SmartHub Pro2

Installation, configuration and user manual

This manual covers the ClockedIn SmartHub Pro2 terminal from first power-on to day-to-day use. It explains what staff see when they clock in, how an administrator registers a palm, a PIN or a fob, how the terminal is connected to a network, and how it is locked so that it can only run the clocking application.

It is written to be worked through in order during an installation, and to be dipped into afterwards when a single task needs doing. Each procedure is shown alongside the screen it refers to.

> **Before you begin — please read**
>
> The terminal requires **mains power** and is **wall-mounted**. It has no internal battery, so it must be sited within reach of a permanent socket.
>
> Wireless connections operate on the **2.4 GHz band only**. A 5 GHz-only network cannot be seen or joined. Where a network hides or separates its 2.4 GHz band, that band must be made available to the terminal. An **Ethernet** connection is also supported (see 8.2).
>
> If joining your wireless network requires a username as well as a password, some additional details will be needed from whoever manages the network. Section 8.5 explains what, and 8.7 gives you wording you can forward to them.

Contents

1. About the SmartHub Pro2 4
1.1 How staff identify themselves 4
1.2 What the terminal needs 4
1.3 What runs on the terminal 4
2. Using the terminal day to day 5
2.1 The home screen 5
2.2 Clocking in and out 6
2.3 If the terminal cannot reach the network 6
3. Administrator access 6
3.1 Signing in 7
3.2 The Admin menu 7
3.3 Super administrator access 8
4. Registering employees 8
4.1 Opening the registration screen 9
4.2 Finding the employee 9
4.3 Registering a palm 10
4.4 Registering a PIN 11
4.5 Registering a fob or card 12
4.6 Checking and saving the record 13
4.7 Replacing or removing a registration 13
4.8 Locations and radius 14
4.9 Registering while the terminal is offline 15
5. Device Settings 15
6. Super Admin Settings 16
6.1 How the terminal is identified 16
6.2 Clock In/Out or Swipe And Go 17
6.3 Enable Pin or Disable Pin 17
6.4 Mobile Mode 17
6.5 Export DB 17
7. Reaching the Android screen 17
7.1 Leaving OnTime 18
7.2 The Android screen 18
7.3 Returning to OnTime 19
8. Connecting the terminal to a network 20
8.1 What you will need 20
8.2 Wi-Fi or Ethernet 21
8.3 Which type of wireless network do you have? 22
8.4 Connecting with a password only 23

8.5 Connecting with a username and password 24
8.6 Advanced options 25
8.7 Information to request from your network administrator 26
9. Locking the terminal to OnTime 27
9.1 Re-locking the terminal 28
9.2 Working on a locked terminal 29
10. Remote support 30
10.1 Checking the connection 30
10.2 Network requirements 31
11. Looking after the terminal 31
11.1 Cleaning the reader 31
11.2 Fobs and cards 32
11.3 Power and siting 32
11.4 Restarting the terminal 32
12. Troubleshooting 35
12.1 Clocking and recognition 35
12.2 Network 36
12.3 The terminal itself 37
13. Getting help 38
Who to contact 38

1. About the SmartHub Pro2

The SmartHub Pro2 is a wall-mounted time and attendance terminal. Staff identify themselves at the terminal and record a clock-in or a clock-out; the terminal timestamps each event and forwards it for processing. Recording an event takes a second or two and needs no training.

1.1 How staff identify themselves

Three methods are available. An employee may have any one of them, or all three, and can use whichever is convenient on the day.

Method	What the employee does	Registered
Palm	Holds a hand over the reader. Contactless — nothing is touched.	At the terminal (4.4)
PIN	Taps **Enter Pin** and keys in a personal number.	At the terminal (4.5), or in the rostering system
Fob or card	Presents a proximity fob or card to the reader.	At the terminal (4.6)

The palm reader is a **palm vein scanner**. It uses infrared to read the pattern of veins beneath the skin rather than the surface of the hand, which is what allows it to work without contact.

That reading is converted to a text template and encrypted to AES 256. The encryption is one way: a template cannot be turned back into an image of a hand, and matching is performed against the encrypted string. No palm image is stored on the terminal or anywhere else.

1.2 What the terminal needs

Requirement	Detail
Power	Mains power, permanently connected. There is no internal battery.
Mounting	Wall-mount.
Network	Wi-Fi on the 2.4 GHz band, or a wired **Ethernet** connection. Full outbound internet access is strongly recommended (see 10.2).
Support	1-year manufacturer warranty, with 3 years of ClockedIn support including repair or replacement.

1.3 What runs on the terminal

The terminal is built for the sole purpose of running **OnTime**, the clocking application. OnTime is what staff see, and it holds the employee registrations and the terminal's own settings. On the Android screen, and in Android's own settings pages, it is named **OntimeAllocate**.

Android itself and the other applications on the terminal are inaccessible to unauthorised users. The terminal starts in OnTime and returns to OnTime whenever the home button is pressed; reaching anything else is a deliberate act by an administrator, described in 7.

The supporting applications that are present — chiefly **Settings** and **TeamViewer Host** — are there for connectivity and support only. Settings is used for the network connection (8), for locking the terminal to OnTime (9) and for restarting it (11.4); TeamViewer Host is used for remote support (10).

