

STATION AND PORTAL INSTRUCTIONS

www.pclocs.com.au | www.lockncharge.com

Cloud Portal – Instructions

CONTENTS

CONTENTS	2
SETUP	4
SAFETY INSTRUCTIONS	4
PHYSICAL INSTALLATION	4
CLOUD ACCOUNT SETUP	5
FIREWALL AND PROXY WHITELISTING	7
RETRIEVE LOCAL HOST ADDRESS	7
ONBOARD STATION/TOWER TO YOUR ACCOUNT	7
ADD ONBOARDED STATIONS TO YOUR ACCOUNT DASHBOARD	8
ACCOUNT	10
SETTINGS	10
TWO-FACTOR AUTHENTICATION SETUP (2FA)	11
RFID FORMAT	11
OWNERS AND ADMINS	11
STATION ADMINS	12
ROLES	12
STATION ADMINISTRATION FROM THE STATION DISPLAY	13
ADMIN MENU OPTIONS	13
BUILT-IN USER DIRECTORY	14
USING RFID	14
ADDING USERS IN BULK	14
REPLACING USERS IN BULK	15
UPDATING USERS IN BULK	15
ADDING USERS ONE-BY-ONE	15
USER GROUPS FOR THE BUILT-IN USER DIRECTORY	16
CREATING USERS' GROUPS	16
ADDING USERS TO USER GROUPS IN BULK VIA CSV	16

Cloud Portal – Instructions

ADDING/REMOVING USERS TO/FROM USER GROUPS VIA THE PORTAL	17
OVERVIEW TAB	17
DASHBOARD / CONNECTED STATIONS	17
ACCOUNT OVERVIEW	17
NODE OVERVIEW.....	18
STATION/TOWER OVERVIEW	18
BAY OVERVIEW	18
USERS TAB	19
ACCOUNT USERS	19
GROUP USERS.....	20
STATION/TOWER USERS.....	20
BAY USERS	20
SETTINGS TAB.....	21
ACCOUNT SETTINGS TAB	21
NODE SETTINGS TAB	22
STATION SETTINGS	22
PUBLIC VS MANAGED MODES.....	24
SETUP CHECK-IN/CHECK OUT WORKFLOW.....	25
SETUP BREAK-FIX WORKFLOW.....	26
LIMIT USER RESERVATIONS FEATURE	28
CURFEW FEATURE	28
EVENT LOGS	30
INTEGRATIONS	30
APP CLIENT	31
WEBHOOKS.....	31
EXTERNAL USERS (ACTIVE DIRECTORY INTEGRATION)	31
SINGLE SIGN-ON (SSO)	31

Cloud Portal – Instructions

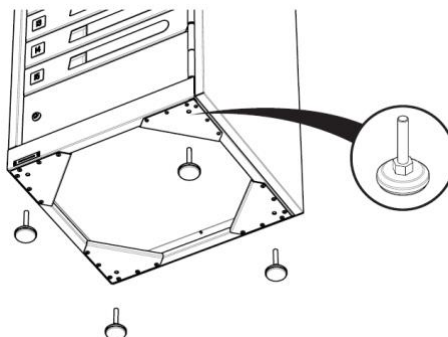
SETUP

SAFETY INSTRUCTIONS

- For your safety – Do not operate the unit if the plug, power socket or power cable is damaged.
- To reduce the risk of fire, electrical shock and/or injury, the following basic precautions should be followed:
- This device (station) is not intended for use by persons (including children) with reduced physical, sensory, and mental capabilities, or lack of experience and knowledge, unless they have been given supervision or instructions concerning the use of the device by a person responsible for their safety.
- CAUTION: To reduce the Risk of Electric Shock – use only indoors.
- Keep away from all sources of water or moisture. Never expose the devices to the rain or dangerous gas.
- Parts of the unit, including devices charging within the unit, may be warm during operation. Install the unit in a dry and cool place and do not cover ventilation holes. Always ensure sufficient ventilation.
- Do not overload the socket-outlets.
- Before using the product, check and make sure all devices are correctly and properly connected.
- Arrange the power cord away from traffic areas where it will not be tripped over.
- The unit is powered when the main supply is connected and switched on.
- Do not try to repair, disassemble, or modify the unit. There are no user-serviceable parts inside.
- Do not use the product other than for its intended use.

PHYSICAL INSTALLATION

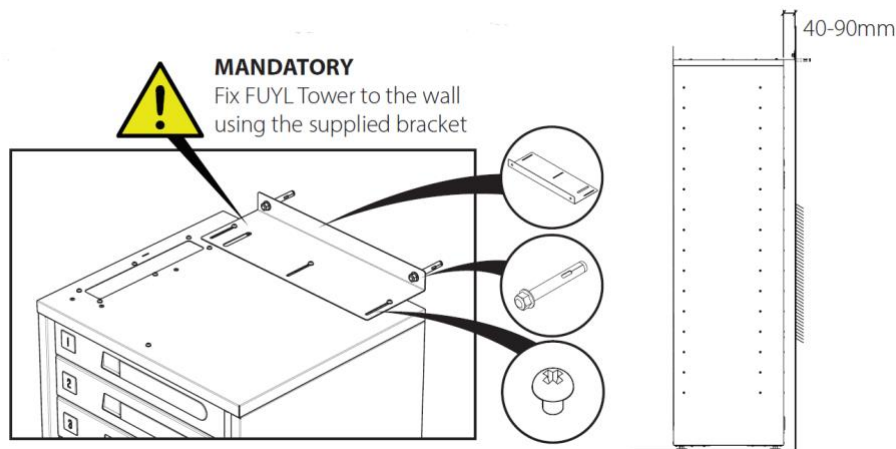
1. CAUTION: The FUYL Tower 15 is heavy (88Kg or 194lbs). The FUYL Tower 5 is 35kg or 77lbs. Take appropriate lifting precautions while moving.
2. With the delivery carton lying horizontal on the FUYL Tower 15 (FUYL Tower 5 is packaged on its back), unpack the carton and free the FUYL Tower from the packaging.
3. Remove the parts box and any additional packaging that is present.
4. The FUYL Tower 15 has four adjustable feet. Locate them in one of the parts boxes and screw them into the corner brackets at the base of the cabinet. FUYL Tower 5 has its feet pre-installed.



5. Manoeuvre the FUYL Tower into an upright position by raising it out of the carton. Use lifting apparatus if necessary for safe lifting. Please discard the packaging with thought for the environment.

Cloud Portal – Instructions

6. When choosing a location for the FUYL Tower, consider the following:
 - a. The LCD display will be more readable when ambient light levels are lower.
 - b. Direct sunlight should be avoided in hot climates, as temperatures within the unit could exceed operating temperatures of stored devices.
 - c. Choosing public, well trafficked areas will contribute to the safety of users and reduce the likelihood of successful break-in.
 - d. The main power lead for the FUYL Tower should be connected in a location that is concealed, to avoid accidental or deliberate power down of the unit while devices are charging.
7. The FUYL Tower will require either a single mains socket or a permanent electrical junction box, preferably directly behind or above the Tower. Any necessary electrical installation should be done by suitably qualified installers before the cabinet is moved into place.
8. If network connectivity will be required, then a LAN port or cable must be provided in an appropriate location close to the cabinet. A suitable LAN cable can then be plugged into the ethernet connector on the rear of the cabinet.
9. The mains supply cable should be fitted to the cabinet before it is moved into the final position. Plug the cable into the mains socket on the rear of the cabinet.
10. Position the FUYL Tower 15 into installation location, 40-90mm from the wall, and level/stabilise the Tower by adjusting the feet at the base. Fix to the wall using the supplied mounting bracket on top of the unit. Fixing to the wall is important for stability of the unit and safe operation.

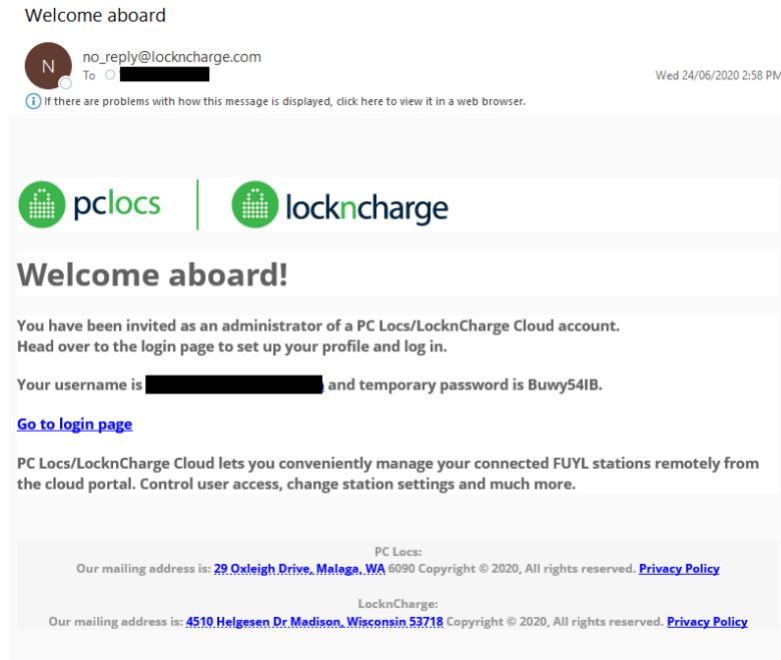


CLOUD ACCOUNT SETUP

Once you have decided on a plan and have purchased, two emails will be sent to the person designated to be the Account Owner. One email will contain the temporary login details for accessing your Cloud Account, and the other will contain your Account Code that is used for onboarding stations to your Account. If you have not received these emails, please check your junk mailbox.

Cloud Portal – Instructions

Example email: temporary login credentials



Example email: Account details including the Account Code



Your subscription is active

Hey John,

Congratulations on your new PC Locs Cloud subscription. Once your product(s) arrive you can onboard 1 of them into your Cloud Account.

To start onboarding your products go to pclocs.io and sign in.

For your convenience we've included some of your details below:

Cloud Account Code: XXXXX
Subscription Plan: Cloud Manager
Subscription Plan Quantity: 10
Next Renew on: 28-Feb-2021

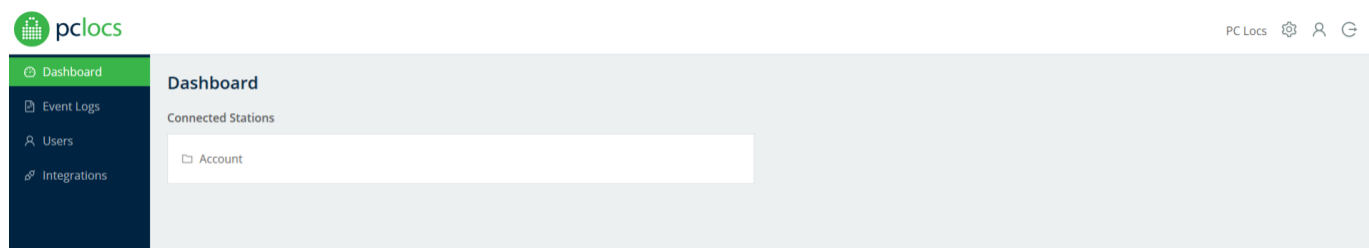
Regards,

PC Locs

We're here to make your life easier. If at any point you need assistance or would like to give us feedback, feel free to reach out to us [here](#). We'd love to hear from you. Our mailing address is: 29 Oxleigh Drive, Malaga, WA 6090 Copyright © 2020, All rights reserved. [Privacy Policy](#)

Login to your Cloud account using your email and temporary password. Please note, the system will force you to update your password on initial login.

