Enter the seven-digit serial number (107XXXX) found on the inside door of the Cloud Node enclosure

Description - Enter an optional description

2.0 Customer Dashboard

Location
Street Address *

Apartment/Suite/Building

City * **State/Province/Region ***

Zip/Postal Code * **Country ***
 v

↶ Use Current Location as Address

Street Address - Enter the Street Address for the Customer.

Time Settings
The time zone will be used for all schedules, rules, and event reporting on this Cloud Node.
Region **Time Zone**
v v

Select the **Region** and **Time Zone** for the Cloud Node

NOTE: If the default Time Zone was set in **System Settings**, it will auto-populate here

2.14.2 General Tab

General Devices Connections Discovery Diagnostics

The **General** tab on the Configuration Page allows an Integrator-Partner to view and edit **Cloud Node** settings.

Details

The screenshot shows a configuration form for a Cloud Node. It has two columns at the top: 'Serial Number' and 'Cloud Node ID'. Below these are two input fields, each with a copy icon. The 'Name' field contains 'Northwest Trust'. The 'Description' field is empty, with a character count '0 / 255' at the bottom right. At the bottom of the form, there is a link 'Learn more about Cloud Node details' and a 'Save Changes' button.

Serial Number - This displays the Cloud Serial number entered during registration and cannot be changed.

Cloud Node ID - This displays an alphanumeric string that is unique to the Cloud Node.

Name - This displays the Name entered during Cloud Node registration. It can be changed after registration, but cannot be left blank.

Description - (Optional) Enter Cloud Node-specific notes, such as Site ID or WiMAC Passphrase; these are visible only to Partners with Integrator Permissions.

Location

Street Address *

Start Typing Address

Apartment/Suite/Building

City *

State/Province/Region *

Zip/Postal Code *

Country *

United States

Use Current Location as Address

Save Changes

Street Address - Enter the Street Address for the Cloud Node.

Time Settings

Region

US

Time Zone

(UTC-06:00) Mountain

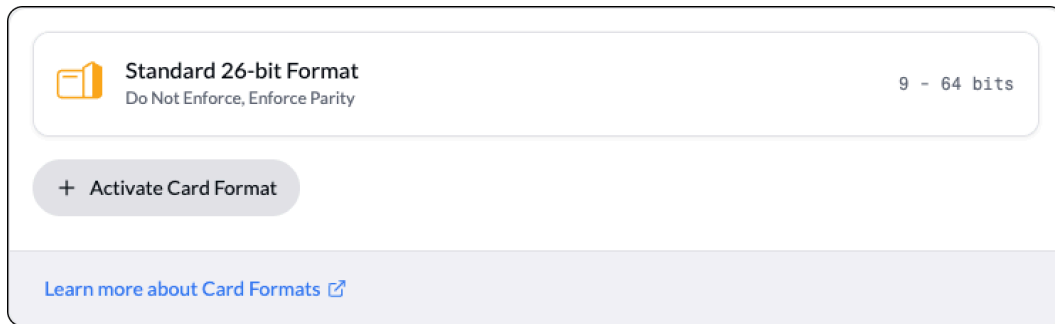
[Learn more about time settings](#)

Save Changes

Region - Select the Region where the Cloud Node is installed.

Time Zone - Select the Time Zone where the Cloud Node is installed.

Card Formats



The **Card Formats** section allows you to view, activate, and deactivate the Card Formats currently selected and available on the Cloud Node.

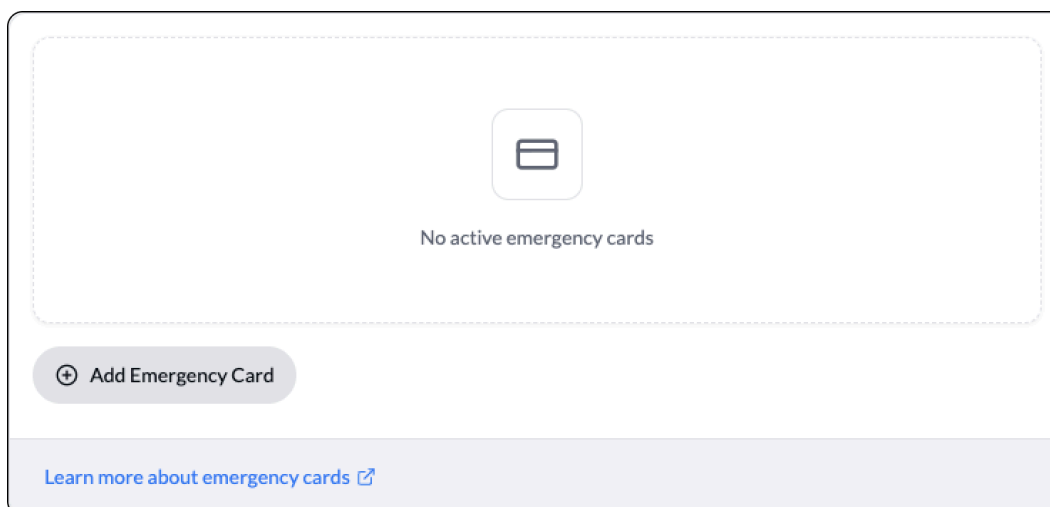
Select the physical Credential encoding formats that will be used on the selected Cloud Node in the Customer Account.

Select + **Activate Card Format** to add another **Card Format**.

Emergency Cards

Emergency Cards, also known as Ecards, are a feature for access control systems that ensure access to devices under certain conditions. **Emergency Cards** can be used to gain access at that door. **Emergency Cards** can be any supported Flexible Card Format (traditional Wiegand or newer high-security credentials) added to the Cloud Node. **Emergency Card** credentials are stored directly on the Controller, with up to ten (10) Ecards entered for each Cloud Node.

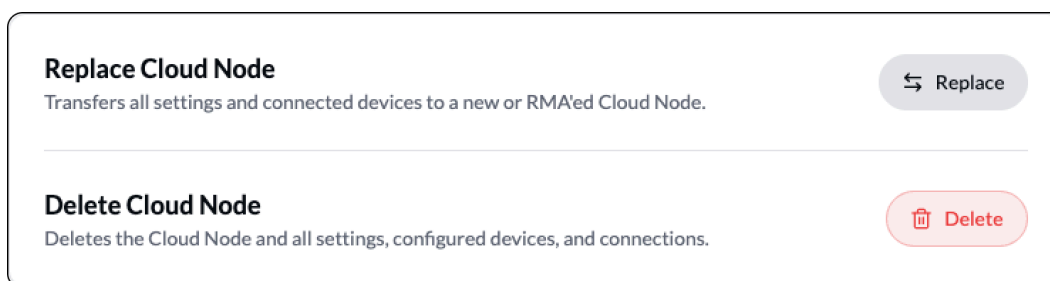
2.0 Customer Dashboard



With Legacy Controllers, **Emergency Cards** activate when communication between the Controller and Cloud Node is lost for longer than four minutes.

With Red-series Controllers, **Emergency Cards** activate when the specified Continuity fall-back time is exceeded.

