

iglooworks Dashboard User Guide for Owner/Admin

Welcome to iglooworks	5
Before you begin	5
Data Architecture and Workflow	6
Organisation data structure	6
Department data structure	7
Lock Access workflow	8
Login	9
2FA login	9
Owner and admin controls	10
1. Overview	11
2. Departments**	11
2A. Add department	12
2B. Edit department	13
2C. Delete department	15
3. Properties	16
3A. Add properties	16
3B. Edit Property	17
3C. Delete property	18
3D. Edit lock name	19
3E. Edit lock Activity log/ Heartbeat Intervals (INB1 Only)	20

3F. Add access	22
- Add Remote PIN Access	22
- Add Custom PIN Access	24
- Add Single Bluetooth Access	26
- Add 2FA Access	27
- Add Multiple Bluetooth Access	28
3G. Edit access	29
- Edit Remote PIN access	29
- Edit Custom PIN access	29
- Edit Bluetooth access	29
- Edit 2FA access	30
3H. Delete access	31
- Delete Remote or Custom PIN access	31
- Delete Bluetooth access	32
- Delete 2FA access	32
3I. View activity logs	33
4. Map	34
5. Users	35
5A. Add users	35
5B. Add Multiple Users	36
5C. Cancel user invite	37
5D. Edit user	37
5E. Deactivate users	38

5F. Reactivate users	39
5G. User Batch Replication	40
6. Jobs List	42
6A. Creating jobs	42
6B. Pushing jobs to lock	42
6C. Deleting jobs	43
6D. Completed jobs	43
6E. Failed jobs	43
- View failed jobs	44
- Retry failed job	44
7. My Profile	44
8. Settings	45
8A. Dashboard Settings	45
8B. Security	45
- 2-step verification	45
- Minimum password length	45
- Maximum failed attempts	45
8C. Audit trail	46
8D. Analytics	46
8E. Email template	46
8F. Change language	47
Unlocking with access	48
9. Unlock with Master PIN	48

10. Unlock with added PIN	49
11. Unlock with Bluetooth access	50
12. Unlock with 2FA access	51
12A. Generate 2FA passcode	51
12B. Reset 2FA passcode	52
13. Search Feature	53
Flat Organisation	54
Help and Support	54
Change password	54
User types and permissions chart	55
Dashboard	55
App	57

Welcome to iglooworks

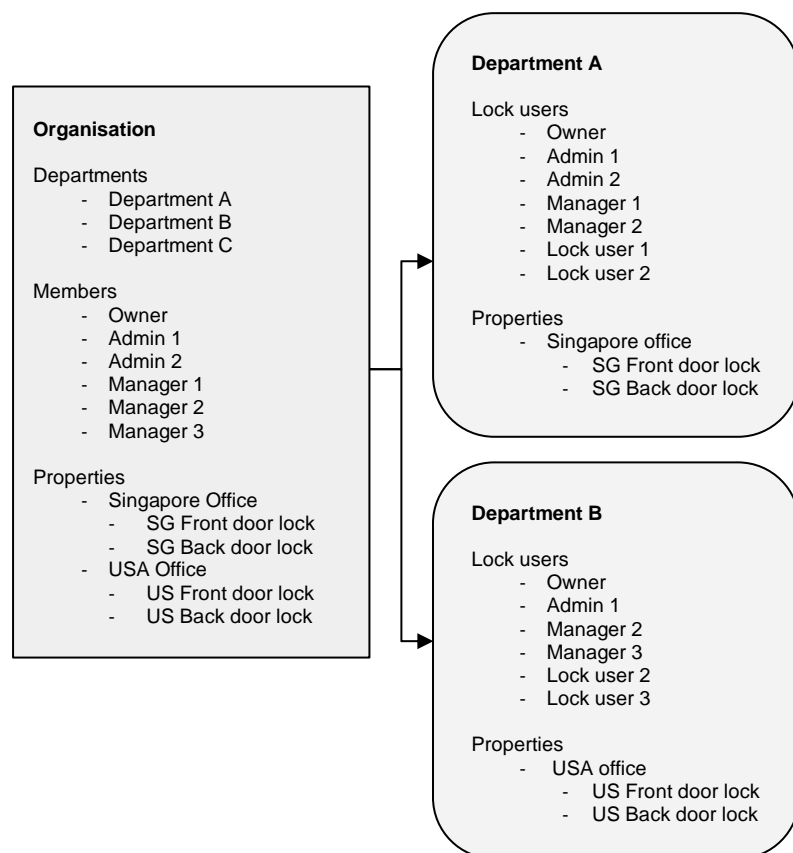
Thank you for choosing iglooworks. Our smart access solutions combine award-winning igloocompany smart locks and enterprise-grade software to allow organisation admins to manage access for multiple locks and users.

Before you begin

1. Use the quickstart guide to set up your account and locks
2. Use a supported browser: Dashboard works best with Google Chrome

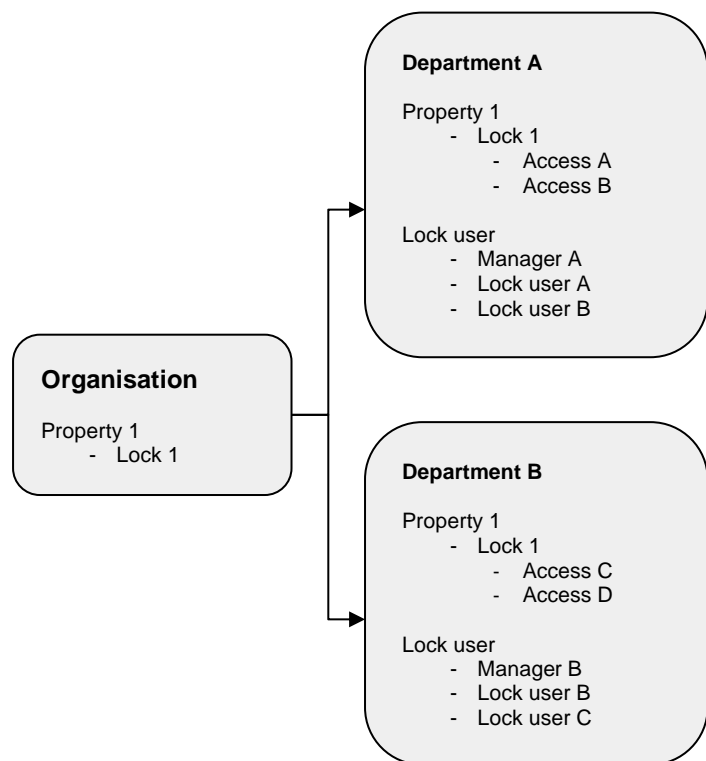
Data Architecture and Workflow

Organisation data structure



The organisation account is managed by the owner and admins. They manage all departments, properties, locks, and members. As part of the account set up, they will assign managers and properties to departments. Managers will then be able to manage access for all the locks in the properties that have been assigned to them.

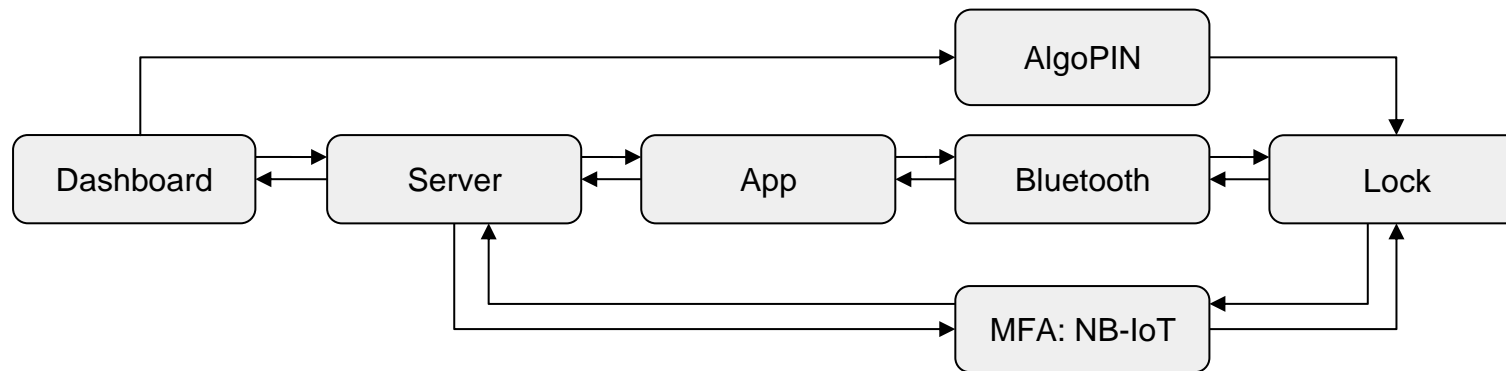
Department data structure



The owner and admin can use a department to assign the properties within the organisation that managers have rights to.

Department data is not shared across departments; if a property is in multiple departments, the access created will not be reflected for the same property in another department. A lock user that has been invited to a department will also not show up in another department unless they are specifically added.

Lock Access workflow

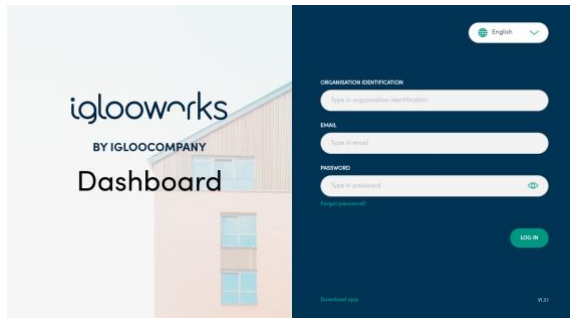



All access is added from the dashboard. Depending on the type of access, there is a different workflow to access the lock:

1. AlgoPINs can be directly used on the lock without any internet or Bluetooth connectivity. However, the activity is not updated until the lock is synced.
2. Bluetooth keys require access to the internet and Bluetooth via the iglooworks App. The activity is updated as long as the app is connected to the internet.
3. For 2FA (2-factor authentication) access, the lock needs to be connected to the NB-IoT network. The activity is updated via the network depending on the sync interval settings.

Login

Go to dashboard.iglooworks.co and login with your credentials.



 Tip: Organisation identification is the same for all users logging into the same organisation.

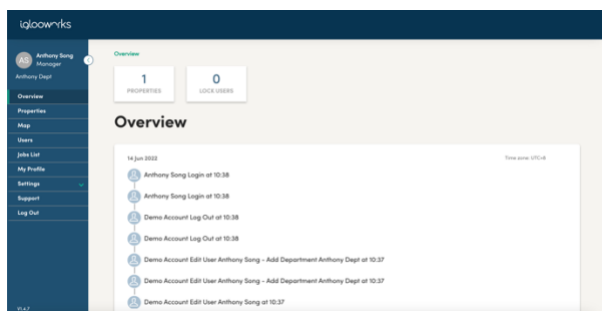
2FA login

If 2FA login is enabled by the admin, verify the OTP to login.

Owner and admin controls

1. Overview

The overview page gives a summary of the organisation.



However, PIN access is not default for all users and will have to be created in order for any user to access the lock via PIN code, with the exception of the Master PIN.

For security purposes, access for the same lock in multiple departments is also not shared. This means that access that a manager created for Lock A in Department A will not be shown to a manager managing Lock A in Department B and vice versa.

Before setting up a department, it is important to think about how the departments in the organisation should be structured, depending on the users who should have access to properties.

2. Departments**

A department allows the owner or admins to control the properties a manager can manage within the organisation account.

An owner/admin may create a Department (Department A) which contains:

- Properties (Building 1, Building 2), and
- Managers (Manager 1, and Manager 2)

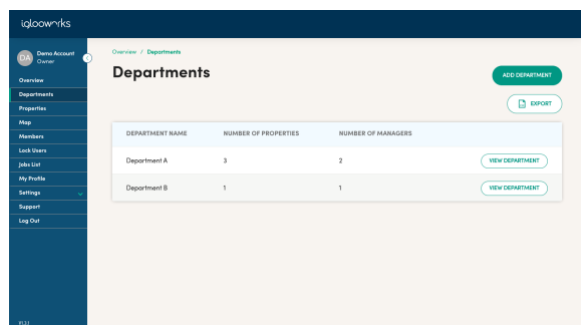
A manager may be assigned to multiple departments.

The owner and admins can manage all departments and have Bluetooth/2FA access to all locks in the organisation by default. Managers have Bluetooth/2FA access to all locks in the departments by default. Lock users will only have Bluetooth/2FA access if access is added to them.