- If you are in Australia or New Zealand, go to www.pclocs.io.
- If you are in the US, UK, Europe or elsewhere, go to www.lockncharge.io



At this point, you have the option to:

- Prefill some of the settings available to you from the Settings page in preparation for onboarding your stations. See SETTINGS PAGE section for more details.
- Setup your Admins by clicking the gear icon in the top right corner. See SETUP ADMINIS section for more details.
- Add your users to the cloud directory (must have Cloud Managed tier and above). See USERS PAGE section for more details.
- Prepare your integrations (must have Cloud Integrated tier). See INTEGRATIONS section for more details.

Cloud Portal – Instructions

FIREWALL AND PROXY WHITELISTING

IMPORTANT: Connecting a FUYL Tower to the Cloud Platform requires technical knowledge of your organization's network configuration. Please only proceed if you are experienced with network configuration and have the permission of your network administrator.

When onboarding a FUYL Tower, it will attempt to create an outgoing network connection to contact the Cloud Platform. These addresses may need to be whitelisted if your firewall restricts outgoing connections to unknown addresses.

Address	Port	Protocol
pclocs-firmware-updates-869893548898.s3.us-west-2.amazonaws.com	TCP 443	https
registry.pclocs.io	TCP 443	https
a136cfw17adibc-ats.iot.us-west-2.amazonaws.com a136cfw17adibc-ats.iot.us-east-2.amazonaws.com a136cfw17adibc-ats.iot.eu-west-2.amazonaws.com a136cfw17adibc-ats.iot.ap-southeast-2.amazonaws.com	TCP 8883	mqtt
time1.google.com, time2.google.com, time3.google.com, time4.google.com	UDP 123	ntp

The addresses in the table above may not be up to date. Please visit our [Networking Guide page](#) for the latest information.

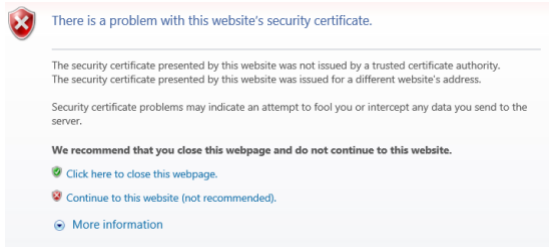
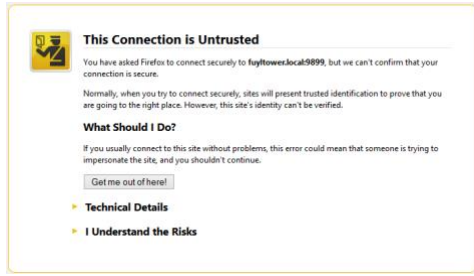
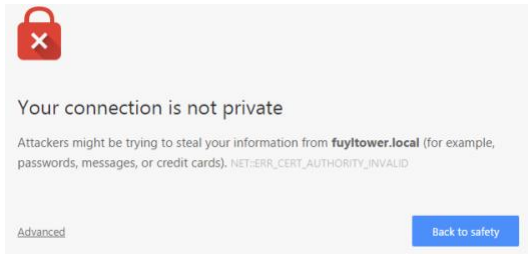
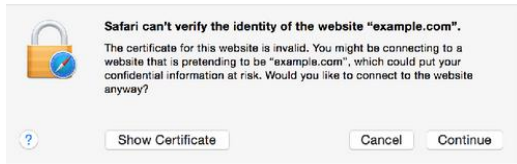
RETRIEVE LOCAL HOST ADDRESS

1. Connect the FUYL Tower to your laptop or to an ethernet wall socket, with the supplied ethernet cable.
NOTE: If you are connecting to a Laptop, the FUYL Tower should be restarted before retrieving the portal address.
2. Enter the administration menu on the Station display by pressing “00” on the keypad and then “OK”.
3. Enter the default PIN: 31082018
4. Select option 2 (System Status), then option 1 (Network Status), and record the ‘Portal’ address.

ONBOARD STATION/TOWER TO YOUR ACCOUNT

Open a web browser and type the Portal address as recorded in step 4. NOTE: Some browsers will report security warnings. The security warnings appear because the station has generated a self-signed certificate to secure your connection. It should be safe to bypass the following browser security warnings in this situation because it is a temporary connection to the local host on the station.

Cloud Portal – Instructions

<p>Internet Explorer</p> 	<p>Mozilla Firefox</p> 
<p>Google Chrome</p> 	<p>Apple Safari</p> 

NOTE: The Google Chrome browser may not let you continue. In this case you will need to type in 'thisisunsafe'

Enter the default login credentials.

Username: **admin**

Password: **31082018**

Follow the onboarding wizard to connect your Tower to your Cloud Account. In addition to the networking requirements highlighted in the ONBOARDING STATIONS TO YOUR CLOUD ACCOUNT section, you will also need to have your **Account Code** available which would have been emailed to you on sign up.

TIP: adding a friendly name is particularly important when you are adding multiple products to your Cloud Account. This will help know which product you are administering. If you do not add it at this point, you can update its 'name' from the Cloud portal.

ADD ONBOARDED STATIONS TO YOUR ACCOUNT DASHBOARD

Login to your Cloud account using your Cloud credentials. If you are in Australia or New Zealand, go to www.pclocs.io. If you are in the US, UK, Europe or elsewhere, go to www.lockncharge.io

1. Username: email that was used to sign up to PC Locs/LocknCharge Cloud
Password: temporary password sent via email

NOTE: the system will ask you to change your password before you can proceed.

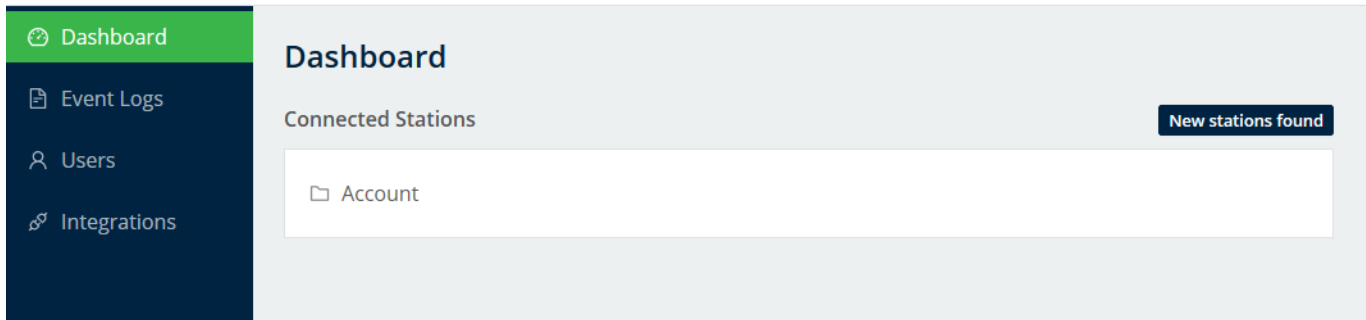


Log in

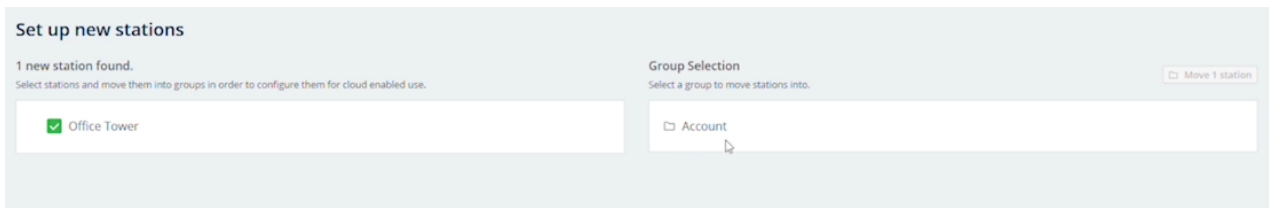
[I forgot my password.](#)

Cloud Portal – Instructions

- Click on the 'New stations found' button to bring Stations into the account and to begin

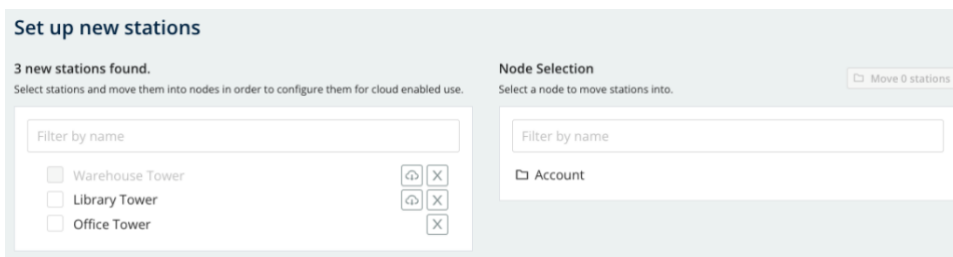


- Click on the check box of the station(s) and select the node in which to add it to.



The Station(s) will begin to adopt the settings and configurations set on this node. E.g., Users, network settings etc.

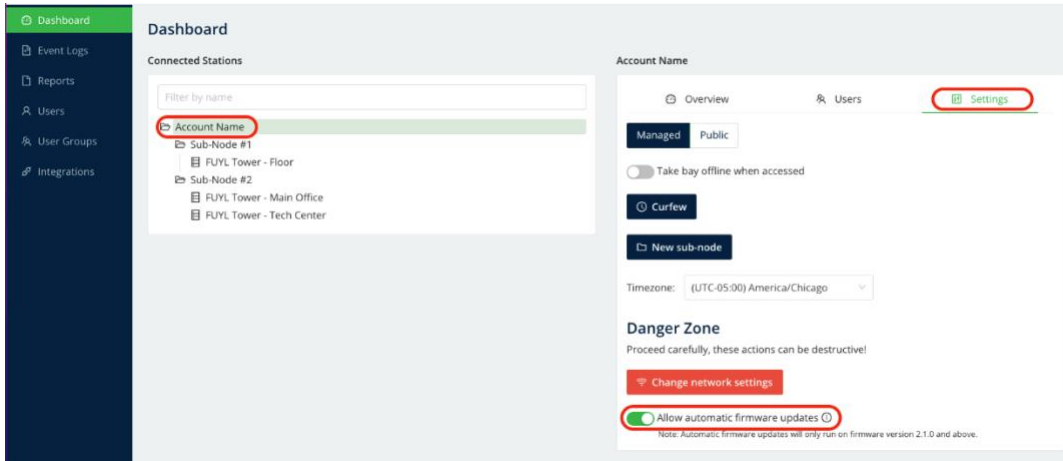
- If the station is on an older version of firmware than 2.3.0, the checkbox to onboard will be disabled, and an icon will be displayed to indicate that a firmware update is available. To bring the station into the account, you must click this icon to update the firmware. Once the firmware has been updated, the checkbox will be enabled, and station can be onboarded into the account.