Advanced



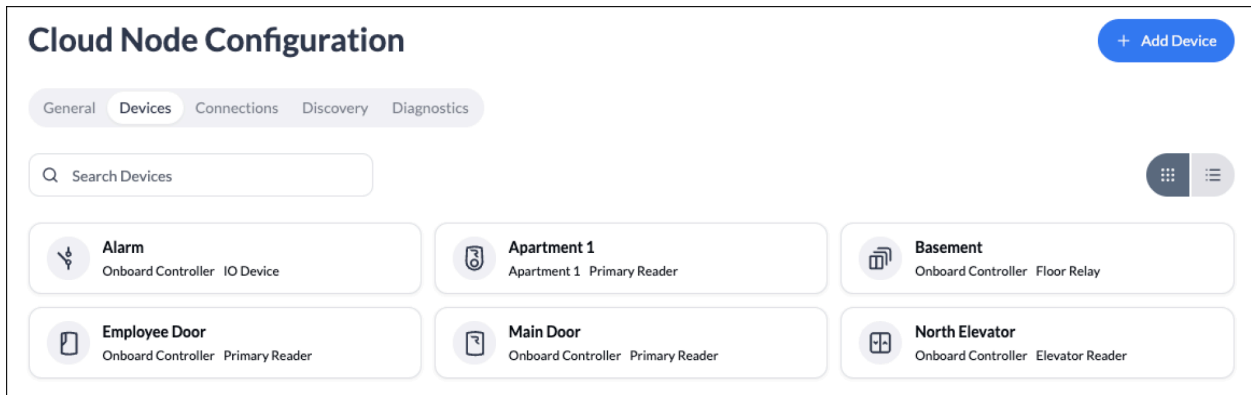
Replace Cloud Node - If a Cloud Node needs to be replaced (for example, due to failure/RMA), select **Replace**, enter the **Serial Number** for the replacement **Cloud Node**, and select **Replace** to remove the old Cloud Node and add the new Cloud Node. The sync process will begin.

Remove Cloud Node - If a Cloud Node needs to be removed entirely from the Customer Account, select **Delete**.

2.14.3 Devices Tab



The Device list is displayed here and can be searched by name. New Devices can be added, or previously configured Devices can be viewed.



Adding a Device



Select + Add Device

Depending on the type of Device being added, select one of the four categories:

Device Category

Door or Gate

Red Wireless Lock

IO Device

Elevator

NOTE: If Red Wireless Lock is not a listed option, please ensure your system has the following:

- Cloud Node Software 2.3.x or higher
- Configured Red Hub

Select Device Type

Depending on the selected **Device Category**, different options will be presented for choosing **Device Types**.

Device Category	Device Type
Door or Gate	Main Door Onboard Controller Primary Reader Employee Door Onboard Controller Additional Reader

2.0 Customer Dashboard

 Red Wireless Lock	 Front Door Front Door Primary Reader
 IO Device	 Alarm Onboard Controller IO Device  Lockdown Onboard Controller Premium IO Device
 Elevator	 North Elevator Onboard Controller Elevator Reader  Top Reader Onboard Controller Additional Elevator Reader  Basement Onboard Controller Floor Relay

Enter Device Details

Next, fill in the provided fields based on the Device Type selected above, then select **Save**. These details can be edited by selecting the Device name.

2.0 Customer Dashboard

Details

Name

Connection

Port

Icon

Wireless Connected Devices

Primary Reader

Name

Floor 1 East Stairs

Connection

Wireless Coordinator

Port

1

Wireless Address

Name - Select to change the Device name.

2.0 Customer Dashboard

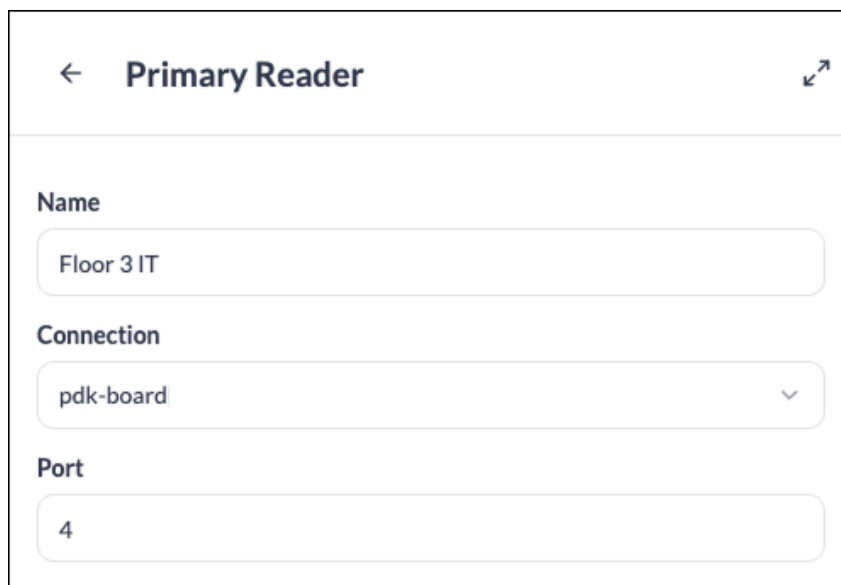
Connection - Select to change the Connection type. To do this, select **Connection**, then choose from the list of configured connection device types.

Port - Select to change the **Port**.

Note: Each controller starts at Port 1.

Wireless Address - Select to change the MAC address for the WiMAC Controller.

Ethernet Connected Devices



The screenshot shows a configuration interface for a 'Primary Reader'. At the top, there is a header bar with a back arrow on the left and a refresh icon on the right. Below the header, there are three labeled input fields: 'Name' with the value 'Floor 3 IT', 'Connection' with a dropdown menu showing 'pdk-board', and 'Port' with the value '4'.

Name - Select to change the Device name.

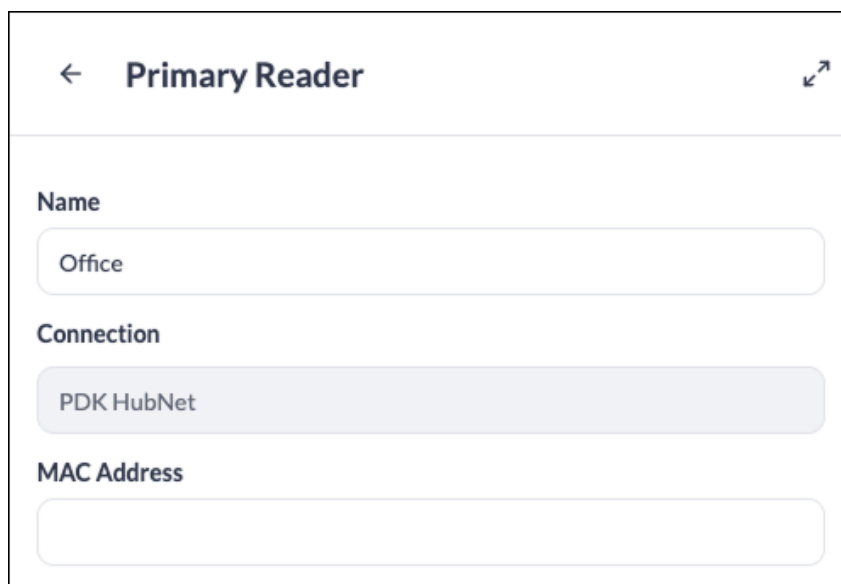
Connection - Select to change the Connection type. To do this, select **Connection**, then choose from the list of configured connection device types.

Port - Select to change the **Port**.

Note: Each controller starts at Port 1.