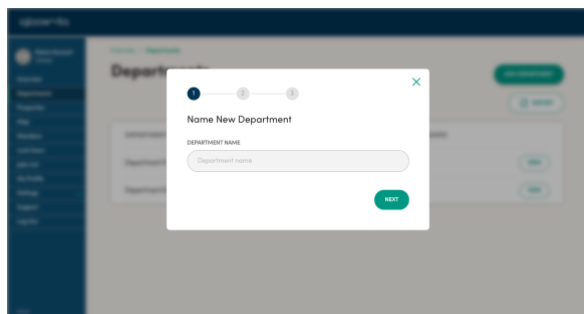
** Not for organisations under Flat Organisation

2A. Add department

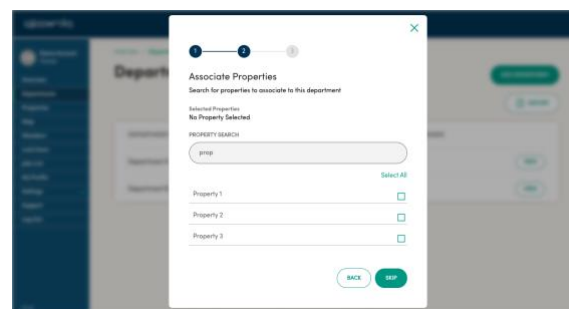
1. Click on 'Add Department'



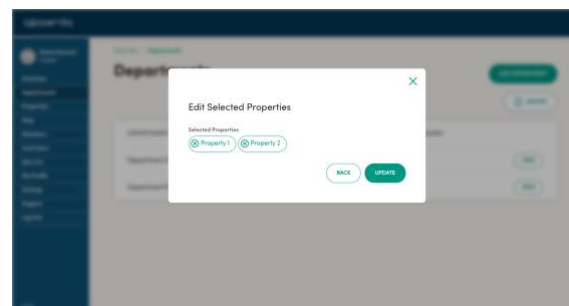
2. Set a name for the department



3. Search for properties and select the checkbox to assign to them to the department.



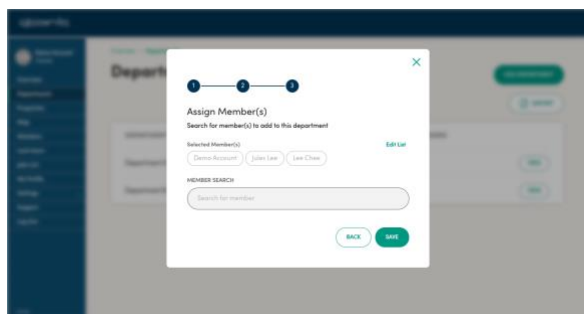
4. To view the full list or remove selected properties, click on 'Edit List' and remove properties by clicking the 'x'. Once the property list looks good, click Update. Click 'Back' to go back without saving



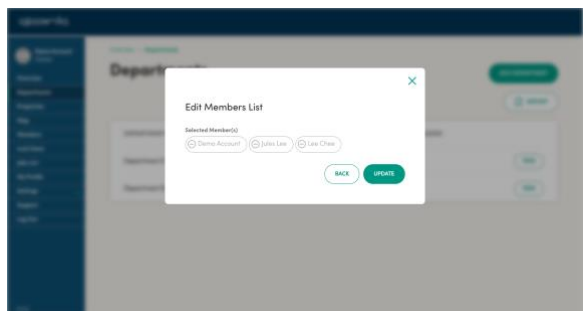
5. Click 'Next' to proceed. You can click 'Skip' if there are no properties in the organisation yet, to add properties to the department at a later time, go to [Edit Department](#)

💡 Tip: There is no limit to the number of properties that can be assigned to a department.

6. Search for the member and select the checkbox to assign them to the department.



7. To view the full list or remove selected members, click on 'Edit List', and remove members by clicking on 'x'. Once the members list looks good, click 'Save'. Click 'Cancel' to go back without saving



8. Click 'Save' to save the new department

💡 Tip: There is no limit to the number of members that can be assigned to a department.

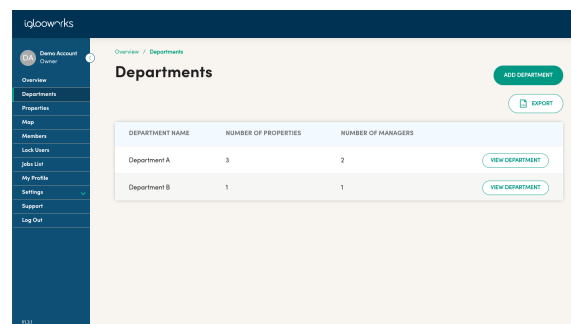
💡 Tip: Department names must be unique.

💡 Tip: Owners and admin are added to all departments as managers by default and cannot be removed.

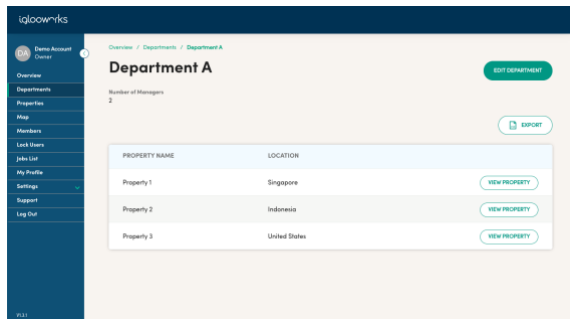
💡 Tip: There is a limit of 20 departments for each organisation.

2B. Edit department

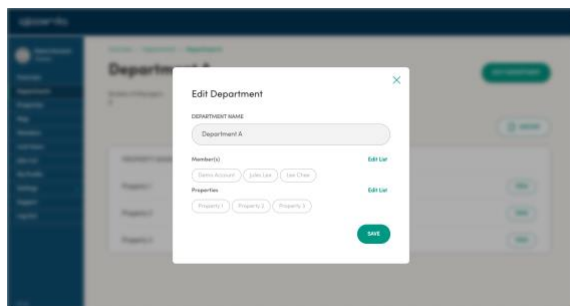
1. Click on 'View department' on the department list



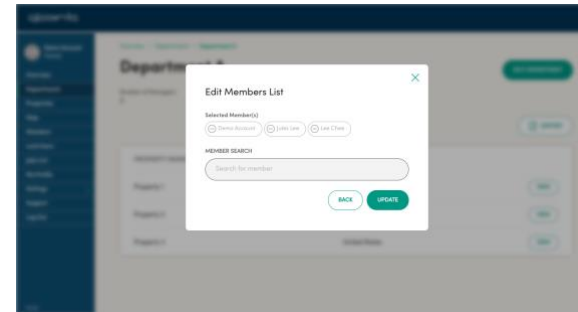
2. Click on 'Edit Department'



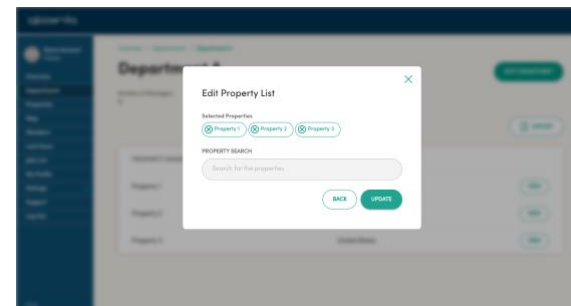
3. Change the name by typing in the Department Name field



4. Click 'Edit List' to edit the members in the department. To add members, search for and select the member in the search results. To remove members, click 'x' next to the name. Click on 'Save'



6. Click 'Edit List' to edit the properties in the department. To add properties, search and select the property in the search results. To remove properties, click 'x' next to the name. Click on 'Save'



8. Click 'Save' to save the changes

2C. Delete department

A basic deletion feature is available. This feature currently only allows you to delete certain types of departments:

- Departments without a property
- Departments with a Property, but the Property has no locks
- Departments with a Property, the Property has locks, but the Department does not have any active PINs on those locks
- Departments with a Property, the Property has locks, and the Department has active Bluetooth Keys on those locks

3. Properties

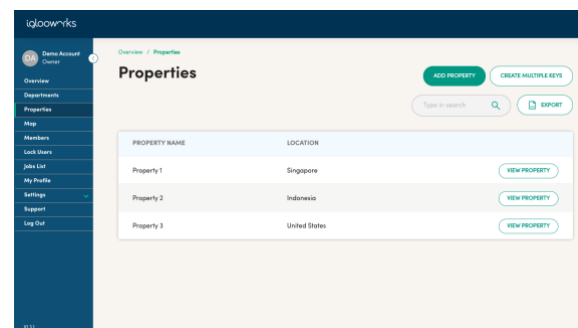
Before pairing locks, properties need to be added to the organisation. Properties are used to group locks, and they also set the lock's time during pairing.

As a rule of thumb, properties should be created based on the location of the locks e.g. if there are 2 offices in the organisation, 2 properties should be added. However, properties do not necessarily have to represent a physical location as long as the time zone is the same for the locks in the property.

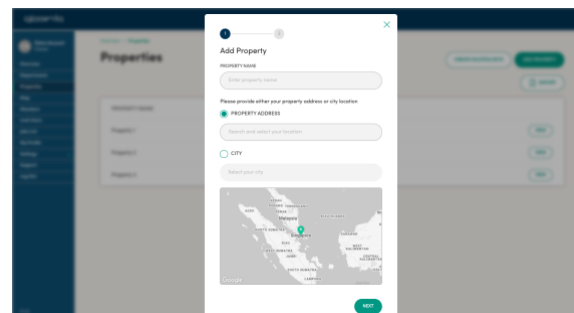
It's a good idea to plan out the properties to add as they will later be managed with departments.


3A. Add properties

1. Go to Properties and click on 'Add Property'

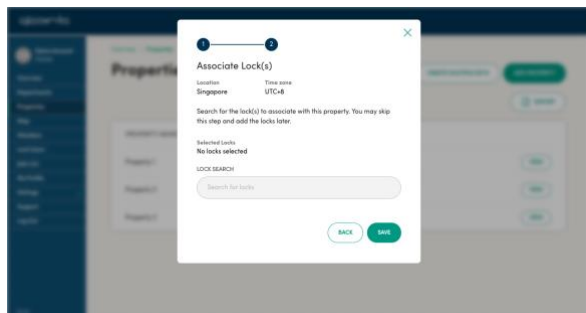


2. Enter the property name, select either address or city, then search for the location for this property. Click 'Next' to proceed.



 **Tip:** Providing the property address allows it to show up on the map in the department view, while providing the city does not. The city option is for organisations who do not want to store the specific address of the property.

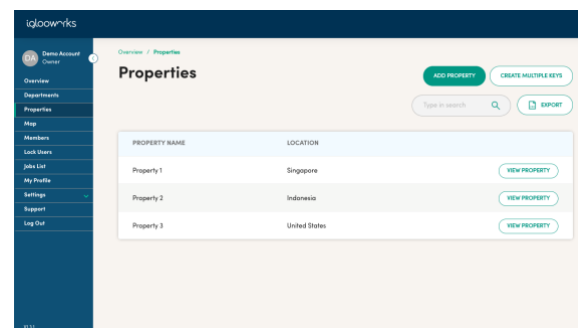
3. Search for locks and select the checkbox to associate the lock. Click on 'Edit List' to edit the locks for the property and click 'x' to remove locks. Click 'Save' to add the property.



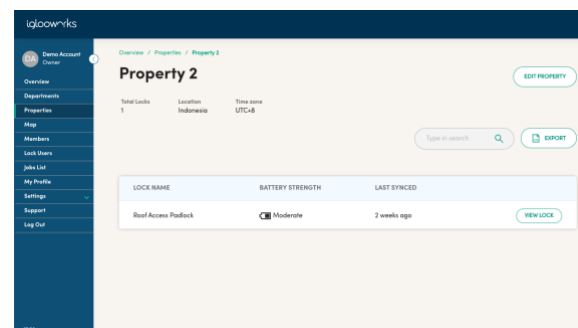
Tip: For a new organisation setup, there are no paired locks yet, so lock association can be skipped

3B. Edit Property

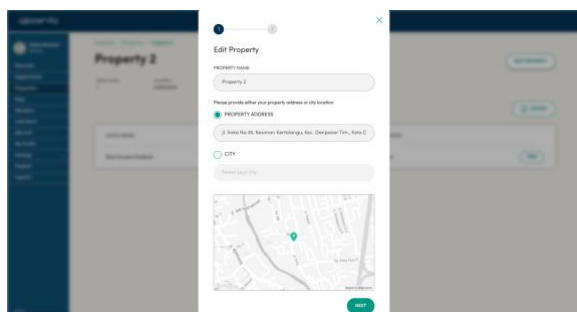
1. Click 'View Property' on the property list



2. Click on 'Edit Property'

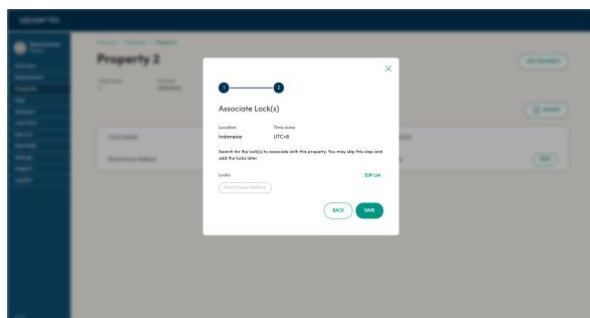


3. Property name and the address or city can be changed here. Click 'Next' to proceed

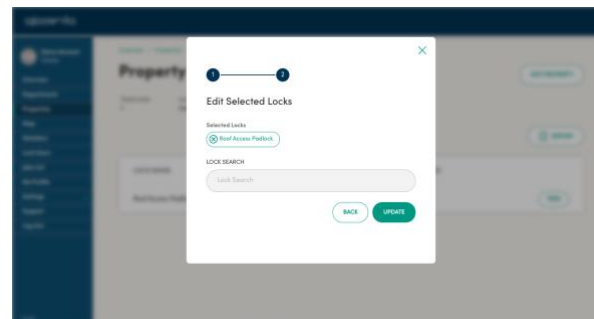


💡 Tip: A property's address cannot be changed if the new address is a different time zone from the current address

4. Click on 'Edit List' to edit the locks associated to the property



5. Search for locks and select the checkbox to associate the lock. Click 'x' to remove locks. Click 'Update' to save changes or 'Back' to go back without saving.