If the station is on firmware 2.3.0, but a newer version of firmware is available, the station can be onboarded without a firmware update. However, it is recommended that firmware be updated to the latest version as soon as possible after onboarding to ensure the best user experience.

Cloud Portal – Instructions

TIP: Turn on auto-updates in the account settings page. Firmware updates will apply automatically between 00:00 and 01:00 local time.

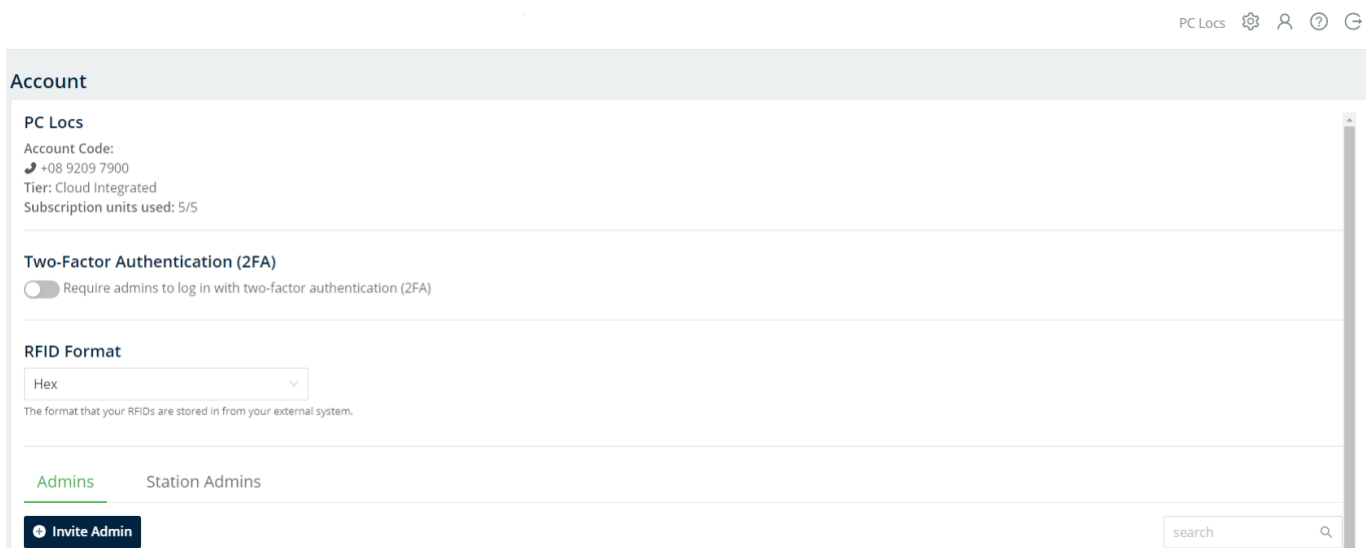


If the station is on the latest firmware, an update icon will not display, and the station can be onboarded.

NOTE: Up to 10 stations can be onboarded at once.

ACCOUNT

Clicking the gear icon in the top right corner takes you to the section of the portal that summarises your account; what your Account Code is, your subscription tier and how many units of your subscription that have been onboarded and are in action.



SETTINGS

The settings tab includes configuration options for Two-Factor Authentication (2FA) and RFID Format for external systems. Note, Only Owner administrators have access to Settings.

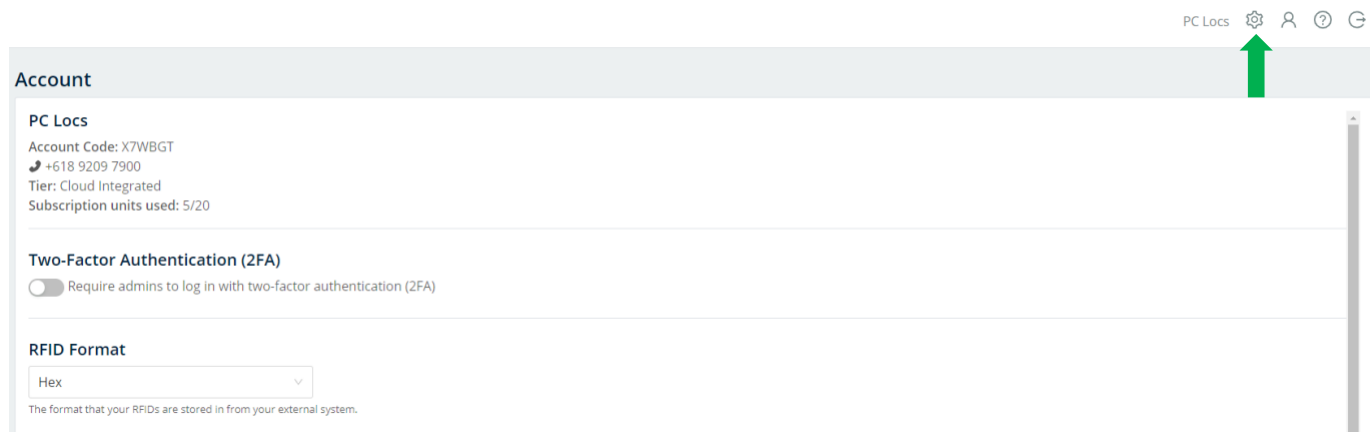
Cloud Portal – Instructions

TWO-FACTOR AUTHENTICATION SETUP (2FA)

Two-Factor Authentication (2FA) can be used to help protect your account from unauthorized access by requiring admins to enter an additional code to login to the portal. The 2FA feature currently supports the use of an authenticator app authentication method.

Owner level administrators can enforce 2FA is used on their account for logging into the portal. The second factor of authentication is done via an authenticator app.

To toggle 2FA 'on', go to the account preferences page (gear icon, top right).



The next time the admin logs in, it will ask them to setup 2FA, and then every other login, the portal will ask them to authenticate themselves.

Alternatively, admins can enable 2FA for themselves even if the toggle is not turned 'on'. To do this, go to the admins profile page (person icon, top right).

RFID FORMAT

The format that your RFIDs are stored in from your external system. Note: this is only applicable if you are integrating your external user directory to the Cloud platform (minimal tier is Cloud Integrated).

[Click here for a full list of compatible RFID formats.](#)

OWNERS AND ADMINS

There are now 3 Administrator types – Owner, Admin and Station Admin

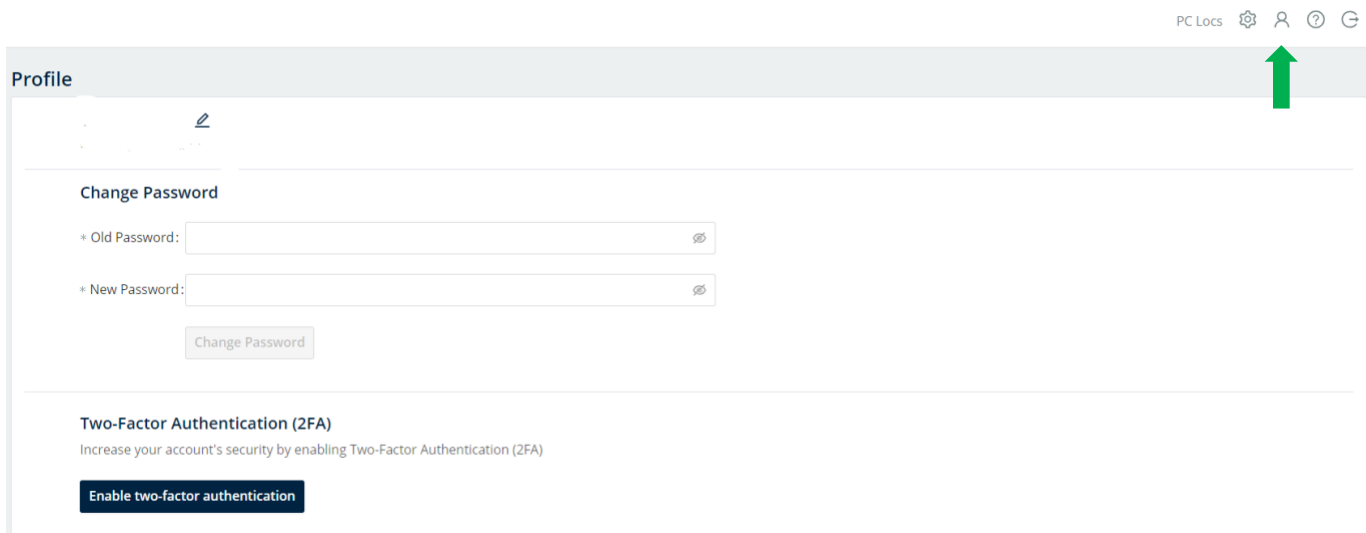
- The 'Owner' has complete administration control of the Portal and Station. The Owner profile can:
 - Invite as many users as they like, including other Owners, as well as creating Station Admins. There must be at least one Owner on every account.
 - Create custom roles
- 'Admins' can do everything that an Owner can do except:
 - Invite and delete 'Owners' and 'Admins'
 - Create and delete 'Station Admins'
 - View other 'Owner,' 'Admins' and 'Station Admin'

Cloud Portal – Instructions

- Create custom roles
- ‘Station Admins’ can only perform administration functions that are available to them on the LCD menu. Refer to the ‘STATION ADMINISTRATION FROM THE STATION DISPLAY’ section for details on what these functions are. Station Admins do not get a login for the Cloud portal.

To invite an Admin (Owner functionality only), press the ‘invite admin’ button which will open a modal

- Email address will be the login username
- Role: Owner, Admin or any other custom role that has been created
- Enable station access to give this administrator access via the Stations display as well as remote access via the portal.
- RFID: add to enable the administrator to access the administration menu from the Stations display.
- PIN: this is a unique autogenerated number that is used to access the administration menu from the Stations display.
- The person invited will get an email with a temporary password. Be sure to also check the junk mailbox.
- After successfully logging in with the temporary password, the system will prompt them to update create a new password.



PC Locs [Settings] [User] [Help] [Green Arrow]

Profile

Change Password

* Old Password:

* New Password:

Two-Factor Authentication (2FA)

Increase your account's security by enabling Two-Factor Authentication (2FA)

STATION ADMINS

Station Admins are created rather than invited. This role only gives administration access via the stations display.

To create a station admin, press the ‘add station admin’ and add in their details.

ROLES

Owner administrators can limit the permissions of non-Owner administrators to specific nodes.