Red Hub Connected Devices

2.0 Customer Dashboard



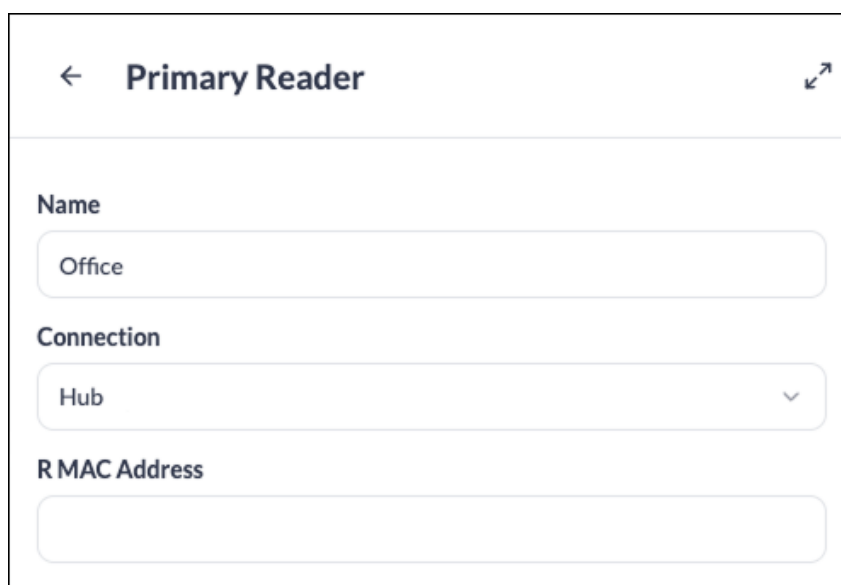
The screenshot shows a mobile application interface for configuring a 'Primary Reader'. At the top, there is a header bar with a back arrow on the left and a refresh icon on the right. Below the header, the title 'Primary Reader' is centered. The main content area contains three sections: 'Name' with a text input field containing 'Office'; 'Connection' with a dropdown menu showing 'PDK HubNet'; and 'MAC Address' with an empty text input field.

Name - Select to change the Device name.

Connection - Displays the selected connection type. This will be **PDK HubNet** and cannot be changed.

MAC Address - Displays the device's **MAC Address** and cannot be changed.

Aperio Connected Doors



The screenshot shows a mobile application interface for configuring a 'Primary Reader'. At the top, there is a header bar with a back arrow on the left and a refresh icon on the right. Below the header, the title 'Primary Reader' is centered. The main content area contains three sections: 'Name' with a text input field containing 'Office'; 'Connection' with a dropdown menu showing 'Hub'; and 'R MAC Address' with an empty text input field.

2.0 Customer Dashboard

Name - Select to change the Device name.

Connection - Select to change the Connection type. To do this, select **Connection**, then choose from the list of configured connection device types.

R MAC Address - Select to change the **R MAC Address** for the Aperio lock hardware.

Details Continued

Appearance - Displays the Public icon of the current device. Select from the available public icons with the dropdown.

Appearance



▼

Reader Type - Readers can be configured to show a different icon depending on the Reader Type configured for the Device. The different Reader Types are outlined below:

Standard - This is the default Reader Type and applies to all readers except Touch io and Red-series readers.	Reader Type Standard▼
Touch io - Choosing this Reader Type enables functions specific to the Touch io readers.	Reader Type Touch io▼ Details Delete Reader 

2.0 Customer Dashboard

Red - Choosing this Reader Type enables functions specific to Red-series readers, detailed below.	Reader Type Red ▾ Reader Serial Number XXXXXXXXXXXXXXXXXXXX 
---	---

Credentials - This section displays only when using Red-series Readers or Red Wireless Locks.

Credentials

☒ **Support Bluetooth Credentials**

☒ **Only Accept Secure Credential Reads**

If this box is checked, older, less secure credential technologies such as 125khz prox will not be accepted by the system.

- **Support Bluetooth Credentials** - To enable the Bluetooth function on a Red-series Reader or Red Wireless Lock.
- **Only accept Secure Credential Reads** - If this box is checked, the system will not accept older, less secure credential technologies such as 125 kHz prox.

NOTE: **Support Bluetooth Credentials** will be enabled by default for Red Wireless Locks and will initiate a Bluetooth Hosting Fee. To avoid this Hosting Fee, uncheck the box before the five-day trial period ends.

Protocol - This lets you select the wiring configuration, either Wiegand or OSDP. If the reader is wired as OSDP and uses multi-drop functionality (connecting multiple Red Readers to a single port), selecting the gear icon lets you set the OSDP Address for the reader.

2.0 Customer Dashboard

Protocol
☒ Wiegand
☒ OSDP
OSDP Address

0

▼



☐ **Require Secure Channel**

OSDP Address - After configuring the OSDP Address for the Red Readers attached to the port, select the Address for the selected reader.

Require Secure Channel - For Red-series Readers only, enabling this option disables Wiegand communications for the reader and accepts communication only through an encrypted OSDP connection.

Authentication Policy - The **Authentication Policy** determines which Credential types are required to gain access.

Primary Authentication Policy
Select one or more credential types. Secondary Policy is available only with Card or Bluetooth.

☐ Card or Bluetooth ⓘ 

☐ PIN 

☐ Mobile Button 

Secondary Authentication Policy
This option is available when Card or Bluetooth is selected as the Primary Authentication Policy. When enabled, the user must enter a PIN after presenting the Primary Credential.

☐ PIN 

2.0 Customer Dashboard

Primary Authentication Options:

You must select at least one **Primary Authentication Policy**:

- **Card or Bluetooth:** Requires a physical card or a Bluetooth credential via the PDK Access App.
- **PIN:** Requires entering a PIN on a reader keypad.
- **Mobile Button:** Requires selecting the Door name in the PDK Access App.

Secondary Authentication Policy (Optional):

The **Secondary Authentication Policy** adds an extra layer of security.

- **PIN:** If the **Primary Authentication Policy** is set to **Card or Bluetooth**, you can require a **PIN** as a second step. The user must scan their credential *and then* enter their PIN.

Important Note: If an **Authentication Policy** is set for the **Device** in **Configuration**, it may conflict with the selected **Authentication Policy** set in the **Access Rule**, causing **Credentials** to function improperly. It is recommended to set this during **Access Rule** creation.

Auto Open After First Allow - When configuring a Device with an Auto Open Schedule rule applied to a Primary Reader or Premium IO device, this option determines the Device's behavior when the Auto Open Schedule begins.

Auto Open After First Allow

If enabled, the device relay will not activate until an 'Allowed' credential input occurs during an Auto-Open Schedule.



Below is an explanation of how this control works in both states.

- **Disabled** - When the Auto Open Schedule begins, the Device relay will activate automatically.
- **Enabled** - When the Auto Open Schedule begins, the Device relay will not activate until an **Allowed** credential input occurs during the Auto Open Schedule.

Auto Lock - Red Wireless Locks only

2.0 Customer Dashboard

Auto Lock

If enabled, the device relay will automatically deactivate after the dwell period specified below.



Auto Locking is enabled by default for Red Wireless Locks. If this is enabled, the Wireless Lock will relock after an open command is sent (with a valid credential or through software) and its specified Dwell Time has elapsed. By default, this setting is set to 30 seconds. The **Dwell** can be adjusted at any time.

Open/Close Delay - The amount of time that the door or device is delayed in opening after a valid credential scan.

Open/Close Delay

Seconds

Open/Close Dwell - The amount of time the Door/Device stays unlocked after a valid credential scan. Set a time duration value that determines how long a device remains unlocked after a valid read.

Open/Close Dwell

Seconds

Relay - Activating or Deactivating a Device will open or close that Device.