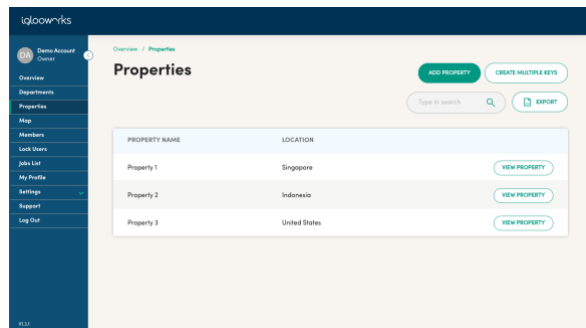
💡 Tip: A lock cannot be removed from the property if it is only in one property

3C. Delete property

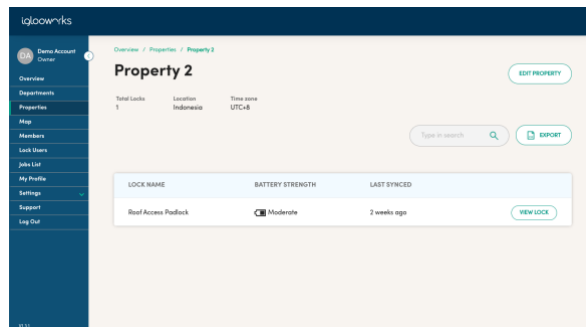
A basic deletion feature is available. This feature only allows you to delete empty properties (i.e. properties that do not have any locks).

3D. Edit lock name

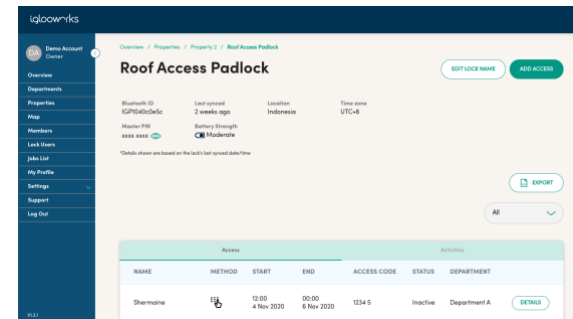
1. Click on 'View Property' on the property list



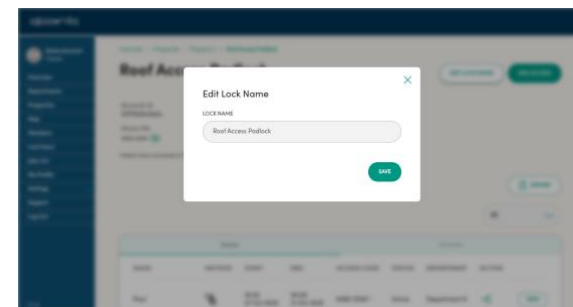
2. Click on 'View Lock' on the locks list




3. Click on 'Edit Lock Name'

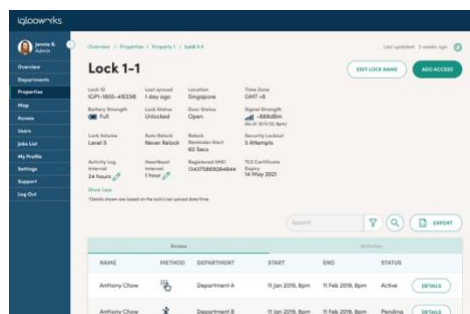


4. Change the lock name and 'Edit'

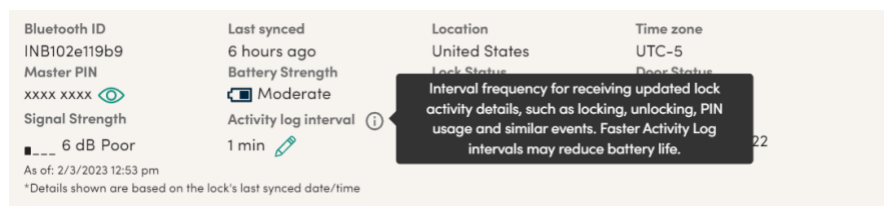


3E. Edit lock Activity log/ Heartbeat Intervals (INB1 Only)

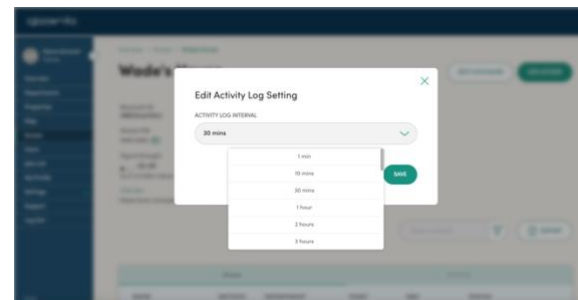
1. On the lock details page, click on the  icon beside the time for Activity log interval




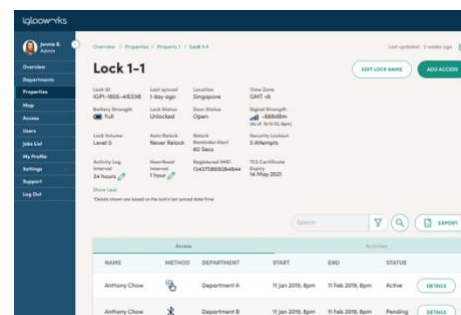
2. Click on “I” beside Activity log interval to read more information about what this represents



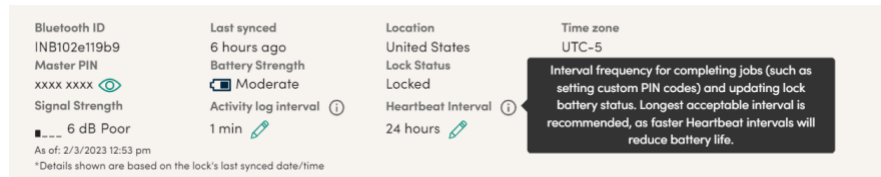
3. Select the new time that you wish to set for Activity log interval: 1 min/ 10 mins / 30 mins/ 1 to 24 hours and click ‘Save’, the new time interval will be set on the next heartbeat.



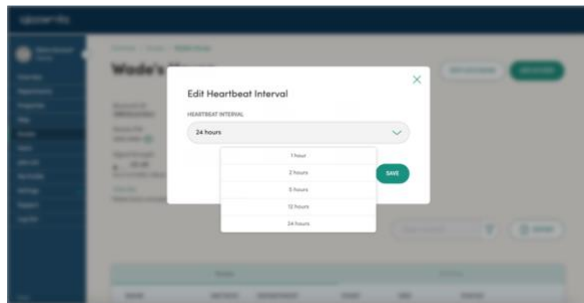
4. On the lock details page, click on the  icon beside the time for Heartbeat interval




5. Click on “I” beside Heartbeat interval to read more information about what this represents



6. Select the new time that you wish to set for Heartbeat interval: 1 hour/ 2 hours/ 5 hours/ 12 hours/ 24 hours and click 'Save', the new time interval will be set on the next heartbeat.



 Tip: Heartbeat transmission includes sync of new logs, pending jobs, battery status, signal strength, carrier and channel band connection info, while activity log transmission includes only sync of new logs.

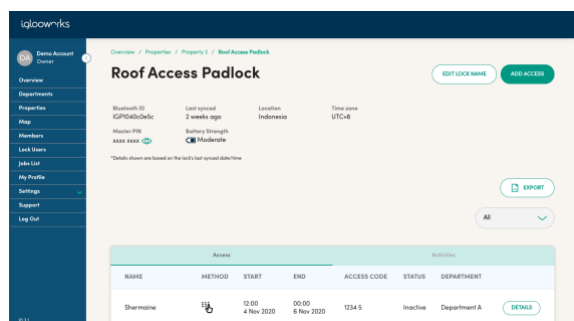
3F. Add access

- Add Remote PIN Access

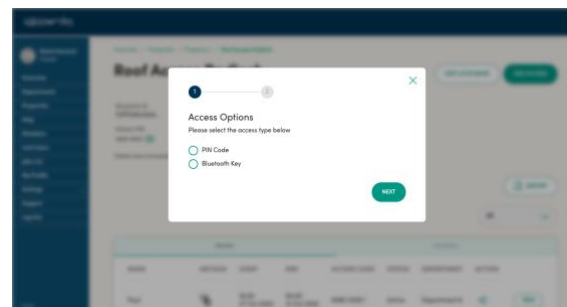
Remote PIN Access is useful for creating a PIN without having to be near the lock. There are 3 PIN types: One time, Duration, and Permanent. There is a limit of 199 active remote and custom PINs at a time.

PINs have to be used within 24 hours of the PIN start time/date. Depending on the lock model, the PIN activity may not be updated in real-time, so a user will have to sync the lock to update the activity logs on the dashboard.

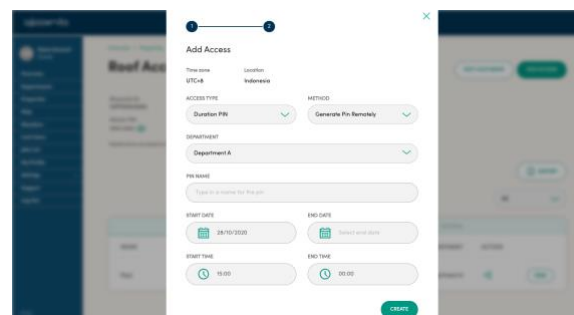
1. Click on 'Add Access'



2. Select 'PIN Code' and click 'Next'



3. Select the Access Type and 'Generate PIN remotely' as the method, then select the Department** and fill in the PIN details. Click "Create" to proceed

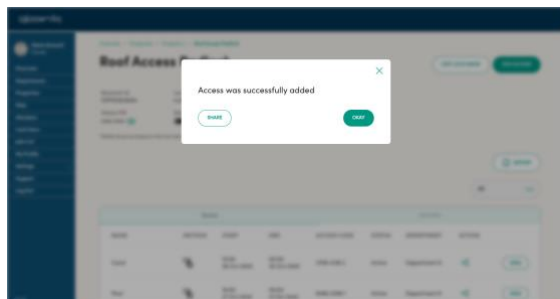


Tip: PIN start date and time cannot be in the past and has to be within 14 days in the future from the time of PIN creation.

** Not for organisations under Flat Organisation

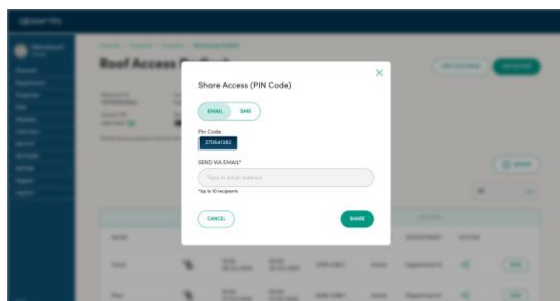
💡 Tip: Only departments that the lock is associated with will appear in the department dropdown selection**.

4. Click 'Share' if you would like to share the PIN via email or SMS



💡 Tip: Country code for phone numbers will be defaulted to the last chosen without the need to select from country list again

5. Enter the recipient's email and click '+'. To share via SMS, toggle to SMS and enter the region code and phone number. Click 'Share'



💡 Tip: Only one type of share method can be used at a time. Up to 10 recipients can be added for email.