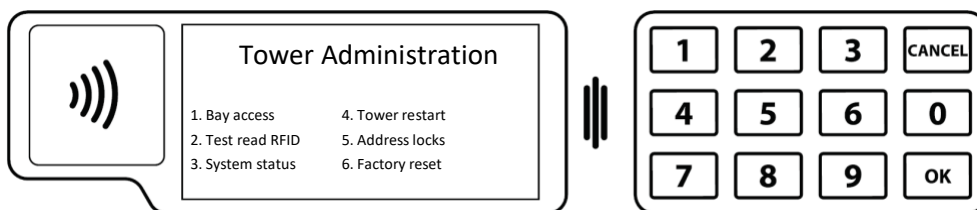
Cloud Portal – Instructions

STATION ADMINISTRATION FROM THE STATION DISPLAY

To access the station from its display, press '00' on the keypad and enter your PIN or tap your RFID, depending on how the admin has been setup.

NOTE: If a Cloud subscription has not been purchased, the station can be administered using the default administrator PIN which is 31082018. We recommend customers change this PIN. This can be done via the LCD screen for non-Cloud subscription customers.

ADMIN MENU OPTIONS



- Bay Access
 - Unlock bay
 - Clear bay
 - Toggle offline
 - Unlock all bays
- Test Read RFID
 - Some RFID scanners read the RFID in diverse ways. To ensure that the number you enter matches the number read by the station, you can perform a test read at the station. To do this, log into the Admin menu on the station display, select 'test read RFID' and then scan an RFID card. The RFID will be shown on the screen and will also be logged to the event log, which can be accessed through the 'Event Log' section of the Cloud Portal. Now that you know the number and the format of how our system reads the RFID, you can adjust your RFID numbers accordingly when you import users, or when you are adding them into the portal one-by-one.
- System status
 - Network status
 - Network config
 - System clock
 - Software version
- Tower restart
- Address locks
- Factory reset
- Admin Credential (only available for non-Cloud subscription customers)

This option is used to change admin credentials

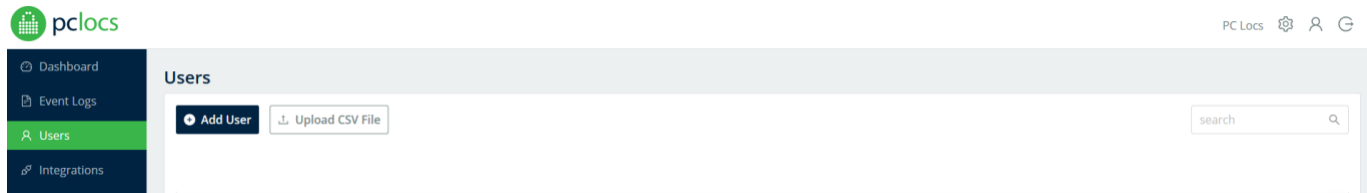
 - Admin access PIN
 - Admin access RFID

Cloud Portal – Instructions

BUILT-IN USER DIRECTORY

This feature allows admins to control who is allowed access to Stations. Please note: to control access, Users can be added, edited, and deleted in the systems user directory.

To access this section, click on the 'Users' link from the menu in the left column.



To integrate to your own directory, go the EXTERNAL USERS section of this document or [click here for more details](#).

USING RFID

FUYL Tower supports a wide range of RFID formats. [For a complete list, click here](#).

Some RFID scanners read the RFID in diverse ways. To ensure that the number you enter matches the number read by the station, you can perform a test read at the station. To do this, log into the admin menu on the station display, select 'test read RFID' and then scan an RFID card. The RFID will be shown on the screen and will also be logged to the event log, which can be accessed through the 'Event Log' section of the Cloud Portal. Now that you know the number and the format of how our system reads the RFID, you can adjust your RFID numbers accordingly when you import users via, or when you are adding them into the portal one-by-one.



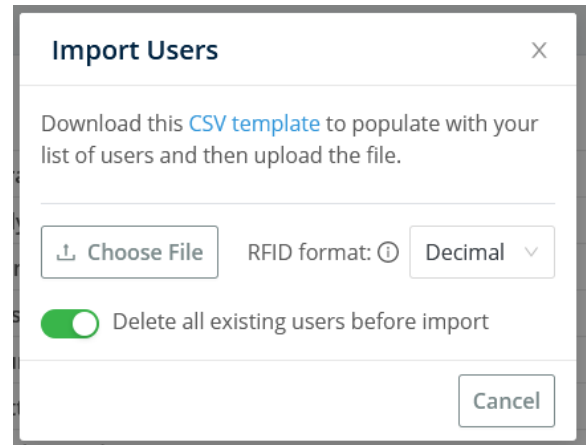
ADDING USERS IN BULK

- Click 'Bulk actions' and from the dropdown, select 'Import users'
- Download the CSV template to populate with your list of users
 - Name*
 - Email
 - PIN**
 - RFID**

Cloud Portal – Instructions

- External Ref ID
- Tags
- User Groups
- *required ** must include one of these options*
- Upload the file

The user directory is now populated with users that you can now grant permission to access station. You can grant users access to; nodes, specific stations, or specific bays. Please see the GRANTING STATION ACCESS TO USERS section for more details on how to do this.



Import Users [X]

Download this [CSV template](#) to populate with your list of users and then upload the file.

RFID format:

☒ Delete all existing users before import

REPLACING USERS IN BULK

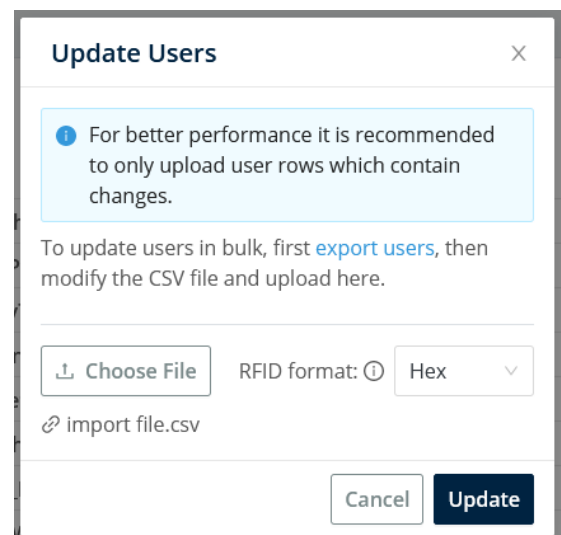
Admins can replace users in their User Directory with a new or updated list of users.

- Click 'Bulk actions' and from the dropdown, select 'Import users'
- Toggle ON 'Delete all existing users before import' before you confirm the import

UPDATING USERS IN BULK

TIP: Use the filter to narrow down the users you want to update.
 Once you are happy with the filtered results:

- Click 'Bulk actions' and from the dropdown, select 'Export users' to get a list of users (CSV) you want to update.
- Open the file up in a preferred editor, e.g., Excel, and update the users. Once you have made your updates, save the file.
- Click 'Bulk actions' (in the Users page in the portal) and from the dropdown, select 'Update users'
- Choose the file and press update.



Update Users [X]

For better performance it is recommended to only upload user rows which contain changes.

To update users in bulk, first [export users](#), then modify the CSV file and upload here.

RFID format:

[import file.csv](#)

ADDING USERS ONE-BY-ONE

- Click the 'Add User' button
- Fill in the required fields – First name, Last name, and Email
- Add RFID or PIN or both. This is what they will use to reserve a bay.
- Add tags and ExternalRef (optional) and press 'save'

With the systems user directory populated, you can now set who is allowed access to which stations and bays. Go to the USERS PAGES section for details.

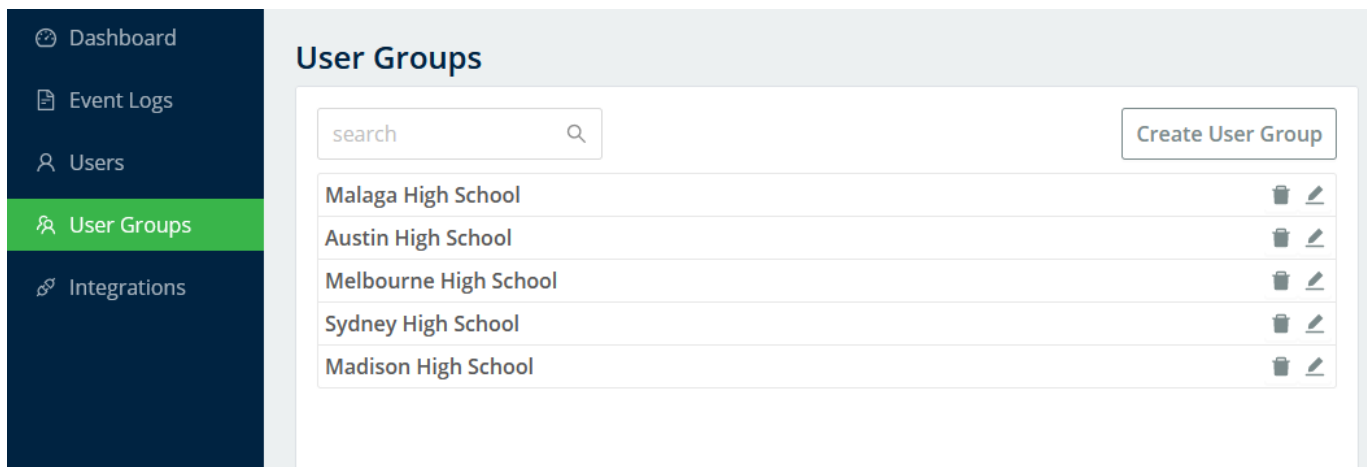
Cloud Portal – Instructions

USER GROUPS FOR THE BUILT-IN USER DIRECTORY

This feature allows admins to create and use 'User Groups' to organise and manage user's bay/station/node access authorisation.

CREATING USERS' GROUPS

- Go to User Groups page from the left side menu
- Press the 'Create User Group' button, name the group(s), and save
- Once you have created your group(s), you can now add users to the groups
 - This can be done directly from the portal, or
 - This can be done via a CSV import



ADDING USERS TO USER GROUPS IN BULK VIA CSV

- NOTE: to import users into user groups, the group must already be existing in the portal.
- Click the 'upload CSV file' button
- Download the CSV template to populate with your list of users
 - Name*
 - Email
 - PIN**
 - RFID**
 - External Ref ID
 - Tags
 - User Groups

NOTE: the group name must be an exact match with the group name in the portal.

**required ** must include one of these options*

- Upload the file
- NOTE: if you have made a mistake, you can bulk delete all and upload a new file through the import process. See the [REPLACING USERS IN BULK](#) section.

Cloud Portal – Instructions

The user directory is now populated with users that you can now grant permission to access station. You can grant users access to; nodes, specific stations, or specific bays. Please see the GRANTING STATION ACCESS TO USERS section for more details on how to do this.