Relay

2.0 Customer Dashboard

- **Activate** - Will send an activation command to the selected Door/Device. For a door or gate device, this will unlock the Device. For a Premium IO Device, this will trigger the expected output. The relay will remain activated until a *Deactivate* command is sent.
- **Deactivate** - Will send a deactivate command to the selected Device/relay. For a door or gate device, this will lock the Device. For a Premium IO Device, this will stop the expected output. The relay remains closed until *Activate* is selected again or a rule under a Person or Group affects the Device.

Inputs - A (DPS) and B (REX) inputs can be enabled or disabled for the Device.

Inputs

Door Position Sensor (DPS) - Input A
Reports a ground received on the "A" terminal as a DPS event. This is required for any System/Group Event using the "On Open" or "On Close" triggers.

☒

Motion Request to Exit (REX) - Input B
Reports a ground received on the "B" terminal as a REX event. This is required for any System/Group Event using the "On REX Open" or "On REX Close" triggers.

☒

Door Position Sensor (DPS) - Input A - A **Door Position Sensor** records the door position (open or closed) at all times. Selecting enables or disables the DPS input on the Device and enables or disables the Prop Alarm option.

Motion Request to Exit (REX) - Input B - A Request to Exit (REX) device allows a System Event to be configured every time the **REX** input is triggered. Selecting this enables or disables the REX input on the Device. Both **REX** and **DPS** must be selected in order to enable the **Forced Alarm** option. This feature is enabled by default after creating a new device.

Alarms - Prop Alarm or Forced Alarm can be configured for the Device.

Alarms
☒ **Prop Alarm**
Use of this feature requires a DPS input to be added.
Prop Delay

Seconds
☒ **Forced Alarm**
Use of this feature requires DPS and REX inputs to be added.

Prop Alarm - The **Prop Alarm** option allows an alarm to be added for System Events and Reports when a door is propped open for the duration entered in the **Prop Delay**. When **Prop Alarm** is enabled, the **Prop Delay** option is available.

Prop Delay - This option is displayed only when Prop Alarm is enabled. **Prop Delay** is the amount of time, in seconds, after a door is propped open before the system triggers a Door Propped Event, allowing time for the door to close.

Forced Alarm - This option logs any time a door opens without a valid card scan or when the REX is tripped, indicating the door was forced open. An alarm can be set for a forced door when **Forced Alarm** is checked. **Forced Alarm** is available only when both **DPS** and **REX** are checked.

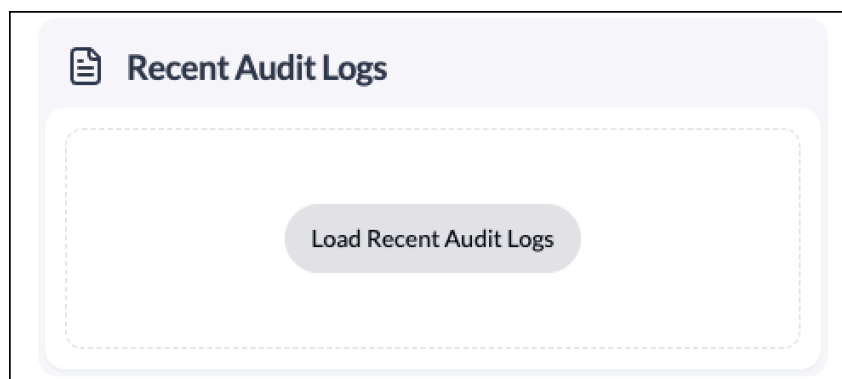
Partition - Existing **Partitions** are listed and can be added to a device. Previously created partitions are listed in alphanumeric order. Select a **Partition** name to view that partition's information and edit it if needed.

Partitions

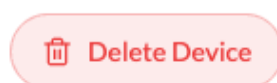
Default

Default

Recent Audit Log - This allows you to view the fifty (50) most recent events and changes for the Device.



Delete Device - To remove a Device, select **Delete Device**.



Save - After making the necessary selections on this screen, select **Save**.

Move to Another Type - Change the Device Type by selecting this icon.



2.14.4 Connections Tab



The Connections tab on the Configuration page lets an Integrator-Partner view, add, edit, and remove Connections to Controllers for the Cloud Node.

2.0 Customer Dashboard

Cloud Node Configuration

+ Add Connection

GeneralDevicesConnectionsDiscoveryDiagnostics

Onboard Controller
Onboard

Red 4 Door Controller (R4)
Ethernet

Wireless Coordinator
Coordinator

Adding a Coordinator Connection

The **Coordinator** allows communication with the onboard WiMAC hardware in most non-Server Cloud Nodes. Normally, you won't need to add this Connection to a Cloud Node unless the Connection was deleted.

← Add Connection

Name

Connection Type

Coordinator

Port

/dev/ttySC

Cancel

Save

Name - Enter a name for the connection here. This is typically named **Wireless Coordinator**.

Port - This will always be 0.

After adding the Coordinator Connection, select **Save**.

Adding an Ethernet Connection

An Ethernet connection is a Controller that uses a CAT5/CAT6 network cable to connect to a Cloud Node on the same local network.

For Red High-Security controllers, it is recommended to discover the Controllers using the **Discovery** tab. If the Controller is not discoverable, you can manually add the connection for Red-series controllers if you have obtained the Controller's IP address. However, this is not recommended, as the Cloud Node may not detect the Controller as a Red-series Controller, limiting Red-series Controller functionality.

With Legacy Controllers (Single IO, Eight IO, Gate IO, and Pedestal IO units), the Lantronix module is initially set up to use DHCP to automatically obtain an IP address. Assign a static IP address using the Lantronix network utility software by configuring a DHCP reservation (contact the Network Administrator for information on this), or through the module's web interface (access it by entering the module's IP address into a web browser).

 **Add Connection**

Name

Connection Type

Ethernet 

Manufacturer

 PDK ☒

 Lantronix ☐

IP Address

IPv4

Port

10001

Cancel

Save

First, select whether the Controller is a **PDK** (Red-series) **Controller** with an integrated PDK module or a **Legacy Controller** with a Lantronix module.

Name - Enter a name for the connection here. This can be anything you like, from an internal code to a descriptive name for the controller, for example, naming the Controller for the door(s) attached or the installation location of the **Controller**.

IP Address - Enter the IP Address for the Ethernet controller.

2.0 Customer Dashboard

Port - Use the default Port 10001 unless PDK Technical Support or IT personnel at the installation site specifies otherwise.

Notes regarding Lantronix Modules:

When configuring an Ethernet connection for Legacy hardware, you **must** select **Lantronix**. Selecting **PDK** for the module will cause issues with the module's functionality.