6. The access will be added to the access list and ready for use (See [Unlock with added PIN](#) on how to use a PIN code)

** Not for organisations under Flat Organisation

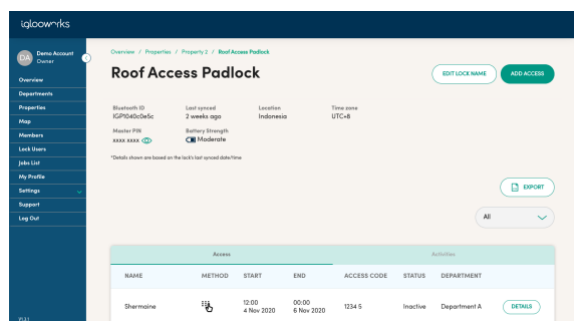
- Add Custom PIN Access

Custom PIN Access is useful for creating a PIN with a preferred 4-6 digit PIN combination. This method creates a Custom PIN job on the dashboard to be pushed to the lock via the app for the PIN to be active. There are 3 PIN types: One time, Duration, and Permanent. There is a limit of 199 active remote and custom PINs at a time.

To create a custom PIN, the lock must only be in 1 department. A lock cannot be added to another department** if a custom PIN has been created for this lock.

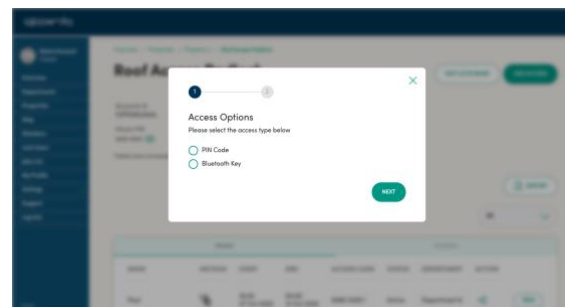
PINs used are not updated in real-time, so a user with Bluetooth Sync access will have to sync the lock for the activity logs to be updated.

1. Click on 'Add Access'

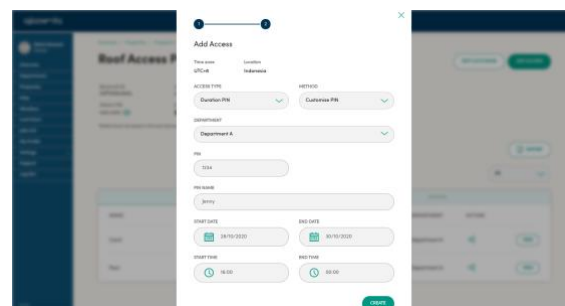


** Not for organisations under Flat Organisation

2. Select 'PIN Code' and click 'Next'



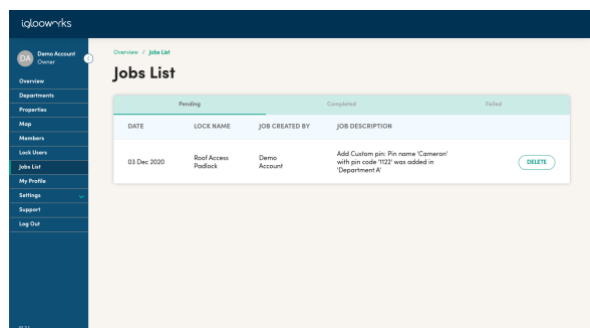
3. Select the Access Type and 'Customise PIN' as the method, then select the Department** and fill in the PIN details. Click "Create" to add this to the job list



Tip: PIN start date and time cannot be in the past and has to be within 14 days in the future from the time of PIN creation.

Tip: Only departments that the lock is associated with will appear in the department dropdown selection**.

4. A success popup will show if the job has been created. Go to the Job List to ensure that the access is in the Pending list



5. As an owner/admin/manager, go to the lock and click 'Sync' on the app to push the PIN into the lock via Bluetooth. For information on pushing jobs, see [Pushing Jobs to Lock](#)

6. After the job is complete, the access will be added to the access list and ready for use (See [Unlock with added PIN](#) on how to use a PIN code)

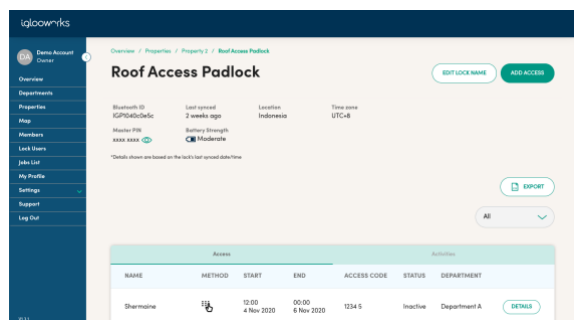
- Add Single Bluetooth Access

There are 3 Bluetooth permissions: Unlock, Sync, Firmware Update.

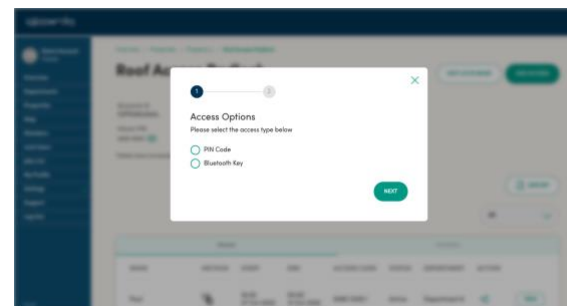
Unlock allows a user to unlock the lock with the app. Sync allows a user to update the activity logs to the dashboard with the app. A lock user needs to be invited to the department** before Bluetooth access can be created (See [Lock users](#)). Firmware Update allows access to update the lock's firmware via iglooworks app.

Owners, admins, and managers already have Bluetooth access by default, so it is not necessary to add Bluetooth access for them.

1. Click on 'Add Access'

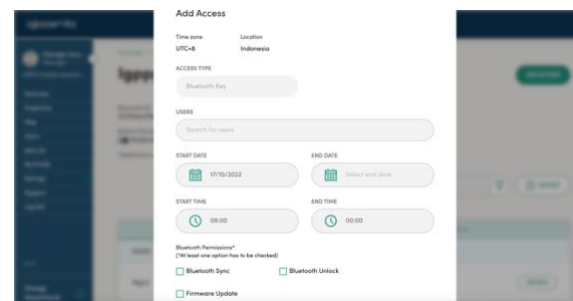


2. Select 'Bluetooth Key' and click 'Next'



3. Select the department** and key in the access details. Click 'Create' (Note: You can add multiple lock users at the same time, but the access time and date will be the same)

** Not for organisations under Flat Organisation



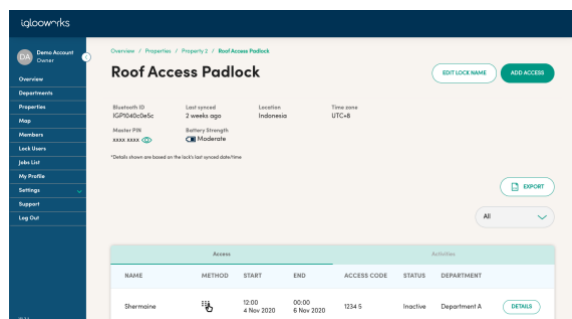
4. The created Bluetooth access can be seen in the lock's access list and will be added to the lock user directly, and they will be able to see it on the iglooworks app. (See [Unlock with Bluetooth access](#) on how to use Bluetooth keys). An email notification will also be sent to the user with the key details.

** Check Firmware Update to give lock user Firmware update rights on iglooworks app for the selected lock

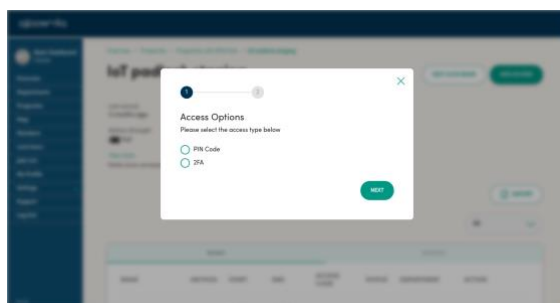
- Add 2FA Access

2FA access is useful for higher security applications where 2 modes of authentication needs to be verified before the lock is unlocked. This access method will only appear if the lock is an NB-IoT 2FA lock. All 2FA users need to be added as a lock user and have a verified mobile number.

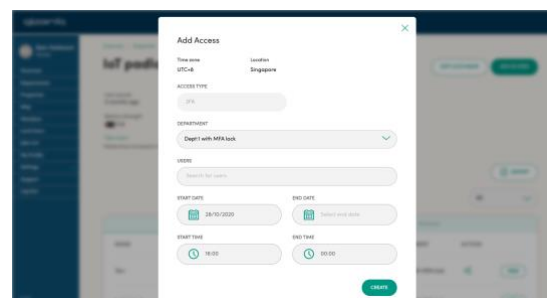
1. Click on 'Add Access'



2. Select '2FA' and click 'Next'



3. Select the department**, key in the access details and click 'Create'

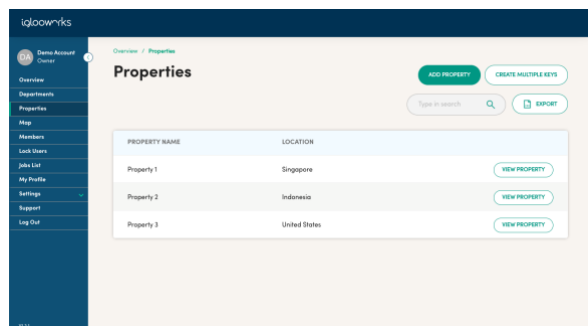


4. The access will be available to use by the user (See [Unlock with 2FA access](#) on how to generate an 2FA passcode)

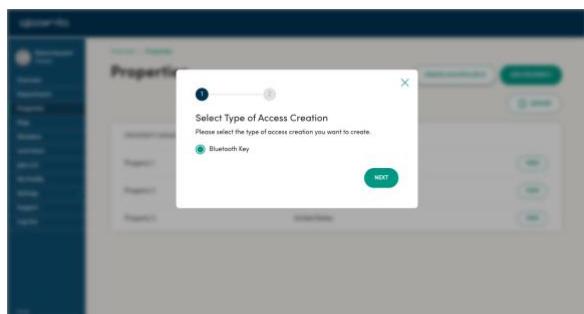
** Not for organisations under Flat Organisation

- Add Multiple Bluetooth Access

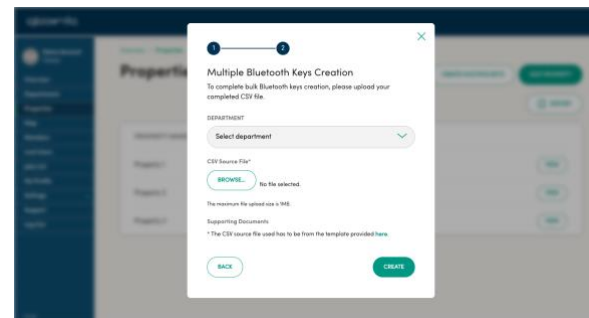
1. On the Properties page, click on “Create Multiple Keys”



2. Select ‘Bluetooth Key’



3. Download the CSV template along with the user and lock list, then upload the completed CSV file by clicking on ‘Browse’ and selecting the file to upload, then click ‘Create’



4. An email report will be sent once the CSV file has been processed.

Tip: Use the README in the template for information on how to prepare a file for uploading.

3G. Edit access

- Edit Remote PIN access

It is not possible to edit a remote PIN. You may choose to Delete the PIN and [add a Custom PIN](#) instead.

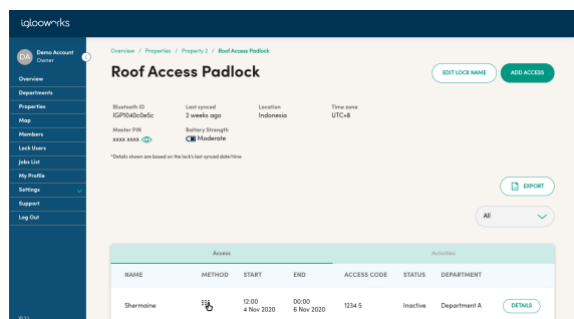
- Edit Custom PIN access

It is not possible to edit a custom PIN. You may choose to Delete the PIN and [add a Custom PIN](#) instead.

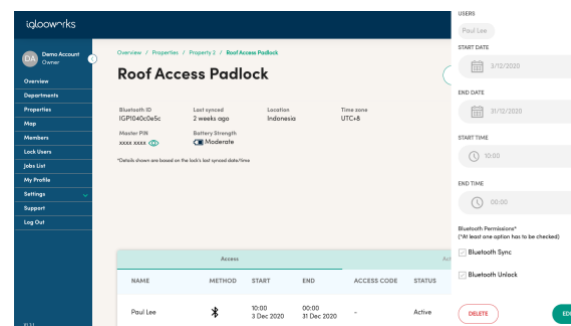
- Edit Bluetooth access

Only the end date and time of the Bluetooth access can be edited provided the access has not expired.