ADDING/REMOVING USERS TO/FROM USER GROUPS VIA THE PORTAL

- In the User groups page, click on the group you want to add users to
- Click add or remove buttons
- Use the filters to find who you want to add/remove
- Select who you want to add/remove by clicking on the name or the 'select all filtered button
- Confirm your action (adding or removal)

OVERVIEW TAB

DASHBOARD / CONNECTED STATIONS

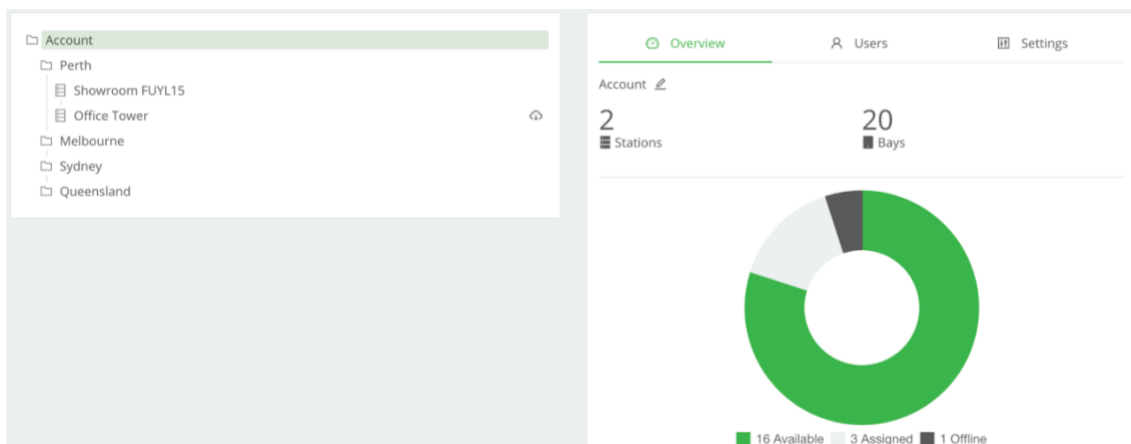
The Dashboard displays the stations you have connected to your account and how you have organised them. It will also display some useful alerts if a firmware update is available for a station and if things are not as they should be. E.g., breached bays or stuck bays.

ACCOUNT OVERVIEW

The Overview tab displays a snapshot of all the Stations in the account. It summarises; how many Stations in the Account, how many bays in total, and what state each bay is in (Available, Assigned or Offline).

Note: the bay state colours reflect the LED colours on the hardware:

- Green = bay LED is green, the door is closed, and the bay available for a user to select for reservation
- White = bay LED is white, the door is closed, and the bay is currently reserved and assigned to a user
- Red = bay LED is red, the door is open
- Dark grey = bay LED is off, the door could be open or closed, and the bay has been taken offline by an admin so that it cannot be reserved or accessed by a user.

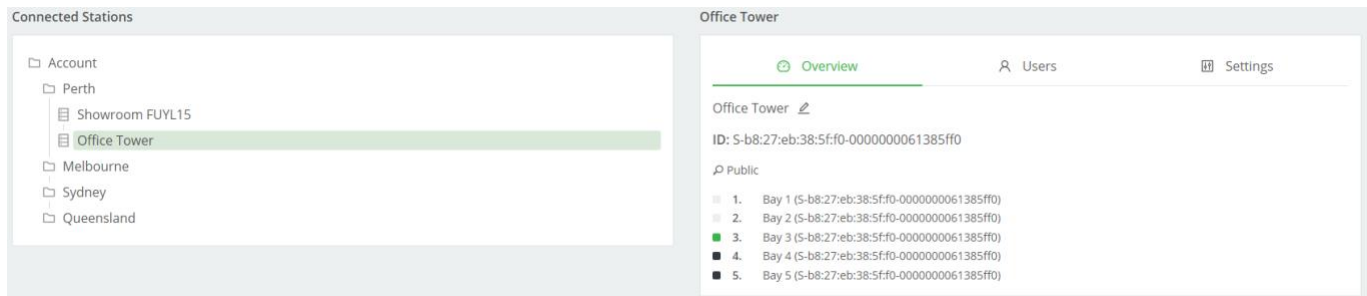


Cloud Portal – Instructions

NODE OVERVIEW

The Overview tab displays a snapshot of all the Stations in the node selected, namely; how many Stations in the node, how many bays in the node, and what state each bay is in (Available, Assigned or Offline). Note: the bay state colours reflect the LED colours on the hardware as mentioned in the ACCOUNT OVERVIEW section.

STATION/TOWER OVERVIEW



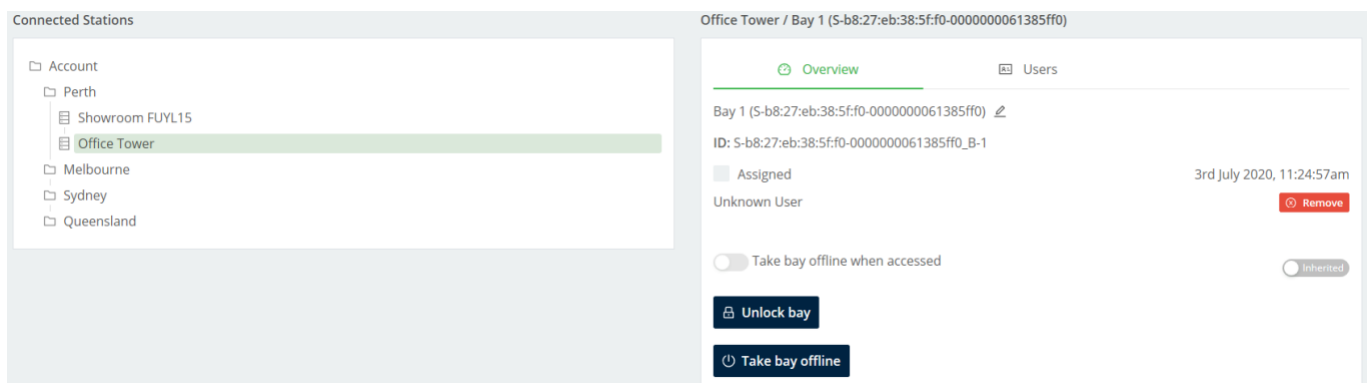
The Overview tab displays:

- How many bays the Station has.
- The state of each bay (Available, Assigned or Offline). Note: the bay state colours reflect the LED colours on the hardware as mentioned in the ACCOUNT OVERVIEW section.
- The stations name and unique ID
- The stations behaviour – Managed or Public.

BAY OVERVIEW

The Overview tab displays:

- The state of the bay (Available, Assigned or Offline).
- The bays name and unique ID
- Whether the bay will turn offline after access (a setting used for break-fix workflow)
- Who has reserved the bay (station must be in 'Managed' mode to display the user)



Cloud Portal – Instructions

It also gives the admin some remote management options such as:

- Remove the bay reservation. This will make the bay available to any user ('Public' mode) or to any user that has been granted access to this bay ('Managed' mode)
- Unlock bay – this will open the bay instantly. Pushing a door close after unlocking will retain the user assignment. This action is used by admins to inspect the contents of a bay. Before performing this action, it is recommended that you are in front of the station or that a colleague is in front of the station.
- Take bay offline – this will prevent any user from accessing the bay, including the assigned user.
- 'Take bay offline when accessed' toggle. This is usually turned on for customers that have configured stations for break-fix workflows.
- Assign temporary credentials (PIN or RFID) directly on a bay (the bay LED colour will turn white). Assigning a PIN or RFID on a bay is a one-time action where the credential automatically clears from the bay after access.

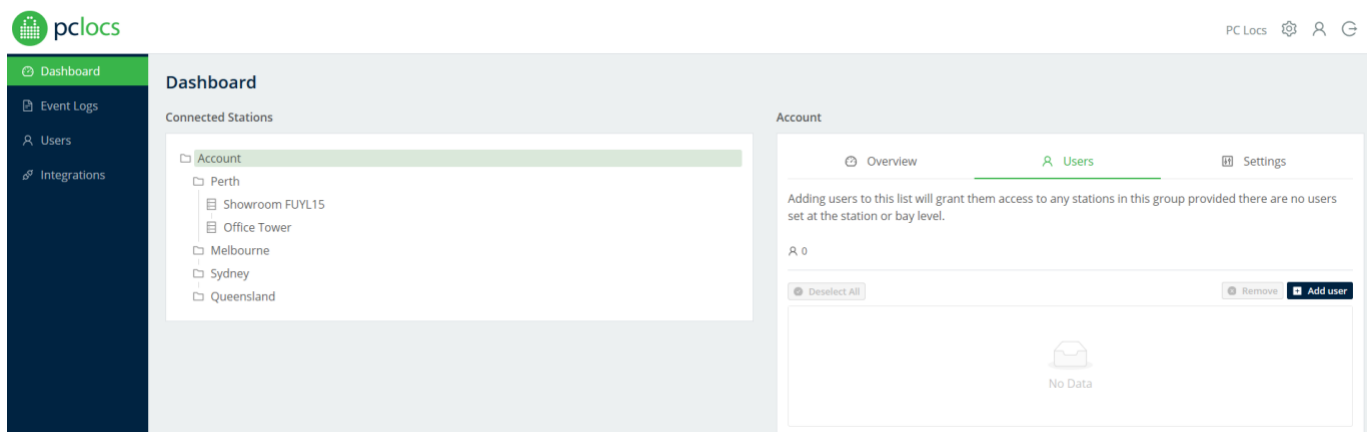
USERS TAB

Before authorising users/user groups to nodes, stations, or bays, you first need to change the stations 'mode' by toggling it to 'Managed' from 'Public,' in the Settings tab.

Note: If this is the intended behaviour for all your stations, this should be done from the Account Settings page. Users authorised from this level will propagate to all stations in your account.

ACCOUNT USERS

Authorising user access from the Account node level will give the users selected authorisation to access every bay of every station in your account.



- Navigate to the Account node
- Click on the 'Users' tab in the right box
- Select one of the two available sub-tabs, users, or user groups, for authorisation.
 - If you want to authorise a few individuals, select 'users'

Cloud Portal – Instructions

- If you want to authorise a group of users, select 'user groups'
- Select the users or user groups that you want to grant access permission and press the 'authorise selected' button. The users/user groups selected are now authorised to access to all the bays on all your stations.

GROUP USERS

Authorising user access to a node (Sub-node of the Account node).

- Navigate to a node
- Click on the 'Users' tab
- Select one of the two available sub-tabs, users, or user groups, for authorisation.
 - If you want to authorise a few individuals, select 'users'
 - If you want to authorise a group of users, select 'user groups'
- Select the users or user groups that you want to grant access permission and press the 'authorise selected' button. The users/user groups selected are now authorised to access to all the bays in this node.

STATION/TOWER USERS

Authorising user access to a specific station.

- Navigate to a station
- Click on the 'Users' tab
- Select one of the two available sub-tabs, users, or user groups, for authorisation.
 - If you want to authorise a few individuals, select 'users'
 - If you want to authorise a group of users, select 'user groups'
- Select the users or user groups that you want to grant access permission and press the 'authorise selected' button. The users/user groups selected are now authorised to access to all the bays on this station.

BAY USERS

Authorising user access to a specific bay.