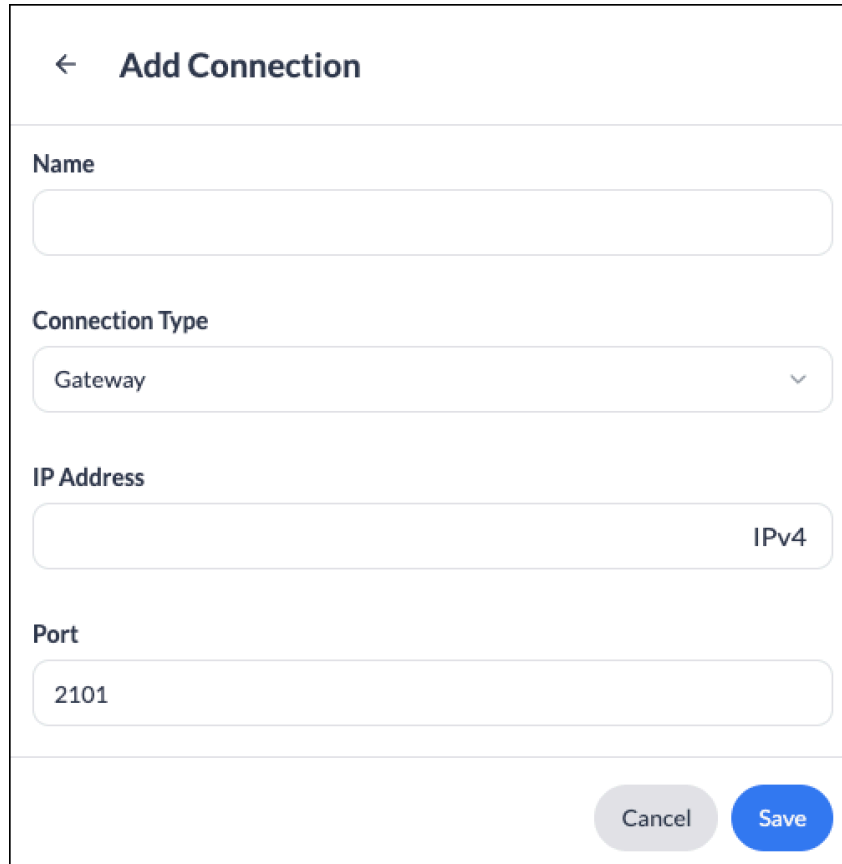
Download the Lantronix Device Installer (either the web-based or stand-alone version) from the Lantronix website to install and use this application.

When adding an Ethernet door controller, ensure that you are connected to the same network as the Legacy Controller and that the correct Network is selected in the Lantronix Device Installer. If the correct Network is not listed in the Lantronix Device Installer, turn off the WiFi on the computer.

After adding the Ethernet Connection, select **Save**.

Adding a Gateway Connection

A **Gateway Connection**, also known as a Wireless Gateway Connection, is a Legacy connection used to provide the WiMAC signal to a Cloud Node without wireless connectivity, such as a server Cloud Node or an Ethernet-only version of Red Cloud Node. Unlike using additional Cloud Nodes in a multi-site Customer Account, a Gateway Connection must be on the same local area network as the Cloud Node.



← Add Connection

Name

Connection Type

Gateway

IP Address

IPv4

Port

2101

Cancel Save

Name - Enter a name for the **Gateway Connection**. This can be anything you like, from an internal code to a descriptive name for the Gateway (for example, the controller's location).

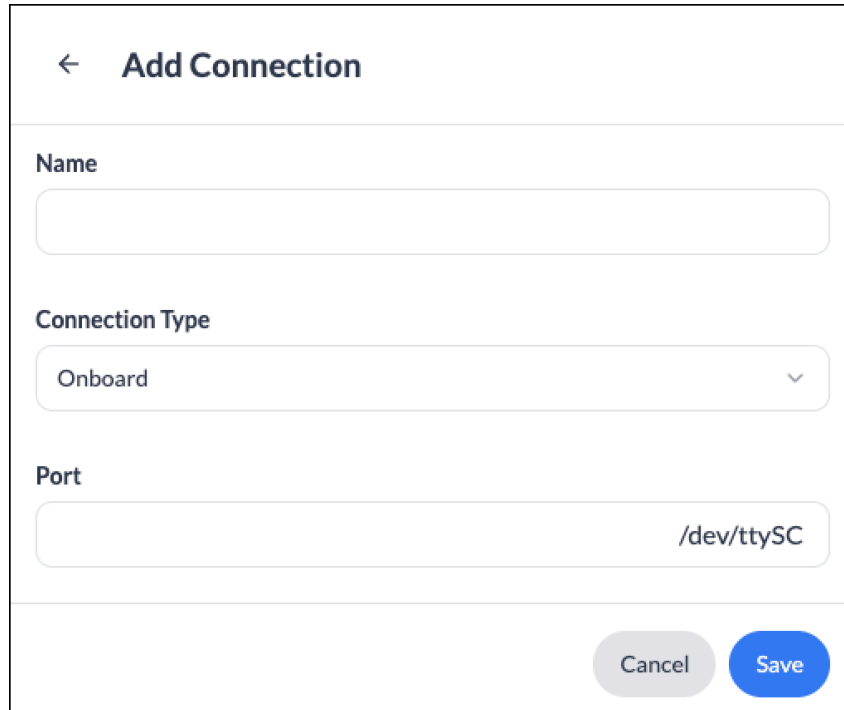
Port - This is normally 2101 unless you change it in the Gateway web interface.

IP Address - Enter the Gateway's IP address. Set this to **Static** in the Gateway web interface.

After adding the Gateway Connection, select **Save**.

Adding an Onboard Connection

An **Onboard Connection** only applies to the built-in **Controller** in non-Server Cloud Nodes, both Legacy and Red series hardware. Normally, you won't need to add this Connection to a Cloud Node unless the Connection was deleted.



← Add Connection

Name

Connection Type

Onboard

Port

/dev/ttySC

Cancel Save

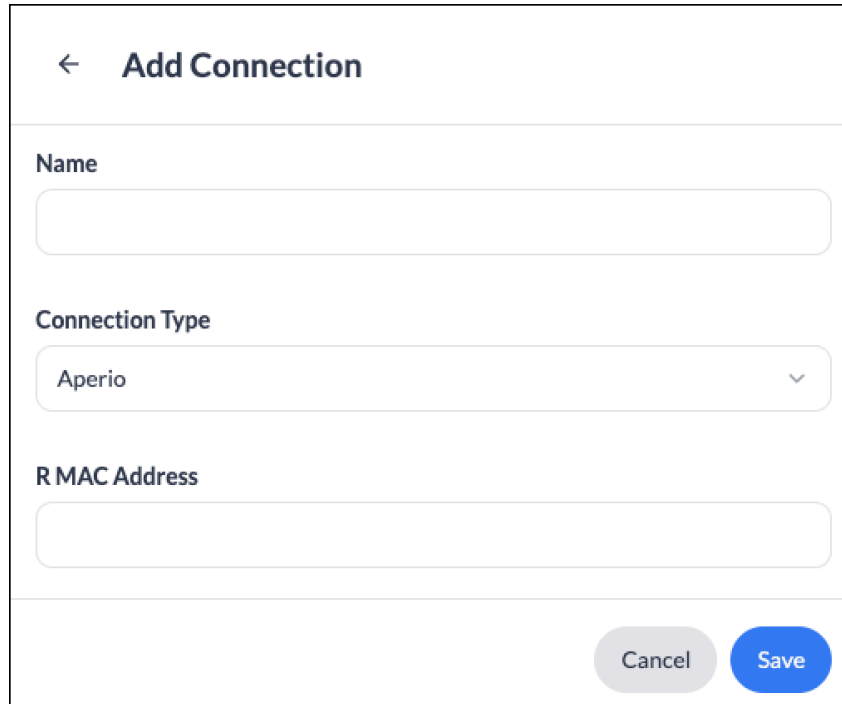
Name - Enter a name for the Onboard Connection here. This can be anything you like, from an internal code to a descriptive name for the controller; for example, naming the Controller for the attached door or the installation location of the **Controller**.

Port - This will always be 1.

After adding the Onboard Connection, select **Save**.