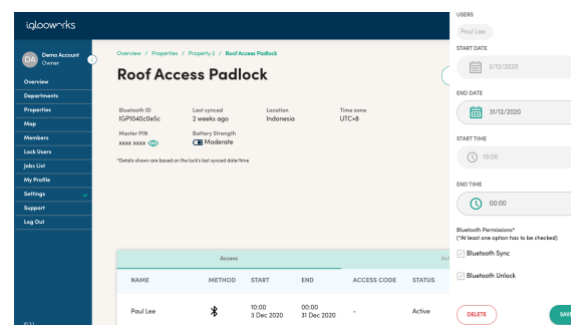
1. Click 'Details' on the access list



2. Click 'Edit'



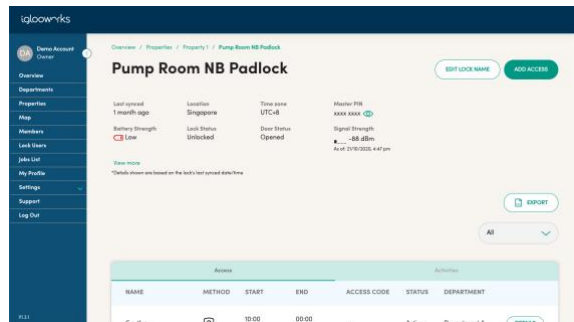
3. Make the changes and click 'Save'



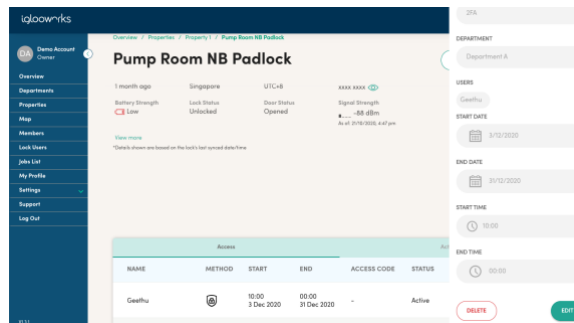
- Edit 2FA access

Only the end date and time of the 2FA access can be edited provided the access has not expired.

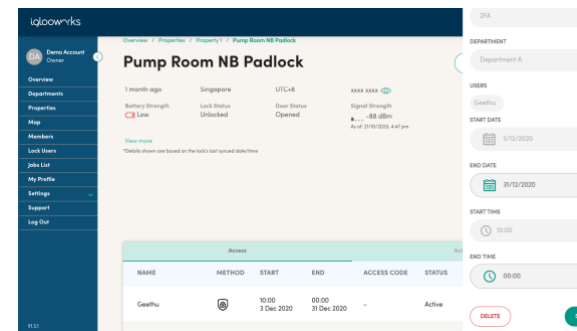
1. Click 'Details' on the access list



2. Click 'Edit'



3. Make the changes and click 'Save'

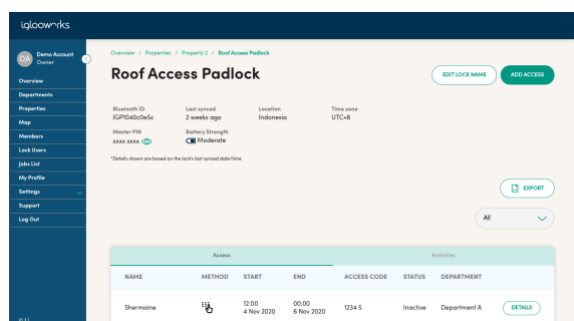


3H. Delete access

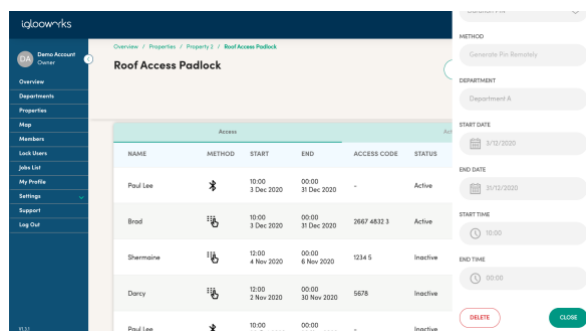
- Delete Remote or Custom PIN access

Deleting PIN code is done via jobs. After adding the job to delete the PIN, use the app to sync the job to the lock.

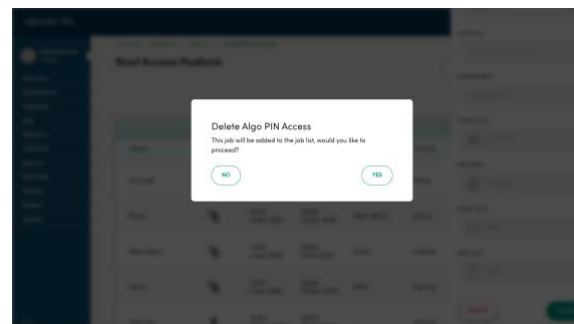
1. Click 'Details' on the access list



2. Click 'Delete'



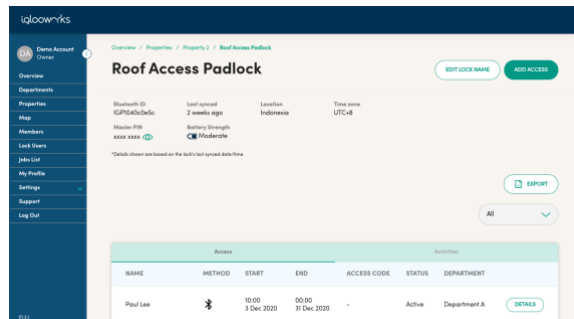
3. Click 'Yes' on the confirmation screen



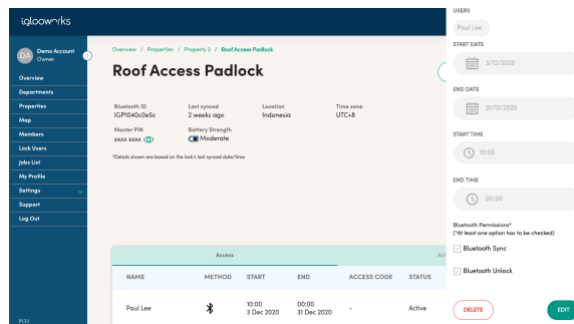
4. The job is now created. Using the app, sync with the lock to complete the job.

- Delete Bluetooth access

1. Click 'Details' on the access list



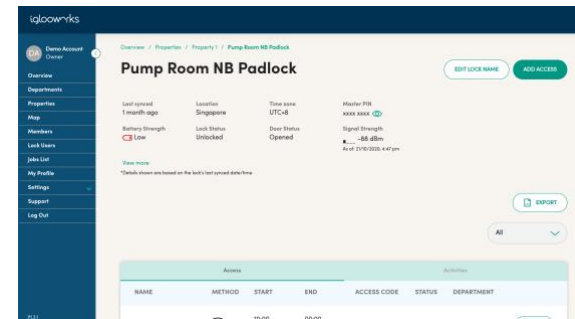
2. Click 'Delete'



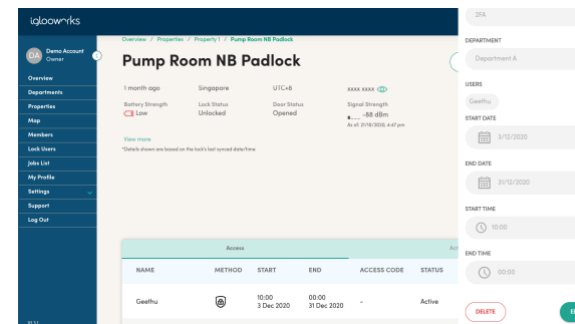
3. Click 'Yes' on the confirmation screen, and the Bluetooth access is deleted.

- Delete 2FA access

1. Click 'Details' on the access list



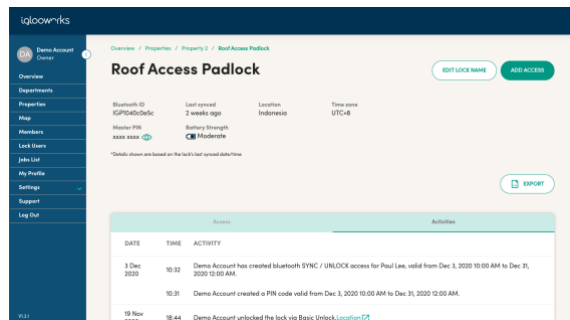
2. Click 'Delete'



3. Click 'Yes' on the confirmation screen, and the 2FA access is deleted.

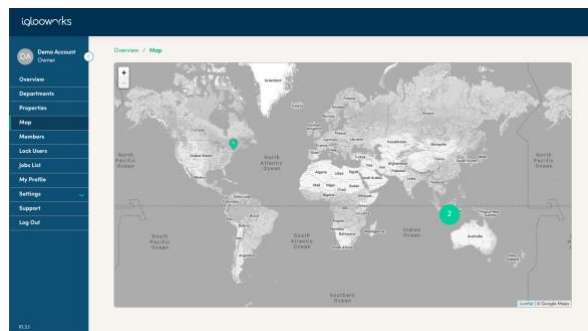
31. View activity logs

On the lock detail page, click on 'Activities' tab to view



4. Map

The map shows where the properties in the organisation are located on the map. For properties spread out over a wider area, click on the number icon to zoom in. Click on the drop pin to select the property, and click on the property name to view the property.

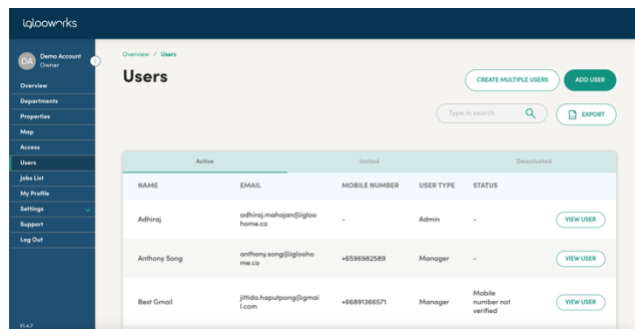


5. Users

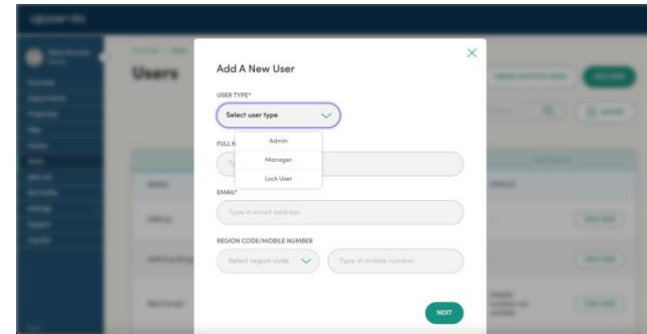
Users include the owner, admin, and managers. In this view, the owner and admin can manage dashboard users. User permissions can be found in the [User Types and Permissions Chart](#) section of this guide.

5A. Add users

1. Go to Users and click on 'Add User'



2. Select 'Admin' from the dropdown if this user is an admin, select 'Manager' if the user is a manager or select 'Lock User' if user is a lock user, key in their details and click 'Next'



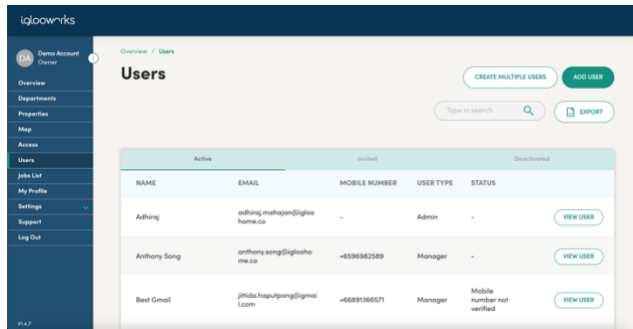
Tip: Country code for phone numbers will be defaulted to the last chosen without the need to select from country list again

3. The team member will receive an invitation email/SMS

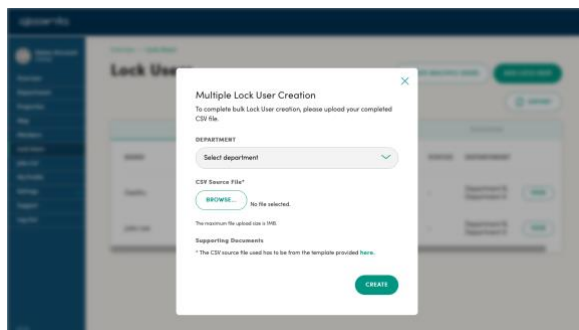
Tip: Managers will not be able to login to the dashboard until a department has been assigned to them

5B. Add Multiple Users

1. Click on 'Create Multiple Users'



2. Download the CSV template and prepare it for uploading. Select the department then upload the completed CSV file by clicking on 'Browse' and selecting the file, then click 'Create'



Tip: Use the README in the template for information on how to prepare a file for uploading.