- Navigate to a bay
- Click on the 'Users' tab
- Select one of the two available sub-tabs, users, or user groups, for authorisation.
 - If you want to authorise a few individuals, select 'users'
 - If you want to authorise a group of users, select 'user groups'
- Select the users or user groups that you want to grant access permission and press the 'authorise selected' button. The users/user groups selected are now authorised to access this specific bay.

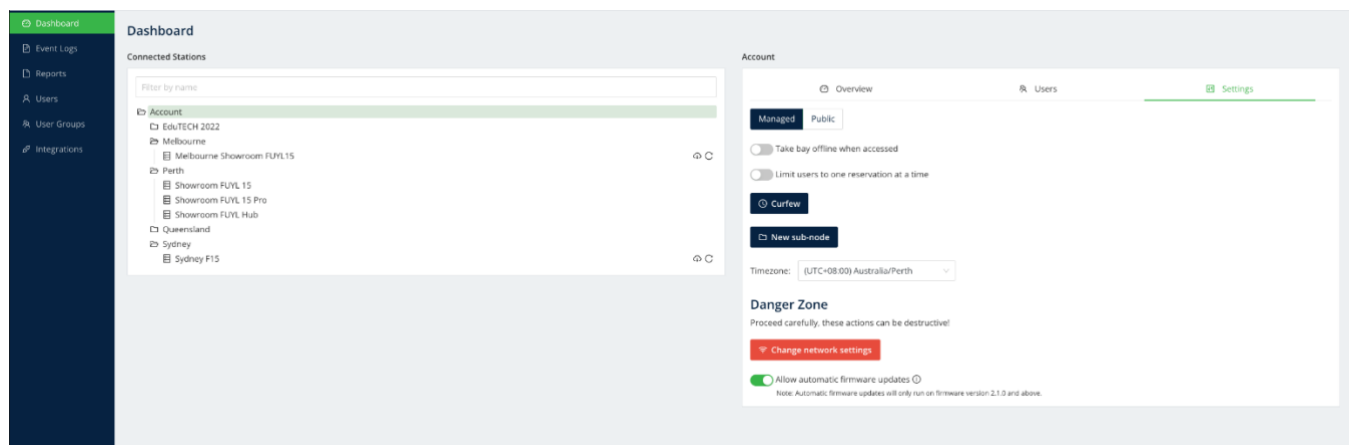
Cloud Portal – Instructions

SETTINGS TAB

The settings tab in the Cloud portal is where you can configure workflow modes, workflow steps, curfew, time zone, resets, network settings and more. Depending on what level you are on (Account, Sub-node or Station, the options available for configuration will differ.

ACCOUNT SETTINGS TAB

Configurations set at the Account level will propagate to all stations that have been onboarded onto an account, including if they are nested in sub-node.



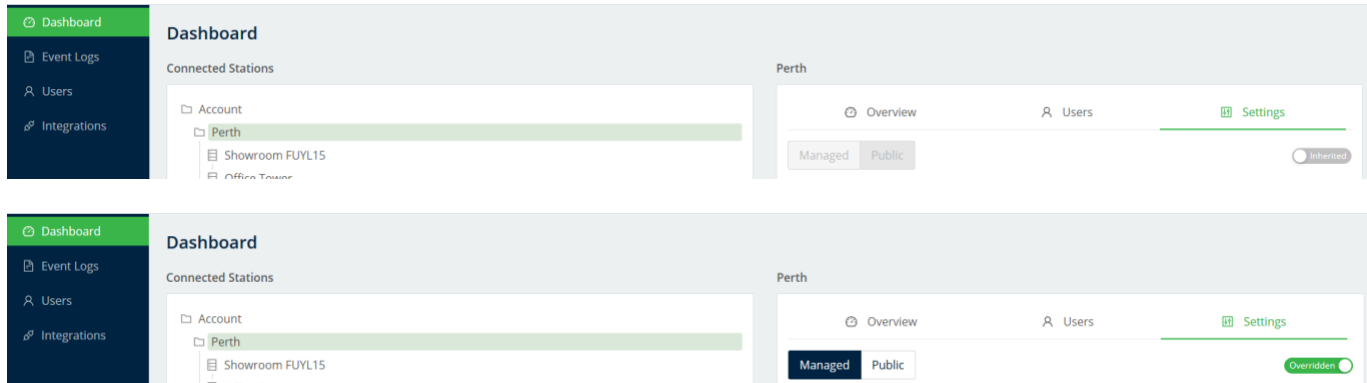
The configuration options available at the Account level include the following.

- Mode of operation switch
 - Public (default). For customers that want their station(s) to operate as a public charging station that anyone can use for secure, on-demand charging.
 - Managed. For customers that want to control which users are allowed access to their station(s). Perfect for Check-in/Check-out and Break-Fix workflows.
- Take bay offline when accessed toggle. Turning this on does as described, it puts that bay offline so that it cannot be accessed or reserved after it is accessed the first time. This is used for customers that want to setup a Break-Fix workflow.
- Limit user reservations toggle. Turning this on limits users to one reservation at a time on any bay in the account. NOTE: This setting is only relevant for stations that are in Managed mode.
- Curfew. Customers can set blocks of time when the stations are inaccessible by users.
- New sub-node. For organising stations into logical groups.
- Time zone.
- Change network settings. This is a 'Danger Zone' setting. Proceed carefully as these actions can be destructive.
- Allow automatic firmware updates. This will be turned off by default allowing the customer to turn it on when appropriate. The default firmware update schedule is set to 00:00 – 01:00 local time of the station.

Cloud Portal – Instructions

NODE SETTINGS TAB

Configurations set at the node level will propagate to all stations that have been onboarded or nested in the node. If you want the node settings to differ from the account's settings, you will need to toggle the specific configurable setting from 'inherited' to 'overridden.' See image below as an example.



The configuration options available at the node level include the following.

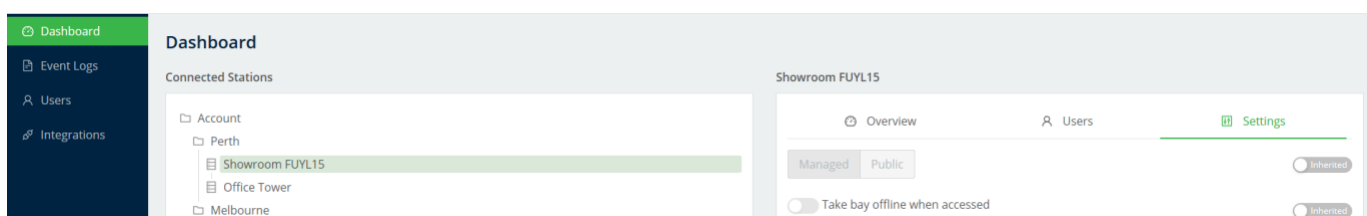
- Mode of operation switch
 - Public (default). For customers that want their station(s) to operate as a public charging station that anyone can use for secure, on-demand charging.
 - Managed. For customers that want to control which users are allowed access to their station(s). Perfect for Check-in/Check-out and Break-Fix workflows.
- Take bay offline when accessed toggle. Turning this on does as described, it puts that bay offline so that it cannot be accessed or reserved after it is accessed the first time. This is used for customers that want to setup a Break-Fix workflow.
- Curfew. Customers can set blocks of time when the stations are inaccessible by users.
- New sub-node. For organising stations into logical groups.
- Time zone.
- Change network settings.

Note: This is a 'Danger Zone' setting. Proceed carefully as these actions can be destructive.
- Delete node.

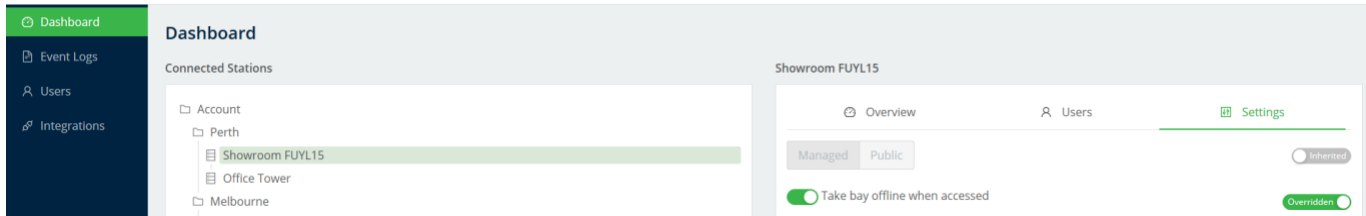
Note: This is a 'Danger Zone' setting. Proceed carefully as these actions can be destructive.

STATION SETTINGS

Configurations set at the Station level will apply to a specific station only. If you want the station settings to differ from the node settings, you will need to toggle the specific configurable setting from 'inherited' to 'overridden.'



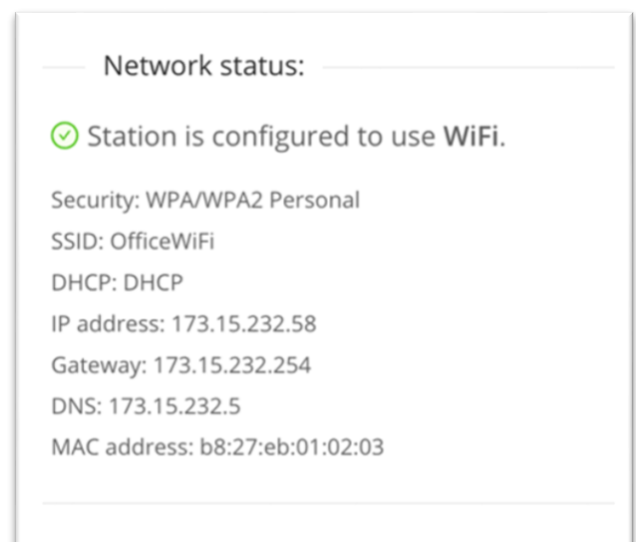
Cloud Portal – Instructions



The configuration options available at the Station level include the following.

- Mode of operation switch
 - Public (default). For customers that want their station(s) to operate as a public charging station that anyone can use for secure, on-demand charging.
 - Managed. For customers that want to control which users are allowed access to their station(s). Perfect for Check-in/Check-out and Break-Fix workflows.
- Take bay offline when accessed toggle. Turning this on does as described, it puts that bay offline so that it cannot be accessed or reserved after it is accessed the first time. This is used for customers that want to setup a Break-Fix workflow.
- Curfew. Customers can set blocks of time when the stations are inaccessible by users.
- Move station. For moving the station from one node to another.
- Restart station.
- Enable station lockdown. For taking an entire station offline so that users cannot access or reserve bays (bay LED's will turn off).
- Change network settings.

Note: This is a 'Danger Zone' setting. Proceed carefully as these actions can be destructive.
- Forget Station. This action will remove the station from the account and restore it back to its factory settings. Note: This is a 'Danger Zone' setting. Proceed carefully as these actions can be destructive.
- Update Firmware. This action will initiate a firmware update on the station. This button will only be displayed if a firmware update is available for this station. An icon will also be displayed in the dashboard organisation view for this station. Note: This is a 'Danger Zone' setting. Proceed carefully as these actions can be destructive.