Adding an Aperio Hub Connection

This connection allows communication with Aperio hubs and the Cloud Node.



← Add Connection

Name

Connection Type

Aperio

R MAC Address

Cancel Save

Name - Enter a name for the connection here. This can be anything you like, from an internal code to a descriptive name for the controller, such as the door(s) attached to the Aperio hub or the location where the Aperio hub is located.

R MAC Address - Enter the MAC address for the new **Aperio** hub.

After adding the Aperio Connection, select **Save**.

Adding a Red Hub Connection

A Red Hub is a Connection that adds the **HubNet** (BLE Network) to your system, allowing you to connect Red Wireless Locks to the Cloud Node.

← Add Connection

Name

Connection Type

Red Hub

▼

IP Address

IPv6

MAC Address

Port

10001

Antenna

Internal

▼

Cancel

Save

Name - Enter a name for the connection here. This can be anything you like, from an internal code to a descriptive name for the connection, such as the Hub's location.

IP Address - Enter the Hub's IPv4 or IPv6 address.

MAC Address - Enter the Hub's MAC Address.

Port - Use the default Port 10001 unless PDK Technical Support specifies otherwise.

Antenna - Select External Antenna if installed; otherwise, select Internal Antenna.

After adding the Red Hub Connection, select **Save**.

Editing or Deleting a Connection

←

Connections

Name

Onboard Controller

Connection Type

Onboard

Port

1

/dev/ttySC1

Delete Connection

Cancel

Save Changes

Selecting a previously added Connection name displays the Connection details, allowing the Connection to be edited. All settings available during initial setup, except Connection Type, are available when editing the Connection. The Connection can also be deleted from the drawer.

Ethernet Connection Options

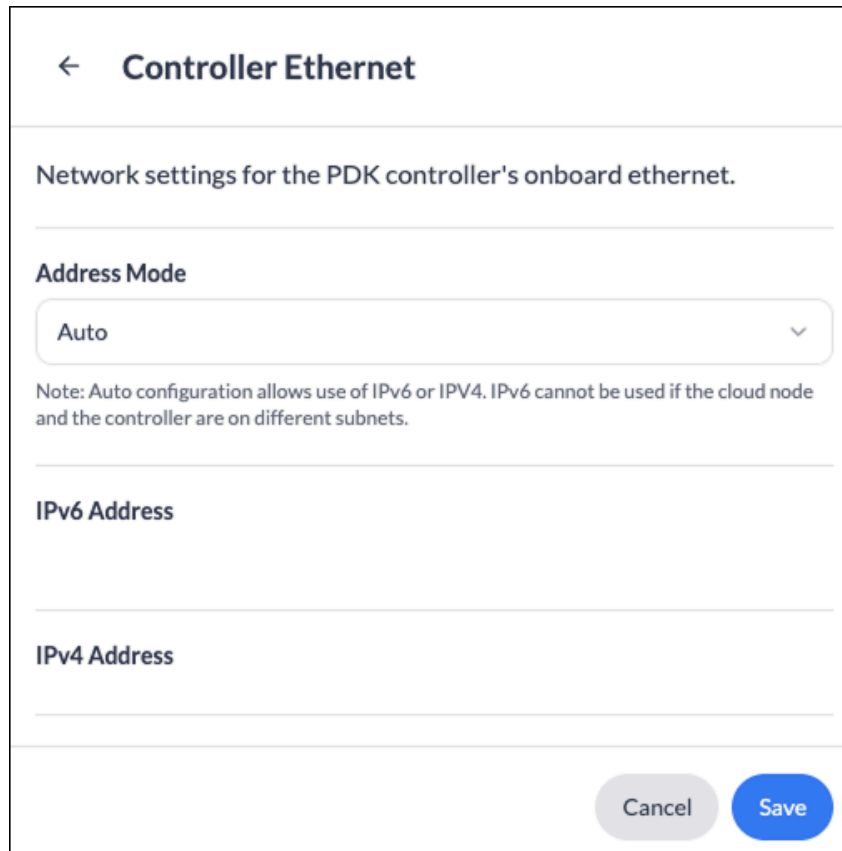
When editing a Red High-security Ethernet connection through the **Connections** tab, the options displayed differ from those shown on Discovery. Use the default IPv6 option to reduce the chance of an IP conflict.

Controller Ethernet

Connection Unlocked

Controller Ethernet

You can adjust the Ethernet Module settings on the Red High-Security device.



The screenshot shows a mobile application interface for configuring the Controller Ethernet settings. At the top, there is a back arrow and the title "Controller Ethernet". Below this, a subtitle reads "Network settings for the PDK controller's onboard ethernet." The main section is titled "Address Mode" and features a dropdown menu currently set to "Auto". A note below the dropdown states: "Note: Auto configuration allows use of IPv6 or IPV4. IPv6 cannot be used if the cloud node and the controller are on different subnets." Below the note, there are two input fields labeled "IPv6 Address" and "IPv4 Address". At the bottom right, there are two buttons: "Cancel" (grey) and "Save" (blue).

Address Mode: This allows the Red High-Security device to use IPv6 or IPv4. Please note that IPv6 cannot be used if the Cloud Node and Red High-Security devices are on different subnets/networks.

Auto - This will show the current IPv6 and IPv4 addresses.

IPv4 Static - This allows you to configure the IPv4 address as a static IP.

← **Controller Ethernet**

Network settings for the PDK controller's onboard ethernet.

Address Mode

IPv4 Static

Note: This address should be provided by your network administrator.

IPv4 Address

Network Mask

Gateway

DNS

Cancel

Save

Connection Locking

This feature allows an Integrator-Partner to **lock** the Connection for the selected Red-series Controller. This removes the ability to physically change the hardware for the current connection on the Cloud Node and use it elsewhere without first **unlocking** the Controller. This will also keep a different Cloud Node on the same network from discovering and adding the Red Controller to the other system.

2.14.5 Discovery Tab

General Devices Connections **Discovery** Diagnostics

The Discovery Tab of the Configuration Page allows an Integrator-Partner to discover Controllers, Hubs, Wireless Locks, and add Devices to a Cloud Node.

Cloud Node Configuration

General Devices Connections **Discovery** Diagnostics



The Cloud Node is now discovering controllers...
Controllers will be listed here once they are discovered.

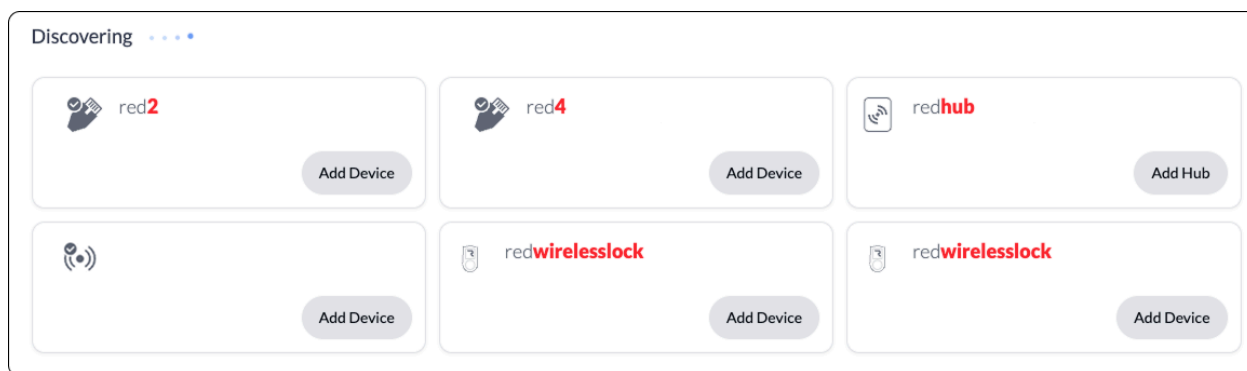
Red-series Controllers using Wireless (WiMAC) or Ethernet communications, Red Hubs, Red Wireless Locks, and Legacy PDK Controllers using Wireless communication use the Discovery process to add any associated Devices to that Cloud Node.