3. An email report will be sent once the CSV file has been processed. The report will state the number of requests that were successful or failed, and a CSV report will be attached.

iglooworks basicigloo Bulk Create Lock User Report Inbox x

do-not-reply@igloohome.co
to igwqa

Hi Basic Dashboard,

This is an automated email to inform you that the bulk request was processed.

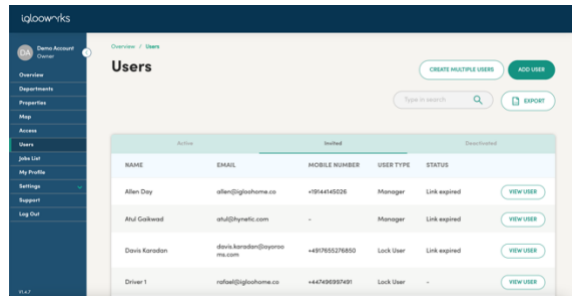
Total requests: 2
Successful: 2
Failed: 0

Please check the attached CSV file for more details.

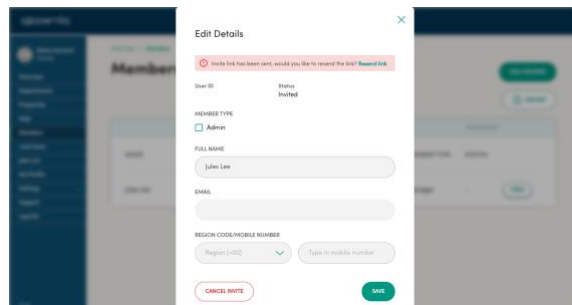


5C. Cancel user invite

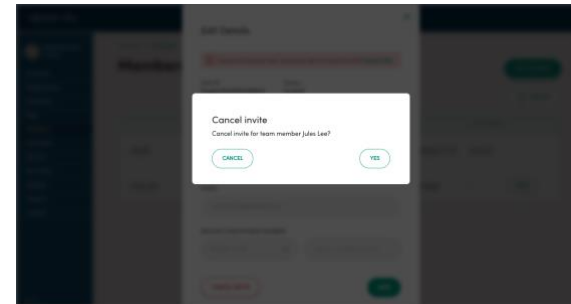
1. Click on the 'Invited' tab and 'View User' on the list



2. Click on 'Cancel Invite'

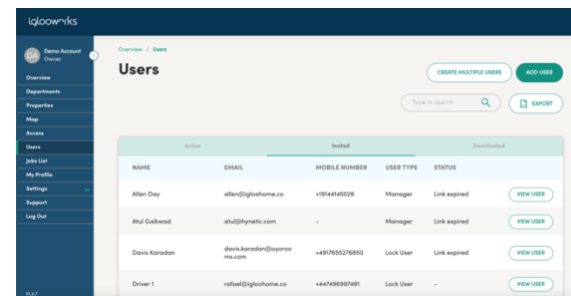


3. Click on 'Yes'

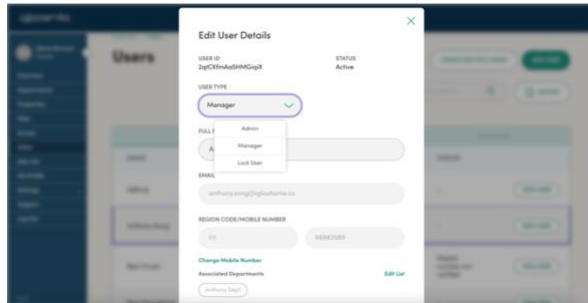


5D. Edit user

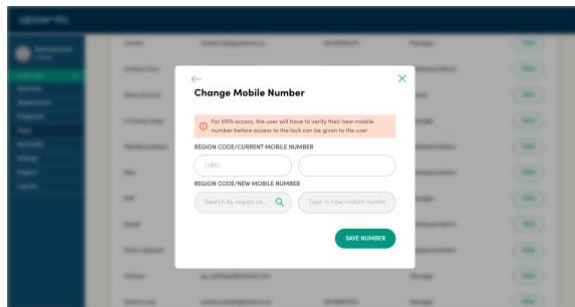
1. Click on 'View User' on the users list



2. Click on the User Type dropdown list to switch the user to Admin, Manager or Lock User. Edit the name and/or click 'Change Mobile Number' to change mobile number for the user, then click 'Save'



4. Enter the new region code and mobile number, and click 'Save Number'



5. Click 'Save'

Tip: For 2FA users, they will not be able to access the locks until the new phone number is verified

Tip: When an admin is switched to manager, they will have access to none of the departments until assigned.

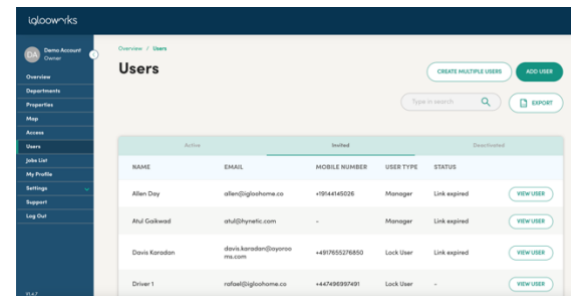
Tip: When managers are switched to admin, they will have access to all departments.

5E. Deactivate users

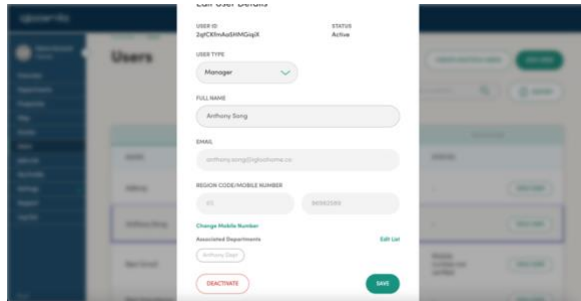
Deactivating a user removes them from the Active user list. They will not be able to login to the dashboard or app after they have been deactivated, and all Bluetooth Access will be removed.

However, any PINs that they had knowledge of can still be used until expired or deleted.

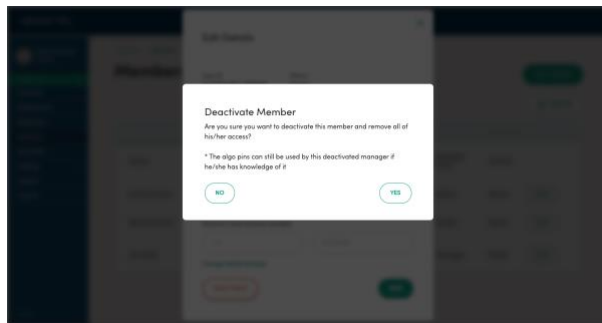
1. Click 'View User' on the users list



2. Click on 'Deactivate'



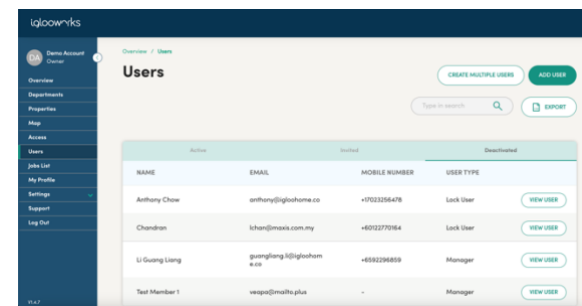
3. Click 'Yes' on the confirmation popup



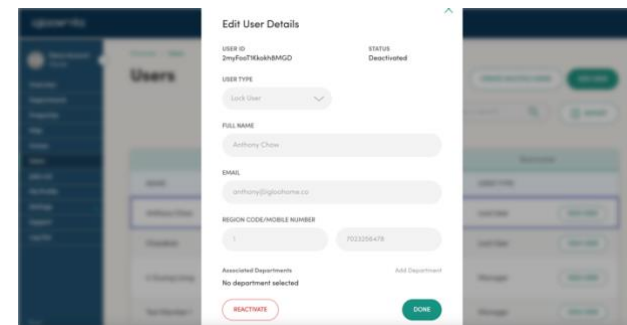
5F. Reactivate users

Reactivating users places them back in the Active user list. They will be able to login to the dashboard and app, however all previously created Bluetooth access will need to be re-created.

1. On the user's list, click on 'Deactivated' tab and click 'View User' on the user list



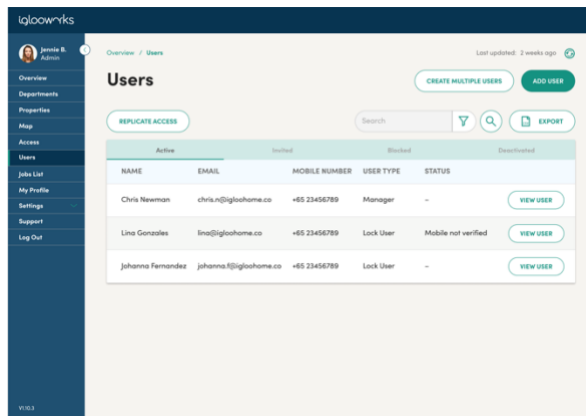
2. Click on 'Reactivate' and 'Yes' on the confirmation popup



5G. User Batch Replication

User Batch Replication will copy a lock user's Bluetooth access for multiple locks to the users selected.

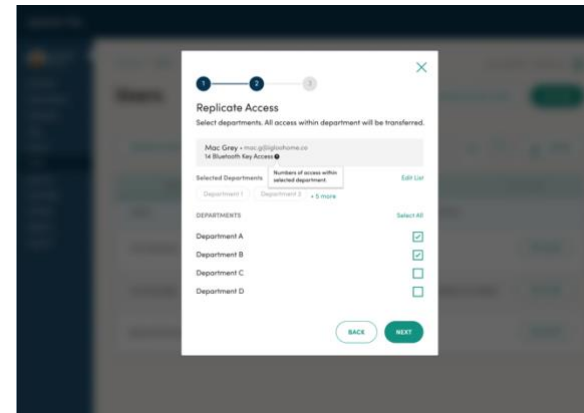
1. On the lock users list page, click on 'Replicate Access' button



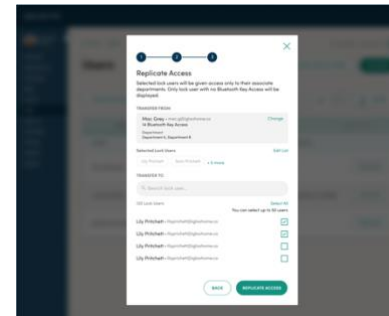
2. Type in the lock user name that you want to base on for replication in the search field and select the lock user from the list



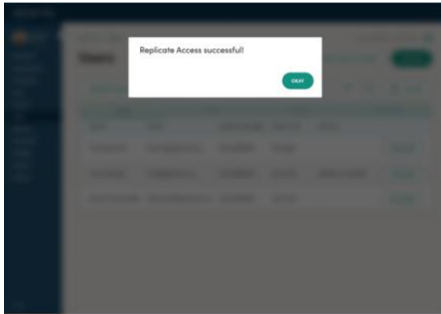
3. Select the departments that contain the locks you want the new lock users to have Bluetooth access to (Pre-requisite: You need to add these new users to the departments before executing User Batch Replication)



4. Select the lock users from the list that you want to replicate Bluetooth access from the initially selected lock user (You can only select up to 50 users)



5. Click on 'Replicate Access' button and a Replicate Access successful message will appear if everything is ok



6. Jobs List

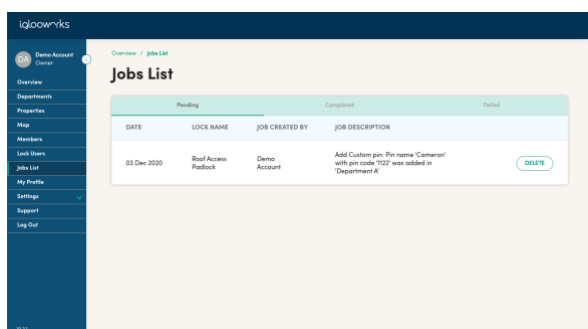
Jobs refer to Bluetooth actions that need to be pushed to the lock. They are created on the dashboard and saved in a job queue for onsite users to synchronize.

6A. Creating jobs

Jobs are created throughout the dashboard and will display on the “Pending” tab of the Jobs list.