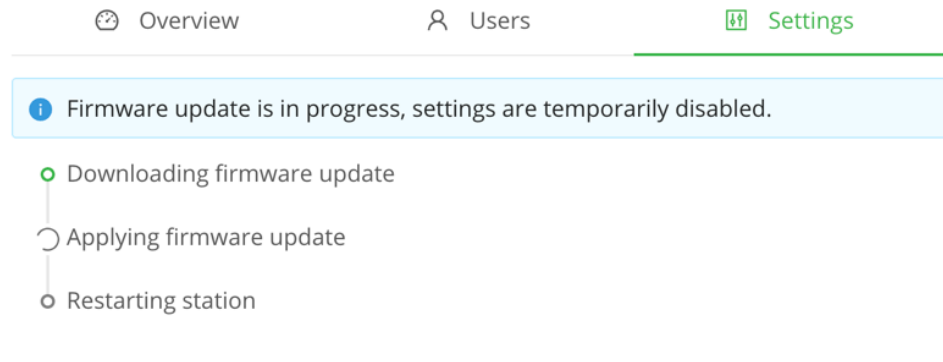


The Station Settings tab also shows some summary information:

- Network Status. This will show the current network settings that this station has configured, it shows information like IP address, MAC address, Wi-Fi SSID and more.

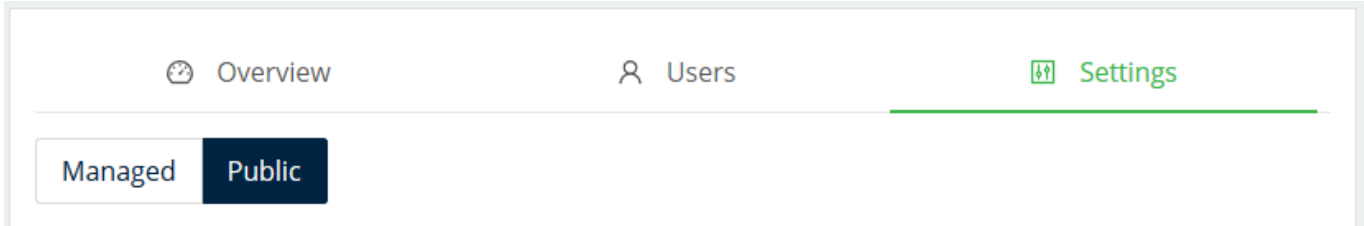
Cloud Portal – Instructions

- Firmware update progress. When the Update Firmware button is clicked the progress of the update can be seen here. When the firmware update is in progress all configuration options on this tab will be disabled.



PUBLIC VS MANAGED MODES

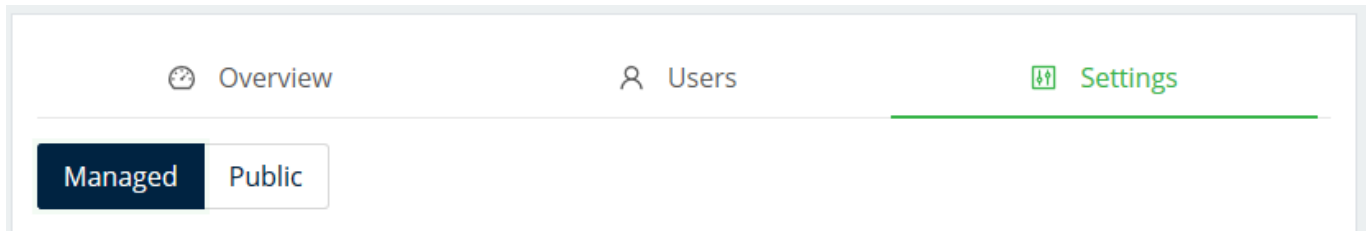
Public is used if you want your Station(s) to operate as a public charging station that anyone can use for secure, on-demand charging.



- Reservation flow:
 - User selects an available bay (green LED)
 - User uses their credential of choice: a PIN of their choice or tap any RFID badge/card to reserve the bay. Note: PIN cannot be repetitive or sequential. E.g., 1234 and 1111 is not permitted.
 - The door will pop open (LED will turn from green to red)
 - User must push the door closed to complete the workflow
 - Bay LED will turn white if the workflow is completed
 - Bay LED will remain red if it has been left open
- Unreserve flow (for retrieving the device that was put in the bay for secure charging):
 - User selects the bay that they reserved (white LED)
 - User must use the credential that was used (PIN or RFID badge/card)
 - The door will pop open (LED will turn from white to red)
 - User must push the door closed to complete the workflow
 - Bay LED will turn green if the workflow is completed
 - Bay LED will remain red if it has been left open

Cloud Portal – Instructions

Managed is used when customers want to control which users are allowed access to the station(s). Customers that want to setup a Check-in/Check-out or Break-Fix workflow should toggle the mode to Managed.



- Reservation flow:
 - User selects an available bay (green LED)
 - User uses their admin assigned credential: PIN or an RFID badge/card
 - The door will pop open after it validates the credential with the cloud platform (LED will turn from green to red).
 - User must push the door closed to complete the workflow
 - Bay LED will turn white if the workflow is completed
 - Bay LED will remain red if it has been left open
 - Unreserve flow:
- Unreserve flow:
 - User selects the bay that they reserved (white LED)
 - User uses their admin assigned credential: PIN or an RFID badge/card
 - The door will pop open (LED will turn from white to red)
 - User must push the door closed to complete the workflow
 - Bay LED will turn green if the workflow is completed
 - Bay LED will remain red if it has been left open

SETUP CHECK-IN/CHECK OUT WORKFLOW

When we refer to Check-in/Check-out workflow, we mean that:

- Admins have pre-loaded the bays of a station(s) with devices
- Admins authorise users to have access to the bays with the devices in them
- The authorised users can check out devices from available bays as they please to do their work
 - Available bays display a green LED on the station and on the Cloud platform overview pages
 - The bay becomes assigned to the user who has checked the device out – the bay LED and the Cloud platform overview page will display white.
- After the user is done with the device, they check that device back into the same bay that the device was checked out from as it has been assigned to them.
- Once the door is closed after the return, the bay will turn back to green and completes the workflow.

For more details about LED colours, see the [OVERVIEW TAB](#) section.

Cloud Portal – Instructions

Setting up a Check-in/Check-out workflow for an entire **account**.

- Go to the Account page
- Navigate to the Settings tab within the account page
- Toggle the mode from Public to Managed
- Go to the Users tab within the account page
- Press the 'Add User' button
- Select the Users that you want to authorise access to the devices that are stored in each bay of every station. Note: You must have users' setup in the User Directory (see [USERS](#) section).

Setting up a Check-in/Check-out workflow for a **node**.

- Navigate to the node that you want to configure
- Note: configurations at this level (Users and Settings) will be greyed out as they are adopting settings from a higher level
- Go to the Settings tab within the node
- Toggle the 'Inherited' switch, that is in line with 'Public | Managed,' to 'Overridden'
- Toggle the mode from Public to Managed
- Go to the Users tab within the node
- Toggle the 'Inherited' switch, to 'Overridden'
- Press the 'Add User' button
- Select the Users that you want to authorise access to the devices that are stored in each bay of each station in this node. Note: You must have users' setup in the User Directory (see [USERS](#) section).

Setting up a Check-in/Check-out workflow for a **station**.

- Navigate to the station that you want to configure
- Note: configurations at this level (Users and Settings) will be greyed out as they are adopting settings from a higher level (from its parent node)
- Go to the Settings tab within the station
- Toggle the 'Inherited' switch, that is in line with 'Public | Managed,' to 'Overridden'
- Toggle the mode from Public to Managed
- Go to the Users tab within the station
- Toggle the 'Inherited' switch, to 'Overridden'
- Press the 'Add User' button
- Select the Users that you want to authorise access to the devices that are stored in each bay of this station. Note: You must have users' setup in the User Directory (see [USERS](#) section).

SETUP BREAK-FIX WORKFLOW

When we refer to Break-Fix workflow, we mean that:

- Admins have pre-loaded the bays of a station(s) with devices

Cloud Portal – Instructions

- Admins authorise users to have access to the bays with the devices in them
- The authorised users can swap their broken device with a spare stored device from the available bays
 - Available bays display a green LED on the station and on the Cloud platform overview pages
- The system will take the bay with the broken device to an offline state so that:
 - other users cannot access the device
 - admins can go and collect the broken device for maintenance
 - replenishing the bay with another spare working device.
- Once the admin has replenished the bay with another spare working device, they will turn the bay back to an available state ready to serve its users with a device when theirs breaks.

Setting up a Break-Fix workflow for an entire **account**.

- Go to the Account page
- Navigate to the Settings tab within the account page
- Toggle the mode from Public to Managed
- Toggle on the 'Take bay offline when accessed' switch
- Go to the Users tab within the account page
- Press the 'Add User' button
- Select the Users that you want to authorise access to the devices that are stored in each bay of every station. Note: You must have users' setup in the User Directory (see [USERS](#) section).

Setting up a Break-Fix workflow for a **node**.

- Navigate to the node that you want to configure
- Note: configurations at this level (Users and Settings) will be greyed out as they are adopting settings from a higher level
- Go to the Settings tab within the node
- Toggle the 'Inherited' switch, that is in line with 'Public | Managed,' to 'Overridden'
- Toggle the mode from Public to Managed
- Toggle the 'Inherited' switch, that is in line with 'Take bay offline when accessed,' to 'Overridden'
- Toggle on the 'Take bay offline when accessed' switch
- Go to the Users tab within the node
- Toggle the 'Inherited' switch, to 'Overridden'
- Press the 'Add User' button
- Select the Users that you want to authorise access to the devices that are stored in each bay of each station in this node. Note: You must have users' setup in the User Directory (see [USERS](#) section).

Setting up a Break-Fix workflow for a **station**.

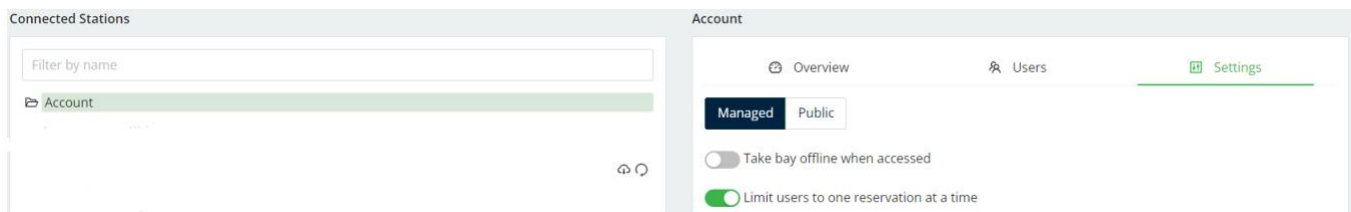
- Navigate to the station that you want to configure
- Note: configurations at this level (Users and Settings) will be greyed out as they are adopting settings from a higher level (from its parent node)

Cloud Portal – Instructions

- Go to the Settings tab within the station
- Toggle the 'Inherited' switch, that is in line with 'Public | Managed,' to 'Overridden'
- Toggle the mode from Public to Managed
- Toggle the 'Inherited' switch, that is in line with 'Take bay offline when accessed,' to 'Overridden'
- Toggle on the 'Take bay offline when accessed' switch
- Go to the Users tab within the station
- Toggle the 'Inherited' switch, to 'Overridden'
- Press the 'Add User' button
- Select the Users that you want to authorise access to the devices that are stored in each bay of this station. Note: You must have users' setup in the User Directory (see [USERS](#) section).