The Cloud Node will automatically begin detecting. Both newly detected Controllers and Controllers with previously configured Devices will be displayed, with the names of the configured Devices listed below their MAC addresses/IP addresses. Red Wireless Locks and Hubs will not be discoverable once added to the system.

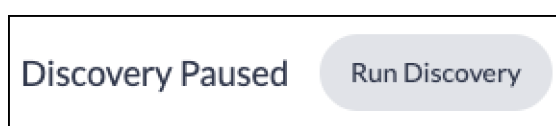
NOTE: At least one Red Hub must be added to the Cloud Node before a Wireless Lock can be discovered.

After discovering available Controllers or Wireless Locks, select **Add Device** or **Add Hub**, then follow the steps above to add Devices.

2.0 Customer Dashboard



Important Note: The contents will refresh to a blank state each time you navigate to the Discovery tab.

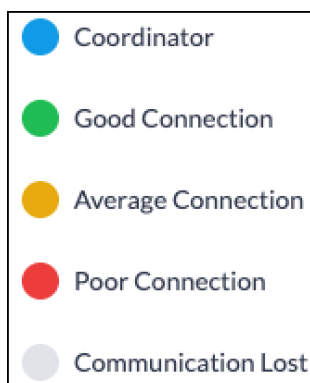


Discovery will **pause** after a period of inactivity. Selecting **Run Discovery** will refresh the available Controllers, Hubs, and Locks.

2.14.6 Diagnostics Tab

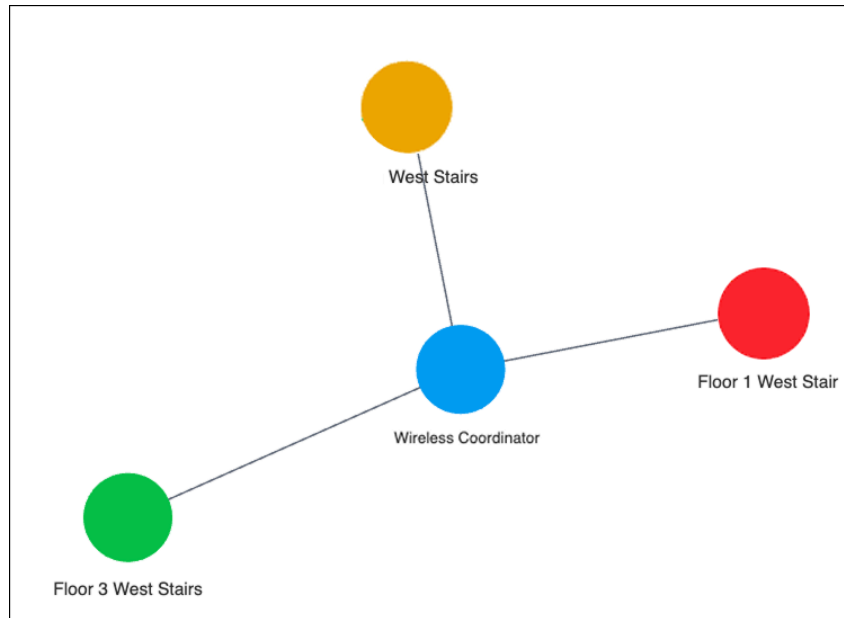


The Diagnostics tab displays a visual representation of the Cloud Node(s) and controller device(s) attached to the system, by connection type.



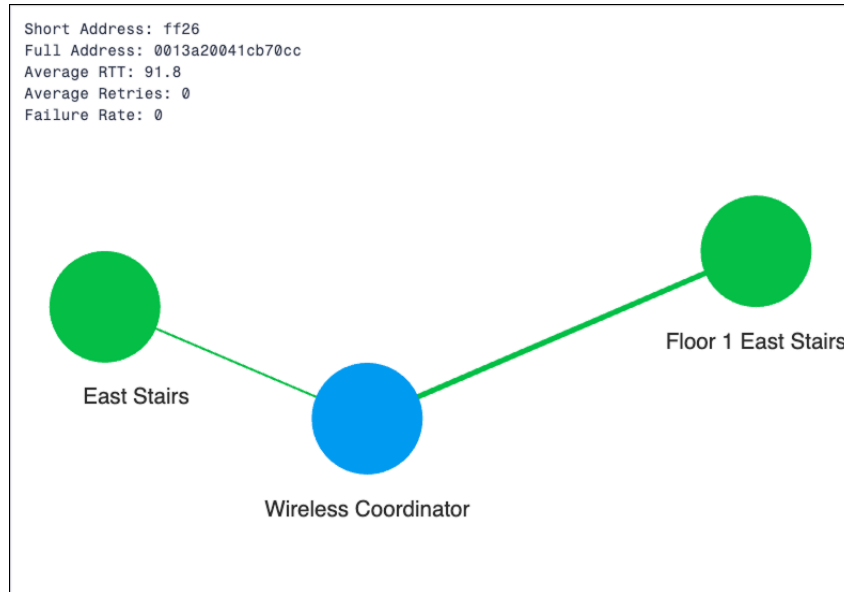
Diagnostics Overview

The image below displays a Cloud Node WiMAC connection, listed as Wireless Coordinator, and the connected WiMAC Controllers. The color codes for each Controller show the relative signal strength when communicating with either the Cloud Node or the next Controller in the mesh network toward the Cloud Node.



Hovering the cursor over a Controller will display the Controller's connection information.

2.0 Customer Dashboard



Short Address - Similar to a local IP Address; used if needed to define a Personal Area Network, dividing devices into different networks.

Full Address - The MAC address of the WiMAC module on the Controller.

Average RTT - Average RTT, or Round-Trip Time, is the time in milliseconds for a communication request to be sent from a selected WiMAC device to the Cloud Node/Gateway or next WiMAC device on the path to the Coordinator and then back to the selected Controller.

If the Controller is more than one jump from the Cloud Node on the mesh network, add the Average RTT for each jump to the Cloud Node to determine the combined communication delay.

Average Retries - The number of retries required to establish communication from the Controller to the Cloud Node, or to the next Controller in the mesh network connection to the Cloud Node.

Failure Rate - The percentage of failed communication attempts for the selected Controller recently. 0 indicates no failure; 1 is 100% failure.

For optimal communication, the following recommendations can help to troubleshoot WiMAC communication issues.

- **Average RTT** - The lower this value is, the better. For example, a combined value over 1000 equals a 1-second communication delay.
- **Average Retries** - The lower this value is, the better.
- **Failure Rate** - Any value above 0 indicates that significant communication interference will need to be identified and resolved.

2.0 Customer Dashboard

The connecting lines between the Cloud Node and Controllers, or between different Controllers on the mesh network, show the Controllers' communication paths. Hovering the mouse cursor over these connection lines displays a general representation of the wireless signal strength. This value will range from 0 to 255, with 255 being the best and strongest possible signal.

Links Test

A blue rounded rectangular button with the text "Start Links Test" in white.