Currently supported Jobs include:

- Create Custom PIN (see [Add Custom PIN access](#) on how to create a create Custom PIN job)
- Delete PIN (see [Delete PIN access](#) on how to create a Delete PIN job)

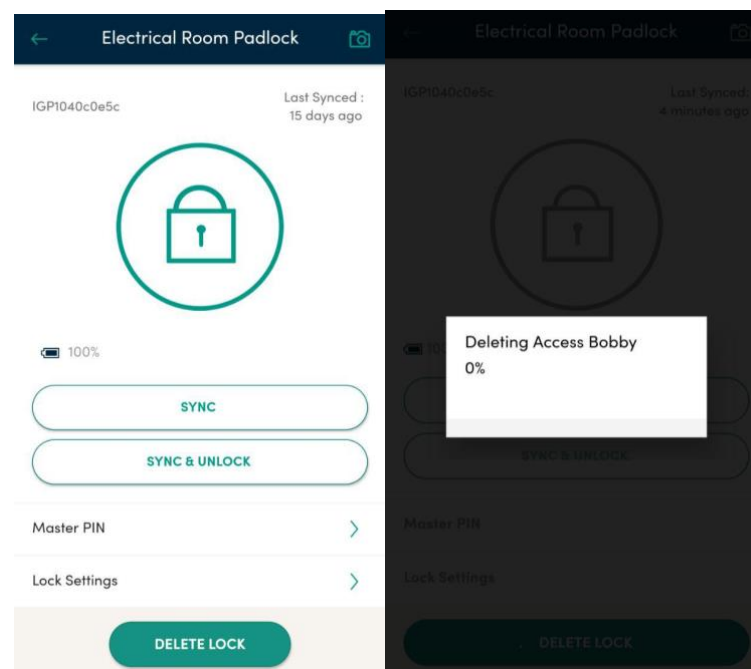


6B. Pushing jobs to lock

The following users have the following permissions to push jobs:

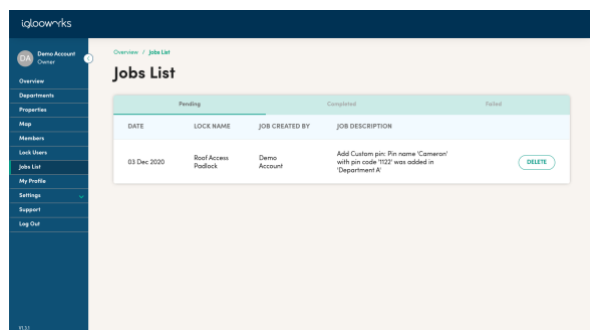
- Owners and Admins can push all jobs for all locks
- Managers can push jobs for locks in their department, but not jobs created for the same lock in another department

To push a job, the user needs to be within Bluetooth range of the lock and click on the ‘Sync’ button on the app. If there are pending jobs for the lock, the app will show a progress bar for the jobs.

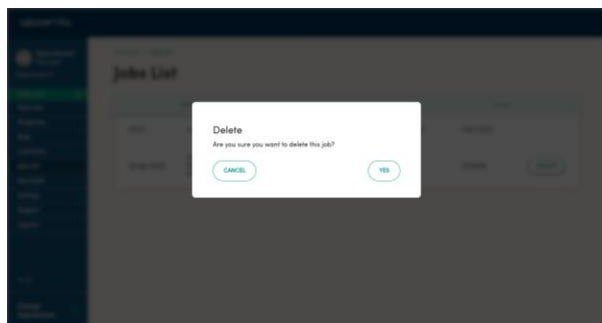


6C. Deleting jobs

1. Click on 'Jobs List' and 'Delete' next to the job to delete



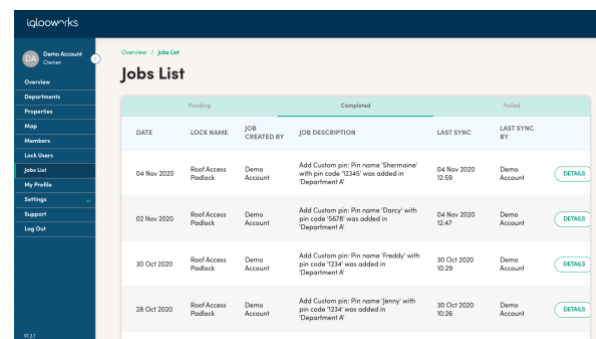
2. Click 'Yes' on the confirmation popup to delete the job



6D. Completed jobs

When jobs have been successfully completed, they will appear in the Completed Jobs List

1. Click on 'Jobs List' and 'Completed' tab to view completed jobs



6E. Failed jobs

When jobs have been processed but failed, they will appear in the Failed Jobs List.


A job is considered failed if the lock had an issue, for example if it was hard reset.

If the job could not be processed due to Bluetooth or Internet connectivity issues, it will stay in the Pending tab.

- View failed jobs

1. Click on 'Jobs List' and 'Failed' tab to view failed jobs

iglooworks

James B.
Manager

Department 2

Overview

Presentations

Shop

Access

Lock Users

Jobs List

My Profile

Settings

Support

Log Out

Overview / Jobs List

Last updated: 2 weeks ago

Jobs List

Pending			Completed			Failed	
DATE	LOCK NAME	JOB CREATED BY	JOB DESCRIPTION	PIN NAME	PIN CODE	LAST SYNC	REASON FOR FAILURE
21 Feb 2019	Lock 1-1	Mark Tan	Edit pin	Christian Santos	88888888	22 Feb 2019, 8pm	Error 401: Bad Bluetooth Connection
21 Feb 2019	Lock 1-1	Mark Tan	Delete pin	Eugenia Tan	88888888	22 Feb 2019, 8pm	Error 401: Bad Bluetooth Connection
21 Feb 2019	Lock 1-1	Mark Tan	Create Bluetooth PIN	Terry Henderson	88888888	22 Feb 2019, 8pm	Error 401: Bad Bluetooth Connection

21 Feb 2019

Change



Tip: A Job can be recreated using the Recreate job button, or by performing the original steps to create the job. However if the job was already recreated using one method e.g. Recreate job button, the other method will be greyed out e.g. Delete PIN from access list

7. My Profile


My Profile is available to organisations with 2FA locks in their account. It enables a user to set a 2FA passcode for lock access.

See [Unlock with 2FA Access](#) for how to generate and reset a 2FA passcode.

- Retry failed job

1. Click on 'Recreate Job' button to push the job back to the Pending List

igloowrks

 James B.
Henderson
Department 2

Switch View

Overview

Properties

Map

Access

Lock Users

Jobs List

My Profile

Settings

Support

Log Out

Overview / Jobs List

Last updated: 2 weeks ago

Jobs List

Pending		Completed			Failed	
JOB CREATED BY	DESCRIPTION	PIN NAME	PIN CODE	LAST SYNC	LAST SYNC BY	REASON FOR FAILURE
Mark Tan	Edit pin	Christian Santos	88888888	22 Feb 2019, 8pm	Chris Lee	Error 401: Bad Bluetooth Connection RECREATE JOB
Mark Tan	Delete pin	Eugenia Tan	88888888	22 Feb 2019, 8pm	Lydia Sim	Error 401: Bad Bluetooth Connection RECREATE JOB
Mark Tan	Create Bluetooth PIN	Terry Henderson	88888888	22 Feb 2019, 8pm	Rebecca Lim	Error 401: Bad Bluetooth Connection RECREATE JOB

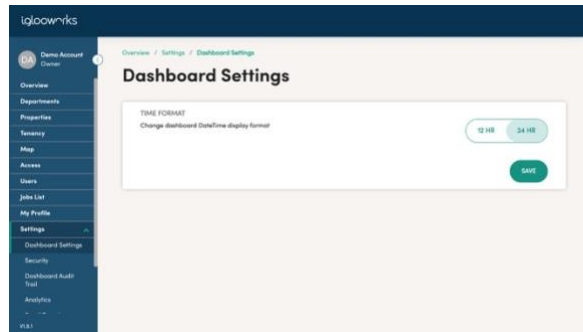
v1.0.3

Change

8. Settings

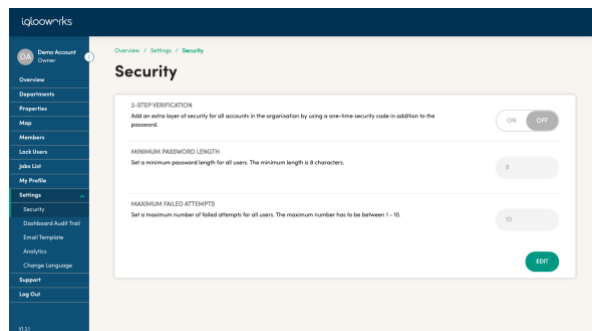
8A. Dashboard Settings

1. Click on '12 HR' or back to default '24 HR' to change the dashboard DateTime display format, and click 'Edit'



8B. Security

1. Click on 'Edit', make the necessary changes, and click 'Save'



- 2-step verification

Owner/admin can switch this on to ensure all accounts verify an OTP during login.

- Minimum password length

Owner/admin can set the minimum password length for security. Users will not be able to set a password shorter than the minimum length. The default minimum length is 8.

- Maximum failed attempts

Owner/admin can set the maximum failed attempts before a user is blocked from logging in.



Tip: In order to restore a blocked account, the user has to change their password.



Tip: There is a built-in security feature preventing users from using a common password.

8C. Audit trail

The audit trail shows the actions that have been performed by users on the dashboard.

USERNAME	DATE	TIME	ACTION
Demo Account	3 Dec 2020	10:53	Log in
Demo Account	3 Dec 2020	10:55	Invite Lock User
Demo Account	3 Dec 2020	10:55	Create 2FA Access
Demo Account	3 Dec 2020	10:52	Create Bluetooth Key
Demo Account	3 Dec 2020	10:52	Create Alpha PIN
Demo Account	3 Dec 2020	10:27	Create Job - Create Custom PIN
Demo Account	3 Dec 2020	10:02	Log in
Demo Account	2 Dec 2020	16:03	Log in
Demo Account	2 Dec 2020	14:19	Log in

8D. Analytics

1. Click on 'Low Battery Alert' to view battery level of all paired locks, then choose either to 'Enable' or 'Disable' daily email notification sent to all organisation admins. 'Filter' can be selected to filter list by department and/or property, while column headers can be clicked to sort lock list according by asc/ desc order.

NAME	BATTERY	LAST SYNCED	DEPARTMENT	PROPERTY
Lock 1.1 (SP2000-001)	95%	a month ago	Department 1	Property 1, Property 2
Lock 1.2 (SP2000-002)	Low	a month ago	Department 1	Property 1, Property 2
Lock 1.3 (SP2000-003)	Low	a month ago	Department 1	Property 1, Property 2
Lock 1.4 (SP2000-004)	Low	a month ago	Department 1	Property 1, Property 2
Lock 1.5 (SP2000-005)	Low	a month ago	Department 1	Property 1, Property 2
Lock 1.6 (SP2000-006)	Low	a month ago	Department 1	Property 1, Property 2
Lock 1.7 (SP2000-007)	Low	a month ago	Department 1	Property 1, Property 2
Lock 1.8 (SP2000-008)	Low	a month ago	Department 1	Property 1, Property 2
Lock 1.9 (SP2000-009)	Low	a month ago	Department 1	Property 1, Property 2
Lock 1.10 (SP2000-010)	Low	a month ago	Department 1	Property 1, Property 2




Tip: Battery strength of SP2E will be shown in percentage (less than 30%) while other lock models will be showing Low

8E. Email template

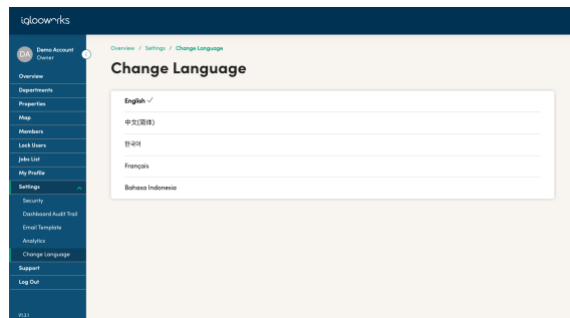
1. Click on 'Email Template' under 'Settings', then select the access type to change the template for, and click 'Edit'

2. Edit the template as desired and click 'Save'

 Tip: There is a maximum limit of 200 and 2000 characters respectively for the subject and message. Each tag needs to be used at least once in the message for it to save successfully.

8F. Change language

1. Click on the desired language and it will change automatically



Unlocking with access

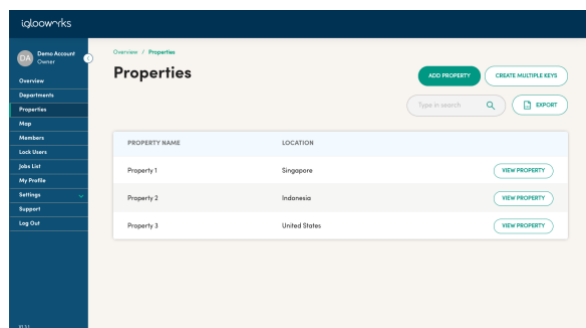
After access has been created, a user can use it to unlock the lock within the stipulated time.