LIMIT USER RESERVATIONS FEATURE

PC Locs/LocknCharge Cloud allows Admins to limit users from reserving more than one bay at a time. This can be done in the Dashboard by clicking the Account level node, selecting the Settings section, and toggling on “Limit users to one reservation at a time”. Bay reservations can only be enforced when using the Managed workflow setting.



Use Case Examples

For workflows where the station bays are empty – such as BYO device programs – Admins can restrict users so they can only reserve one bay for themselves at a time.

For workflows where devices are pre-loaded into stations – such as check-in/check-out or loaner device programs – Admins can restrict users so they can only checkout one device for themselves at a time. This feature ensures each reservation is logged to one user.

Note: The user will receive a “credential incorrect” error on the Tower display if they already have an existing reservation in the system and attempt to reserve a second bay.

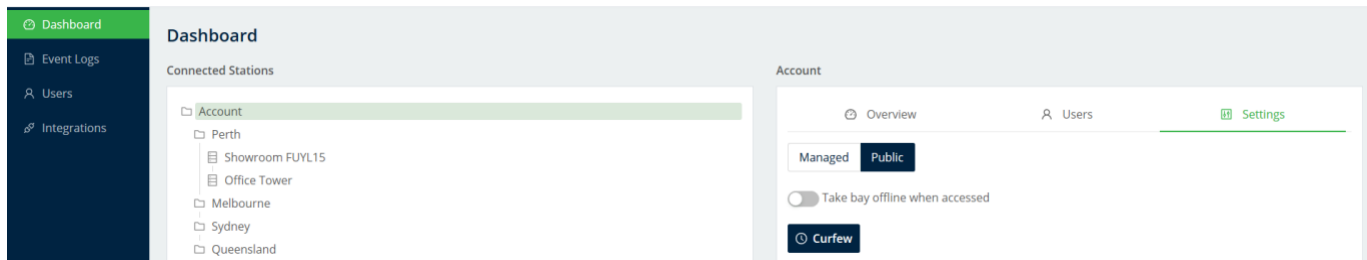
You can find existing reservations for a user by going to the Users page, clicking on the name of the user, and looking under Assignments.

CURFEW FEATURE

PC Locs/LocknCharge Cloud allows Admins to configure Station settings to restrict access to the Station, or a node. Curfews can be set for specific days, every day, single time spans per day or multiple time spans per day.

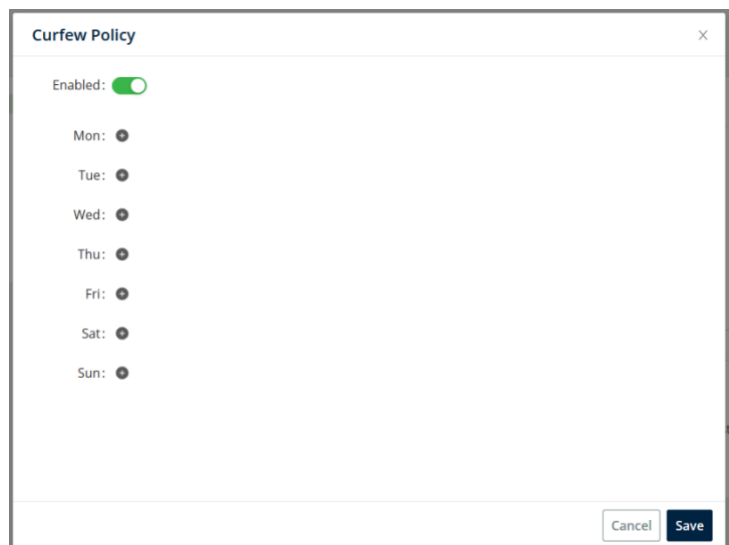
Cloud Portal – Instructions

- Setting up curfews at the account node level will propagate to every station in your account.
- Setting up curfews at a sub-node will propagate to stations nested in the node.
- Setting up curfews at a station will only affect the specific station.



Setting up a curfew for an entire account.

- Go to the Account page
- Navigate to the Settings tab within the account page
- Click on the 'Curfew' button
- A modal will appear. Toggle on the 'Enable' switch
- Press the '+' button against the days that you want to enable curfew
- Drag the bar to the time that you want the curfew to turn on



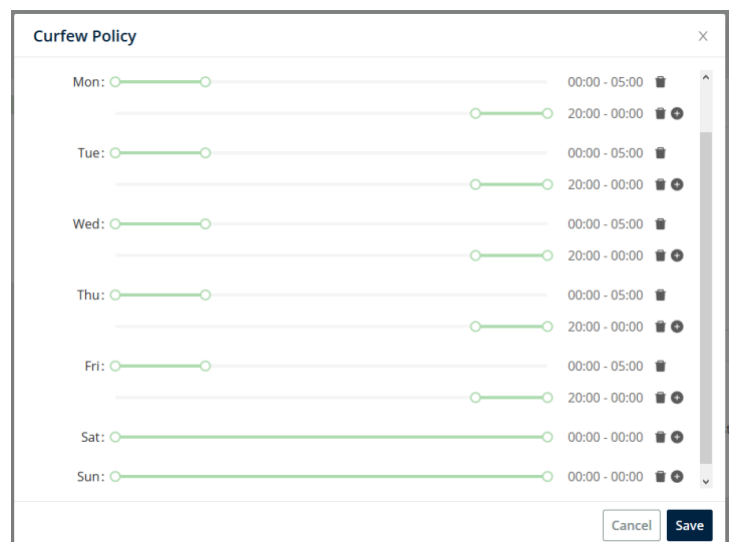
In the example above, the curfew has been set as:

- Monday to Friday, midnight-5AM and 8PM-midnight
- Saturday and Sunday all day

Note: if you do not press save, it will not enable the curfew.

Setting up a curfew on a node or a station.

- Navigate to the node or station that you want to configure
- Click on the Settings tab
- Click on the 'Curfew' button
- A modal will appear. Toggle the 'Inherited' switch, to 'Overridden'



Cloud Portal – Instructions

- Toggle on the 'Enable' switch if it is off
- Add or edit your curfew settings
- Press 'Save'

EVENT LOGS

All user interactions with stations are logged in an event log. These logs can be viewed centrally from the event logs page.

Event Logs	
<div> <div>Dashboard</div> <div>Event Logs</div> <div>Users</div> <div>User Groups</div> <div>Integrations</div> </div>	<div> <div>All</div> <div>App Client</div> <div>Admin</div> <div>System</div> <div>User</div> </div> <div>Feb 12 2021 to Feb 18 2021</div> <div>Search event logs</div>
Event	Date (UTC+08:00)
[System] Bay 1 was closed on HQ Level 1	Feb 18 2021, 11:55am
[System] Workflow started on HQ Level 1	Feb 18 2021, 11:55am
[System] Workflow ended on HQ Level 1	Feb 18 2021, 11:55am
[Robbie Davis] accessed bay 1 on HQ Level 1	Feb 18 2021, 11:55am
[Robbie Davis] unlocked bay 1 on HQ Level 1	Feb 18 2021, 11:55am
[System] Workflow started on HQ Level 1	Feb 18 2021, 11:55am
[System] Workflow ended on HQ Level 1	Feb 18 2021, 11:55am
[System] Bay 5 was closed on HQ Level 1	Feb 18 2021, 11:55am
[System] Workflow started on HQ Level 1	Feb 18 2021, 11:55am

INTEGRATIONS

The Integrations page of the cloud portal is designed to help organisations integrate PC Locs/LocknCharge stations with external systems. The API allows admins to perform actions on a station via a secure REST API. Developer API requests must be authenticated using a bearer auth token.

[Click here to for our API documentation.](https://docs.staging.pclocs.io)

Integrations	
<div> <div>Dashboard</div> <div>Event Logs</div> <div>Reports</div> <div>Users</div> <div>User Groups</div> <div>Integrations</div> </div>	<div> <div>App Clients</div> <div>Webhooks</div> <div>External Users</div> <div>BETA</div> </div> <div> <div>For more information on how to use the API please go to https://docs.staging.pclocs.io</div> <div>New App Client</div> </div>
Client ID	Client Secret

Cloud Portal – Instructions

APP CLIENT

Section where Admins can create credentials for integrating external systems to perform a function on Stations via API.

WEBHOOKS

Webhooks allow Admins to send real-time events from PC Locs/LocknCharge Stations to other systems, to enable automation of downstream workflows.

[Click here to for our Webhook documentation.](#)

Integrations

App Clients
Webhooks
External Users
BETA

Active: ☒

* Name:

* URL:

Description:

Auth Bearer Token:

* Event Types:
☐ Bay {bay} reserved on station {station}
☐ Bay {bay} accessed on station {station}
☐ Bay {bay} closed on station {station}
☐ Bay {bay} stuck on station {station}
☐ Bay {bay} breached on station {station}
☐ Bay {bay} was locked out due to incorrect access attempts on station {station}

Cancel Save

EXTERNAL USERS (ACTIVE DIRECTORY INTEGRATION)

The PC Locs/LocknCharge Cloud can be integrated with Active Directory (AD), Google Secure LDAP service or Okta LDAP Interface using Lightweight Directory Access Protocol (LDAP). For more details, [click here](#).

SINGLE SIGN-ON (SSO)

The SSO feature is only accessible for accounts that are on the integrated tier and has owner permissions to that account. PC Locs/LocknCharge Cloud supports the OIDC and SAML protocols.

[Click here for detailed instructions on how to configure an SSO provider.](#)

Cloud Portal – Instructions

PC Locs, LocknCharge and the Padlock device are Trademarks of PC Locs Pty Ltd. Copyright PC Locs 2020.

Disclaimer

This information is the intellectual property of PC Locs Pty Ltd and may not be distributed, duplicated, or copied in part or full without the written permission. Since the use of this information, the equipment connected and the conditions by which any PC Locs product is used is beyond the control of PC Locs, it is the obligation of the owner and/or user to determine the correct and safe use of any equipment and product. To the extent that the law permits, any liability which may be incurred because of the use or future use of a product manufactured or sold by PC Locs is limited to the cost of repairing or replacing the failed product or component at the discretion of PC Locs either within, or outside of warranty periods, and does not extend to any loss or damage which may be caused because of misuse or failure of the equipment or product or the information contained herein. PC Locs shall not in any event be liable for economic loss of profits, indirect, special, bodily injuries, or consequential damages.