To understand how the **Links Test** function in the Diagnostics tab works, you need to understand how the WiMAC mesh network works. After the WiMAC connections between the Cloud Node and Controllers are established, the Cloud Node periodically sends two commands to the connected Controllers: a ping command and a command to optimize the mesh network connections. Every few minutes, the Cloud Node sends the ping command to confirm the Controller is still online. After every other ping command, the Cloud Node sends the command to optimize the mesh network. This command makes every controller determine the optimal connection path back to the Cloud Node. The WiMAC module firmware determines this optimization and balances WiMAC signal strength, ping times, and the number of devices between the WiMAC device and the Cloud Node.

Selecting **Start Links Test** will begin sending the mesh optimization command every second. This can cause the connection lines between devices to change, and on Cloud Node systems with moderate to large numbers of WiMAC devices, this can cause device communication issues if allowed to run for more than a brief time.

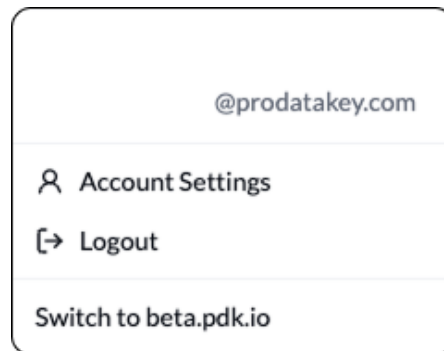
Selecting **Stop Links Test** will end the device connection test.

3.0 Settings

View **Account Settings** by selecting the person icon in the top-right corner of the dashboard. Use the search bar to find People, Groups, Floor Groups, and Cloud Nodes in the System. Display settings can also be adjusted, and selecting the question mark icon opens the knowledge base widget.



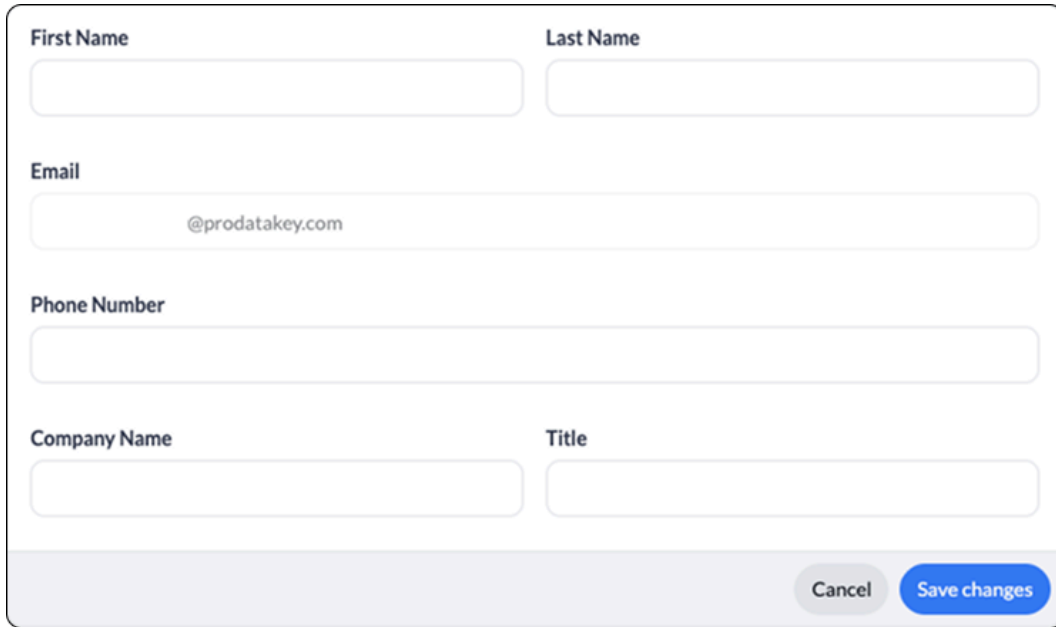
The user can also **log out** or navigate to **beta.PDK.io**.



3.0 Settings

3.1 Account Settings

3.1.1 Personal Information



A form for updating personal information. It contains five input fields: First Name, Last Name, Email, Phone Number, and Company Name. The Email field is pre-filled with '@prodatakey.com'. There is also a Title field. At the bottom right, there are two buttons: 'Cancel' and 'Save changes'.

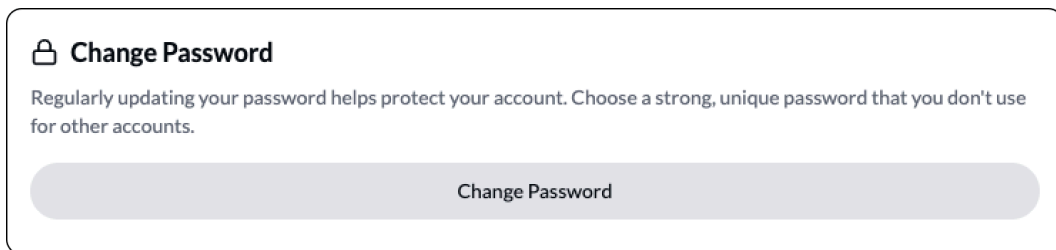
First Name	Last Name
Email	
@prodatakey.com	
Phone Number	
Company Name	Title

Cancel Save changes

After the invite is sent, the user will fill out this information, but all fields except Email are editable here.

3.1.2 Account Security

Change Password



A form for changing a password. It has a title 'Change Password' with a lock icon. Below the title is a message: 'Regularly updating your password helps protect your account. Choose a strong, unique password that you don't use for other accounts.' At the bottom is a button labeled 'Change Password'.

 **Change Password**

Regularly updating your password helps protect your account. Choose a strong, unique password that you don't use for other accounts.

Change Password

Old Password - Enter the current password.

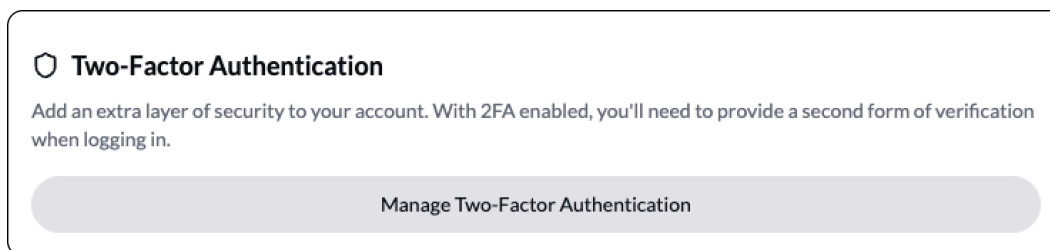
New Password - Enter a new password.

Confirm New Password - Re-enter the new password for confirmation.

3.0 Settings

After entering the above information, select **Change** to save the new Password or select **Cancel** to discard any changes and return to the main Dashboard.

Two-Factor Authentication



Three Multi-Factor Authentication options are displayed. A User with Integrator-level permission must verify themselves in addition to their password, but users with all other permission levels can opt in if desired.

NOTE: With the PDK.io email invite, the Integrator must use an authenticator app to scan the QR code, or enter the provided key. Not just any QR code reading app will work. A generic QR code reader app won't provide the needed code.

3.1.3 Policies

Privacy Policy and Software as a Service Agreement



This displays whether the User confirmed their acceptance of the **Privacy Policy** and **Software as a Service Agreement** displayed when the User initially set up the account.

By selecting **View Policy**, the User can review the agreements.