9. Unlock with Master PIN

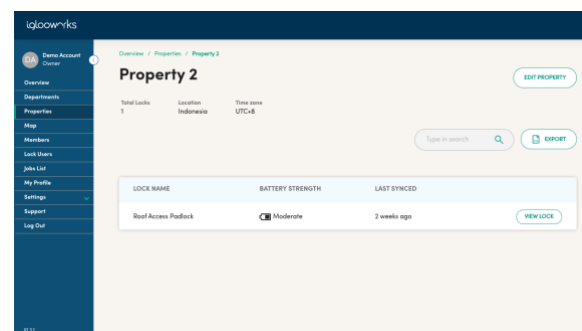
Each lock contains a master PIN after pairing - this should only be known to the owner. Do not share this PIN as anyone with this PIN can unlock the lock at any time.

To view the master PIN (owner only):

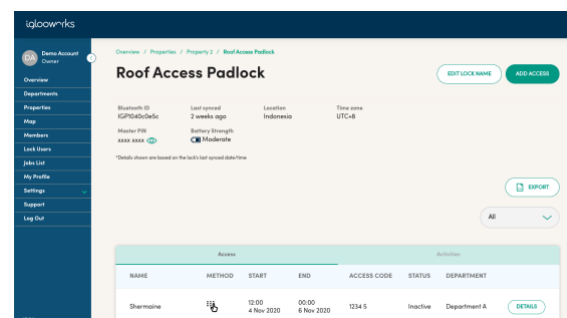
1. Click on 'View' on the property list



2. Click on 'View' on the locks list



3. Click on the eye icon to unhide the PIN code



To use this PIN, enter it on the lock, followed by the unlock icon.

To update the PIN unlock activity to the dashboard, it will require a user with Bluetooth Sync to sync the lock.

10. Unlock with added PIN

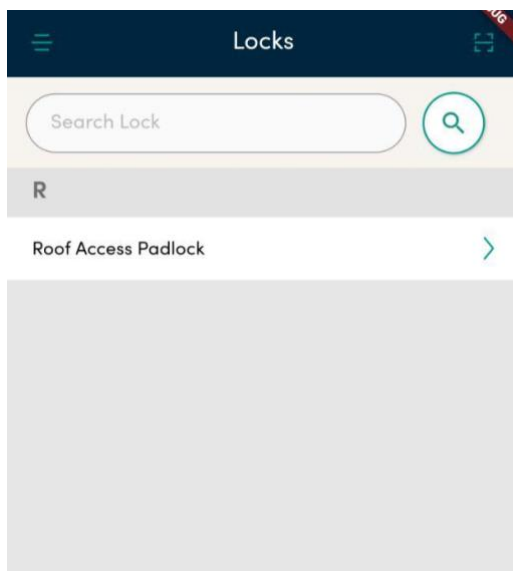
To use the PIN, the lock user can enter this PIN on the lock, followed by the unlock icon.

To update the PIN unlock activity to the dashboard, it will require a lock user with Bluetooth Sync to sync the lock.

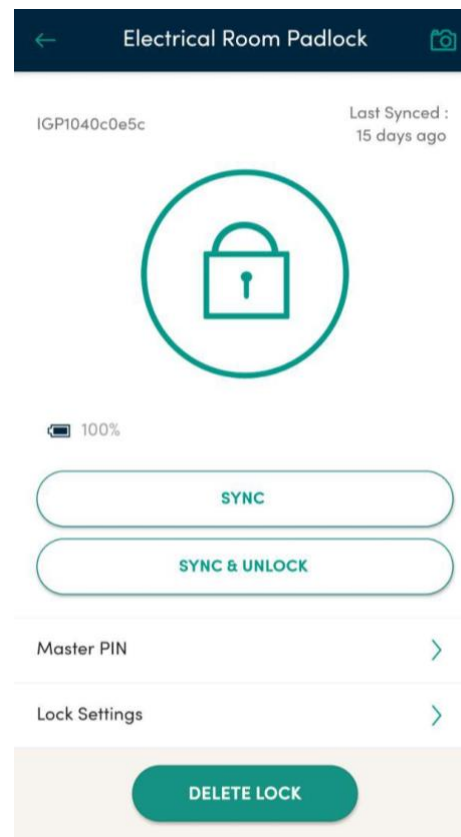
11. Unlock with Bluetooth access

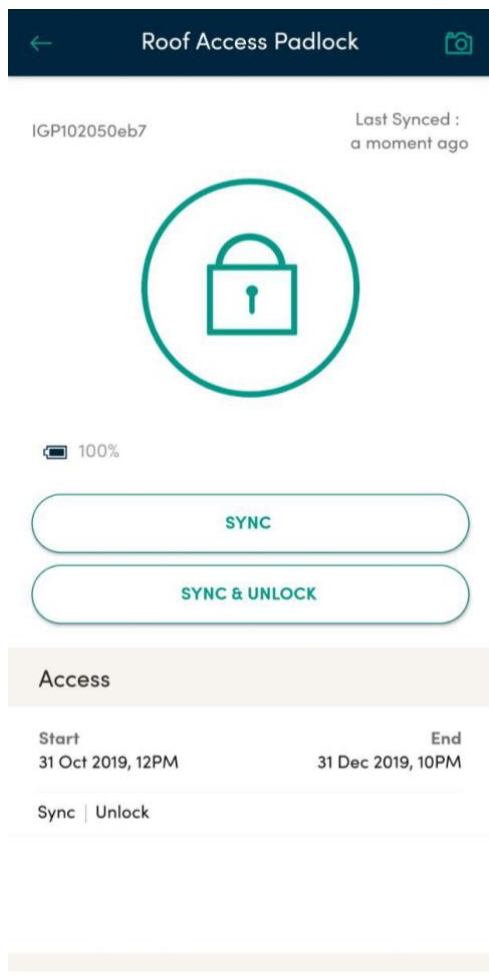
For the owner and admin, they will be able to Bluetooth Unlock and Sync all locks by default. For managers, they will be able to do the same for locks in their department. For lock users, access needs to be added to them first.

1. Login to the app
2. Select the lock



3. Click on the Unlock button (if Bluetooth Unlock access was granted) within 1-2m of the lock. If access was granted by a manager, it will have a start and end date





12. Unlock with 2FA access

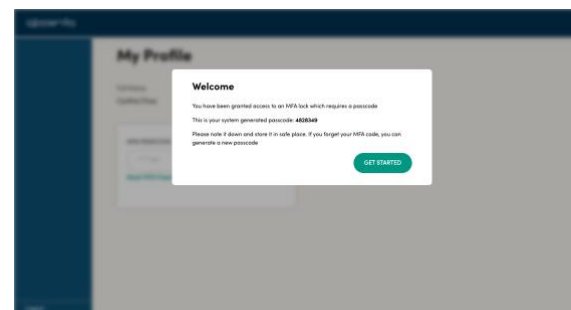
To use 2FA access, the user needs to get an 2FA passcode. This only needs to be done once, and the user can use the same 2FA passcode as the first authentication factor.

With an 2FA passcode and access, the user can unlock by first entering the 2FA passcode on the lock, followed by the unlock icon, and entering the OTP that is sent to them.

12A. Generate 2FA passcode

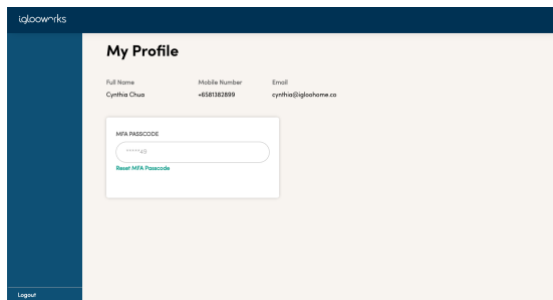
1. Login to the dashboard


2. If it's your first time accessing the My Profile page, a popup will appear with a system-generated 2FA passcode. Take note of this passcode and store it in a safe place.



12B. Reset 2FA passcode

1. Login to the dashboard
2. The passcode can be reset by clicking on 'Reset 2FA Passcode'

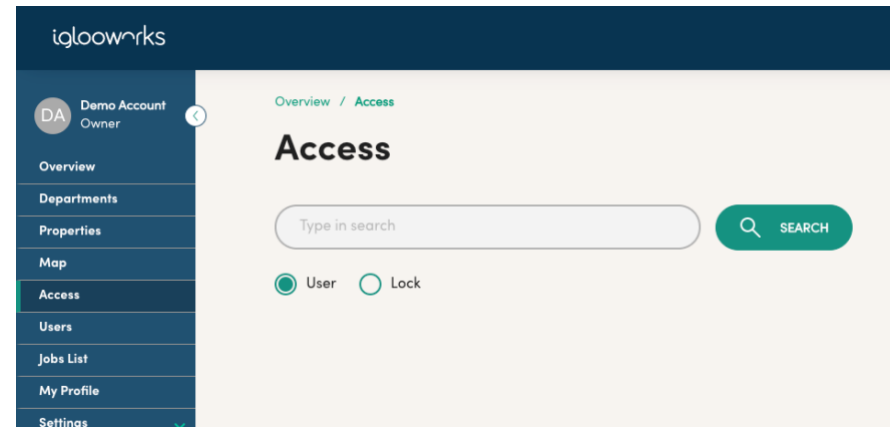


 Tip: My Profile page can only be accessed after the phone number has been added and verified.

13. Search Feature

Search is available for the Owner and Admins to easily find users or locks.

1. Click on [Access] in the menu
2. Select [User] or [Lock]
3. Enter your search query
4. Click the [🔍 Search] button



Flat Organisation

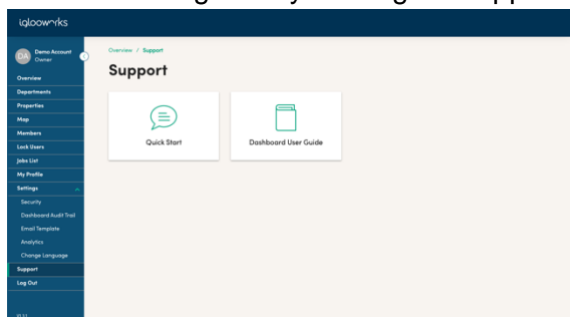
The flat organization structure can be enabled when your account is setup by your igloocompany business development partner. Once enabled, this setting cannot be changed without creating a new account.

Once opted in, departments will be hidden from the iglooworks menu, all locks and employees will be under the organisation without any segregation of departments.

For the PINs access and RFID access previously generated, you can monitor usage by tagging users on editing individual access by adding new users or on multiple access generation page.

Help and Support

View the user guide by clicking on Support



Change password

1. Visit <https://dashboard.iglooworks.co/forgot-password>
2. Key in your organisation ID and email
3. An email will be sent with a link to create a new password

User types and permissions chart

Dashboard

Permissions	Owner	Admin	Manager	Lock User	Mobile responsive
Login/logout	Yes	Yes	Yes	Yes (For 2FA access)	Yes
Generate and reset 2FA passcode	Yes	Yes	Yes	Yes	No
View/add/deactivate lock user	Yes	Yes	Yes	No	Yes
View properties in assigned department	Yes	Yes	Yes	No	Yes
View lock details	Yes	Yes	Yes	No	Yes
Edit Activity log/ Heartbeat Intervals	Yes	Yes	No	No	Yes
Create/edit/delete access	Yes	Yes	Yes	No	Yes
View lock access	Yes	Yes	Yes	No	Yes
View activity logs	Yes	Yes	Yes	No	Yes
Change departments	Yes	Yes	Yes	No	Yes
Create/delete/view jobs	Yes	Yes	Yes	No	Yes
View map	Yes	Yes	Yes	No	Yes
View/add/deactivate manager	Yes	Yes	No	No	Yes
View all properties in organisation	Yes	Yes	No	No	Yes
Add/edit/delete property	Yes	Yes	No	No	No
View department list	Yes	Yes	No	No	Yes

Add/edit/deactivate department	Yes	Yes	No	No	No
Edit lock name	Yes	Yes	No	No	No
View audit trail	Yes	Yes	No	No	Yes
Export audit trail	Yes	Yes	No	No	No
View Master PIN	Yes	No	No	No	Yes
View/add/deactivate admin	Yes	No	No	No	Yes

App

Permissions	Owner	Admin	Manager	Lock User
Login/logout	Yes	Yes	Yes	Yes
BT Unlock	Yes	Yes	Yes	Yes
BT Sync	Yes	Yes	Yes	Yes
Search lock by QR code	Yes	Yes	Yes	Yes
Search lock by BT scan	Yes	Yes	Yes	Yes
Push jobs	Yes	Yes	Yes	No
Perform DFU	Yes	Yes	No	Yes (if granted DFU rights)
Pair lock	Yes	Yes	No	No
Delete lock	Yes	Yes	No	No
Set lock settings	Yes	Yes	No	No
Change Master PIN	Yes	No	No	No
RFID Access	Yes	Yes	No	No