2. Using the terminal day to day

This section is the whole of what an employee needs to know. It can be handed on as it stands, or issued as a quick reference card.

2.1 The home screen

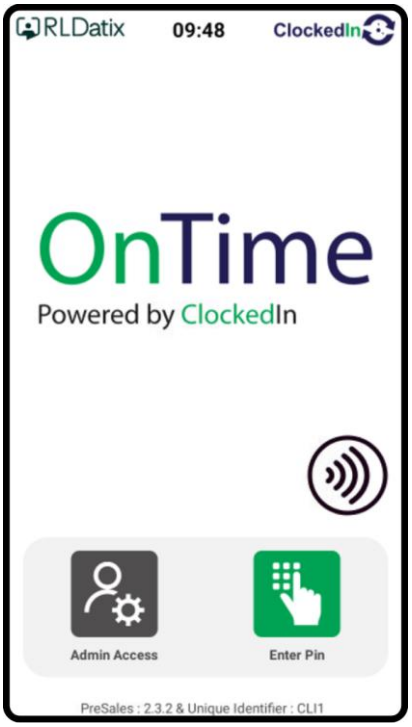


Figure 1 — the OnTime home screen

What you are looking at

The terminal rests on this screen between clockings. The time is shown at the top, and the site's own branding sits to its left.

The contactless symbol above the buttons marks where the palm and fob reader is. Holding a hand or a fob there is all that is needed — there is no button to press first.

Admin Access and **Enter Pin** sit along the bottom. **Enter Pin** is for staff clocking with a PIN; **Admin Access** is for administrators, and is covered in 3.

The line at the very foot of the screen gives the organisation, the OnTime version and the terminal's unique identifier. Quote it whenever you contact support — see 13.

2.2 Clocking in and out

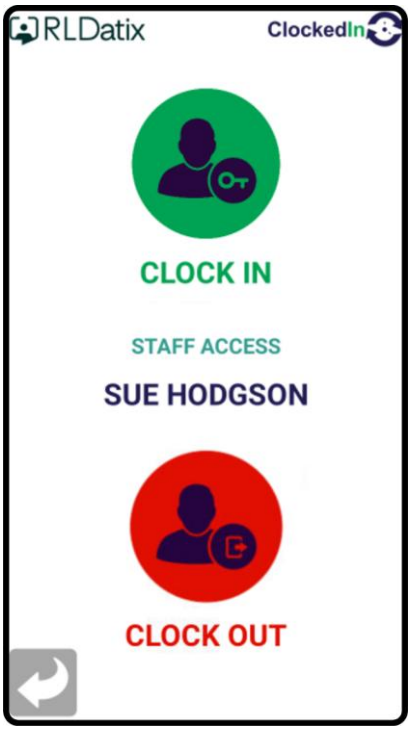


Figure 2 — choosing Clock In or Clock Out

Recording an event

1. Hold your palm over the reader, present your fob, or tap **Enter Pin** and key in your PIN.
2. The terminal recognises you and shows your name.
3. Tap **CLOCK IN** (green) or **CLOCK OUT** (red).

The terminal returns to the home screen by itself, ready for the next person. If you are not recognised, nothing is recorded — try again, and see 12 if it keeps happening.

Where the terminal has been set to **Swipe And Go** instead, there is no choice to make: being recognised is the event, and the terminal works out whether it is an in or an out. See 6.3.

2.3 If the terminal cannot reach the network

Clocking continues to work. Events are held on the terminal and sent on once the connection returns, so staff should carry on using it as normal. Nothing is lost and nothing needs re-entering.

3. Administrator access

Registering employees and changing settings both require an administrator. There are two levels: an administrator, and a super administrator with a small number of additional powers.

3.1 Signing in

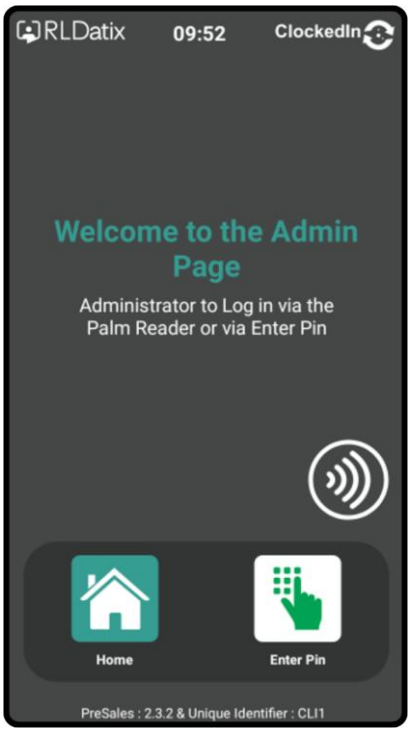


Figure 3 — the administrator sign-in screen

Reaching the Admin page

1. Tap **Admin Access** on the home screen.
2. Identify yourself with the palm reader, or tap **Enter Pin** and key in your administrator PIN.

The screen turns dark, which is the quickest way to tell an administrator screen from a staff one at a glance.

Home returns to the clocking screen without signing in.

3.2 The Admin menu

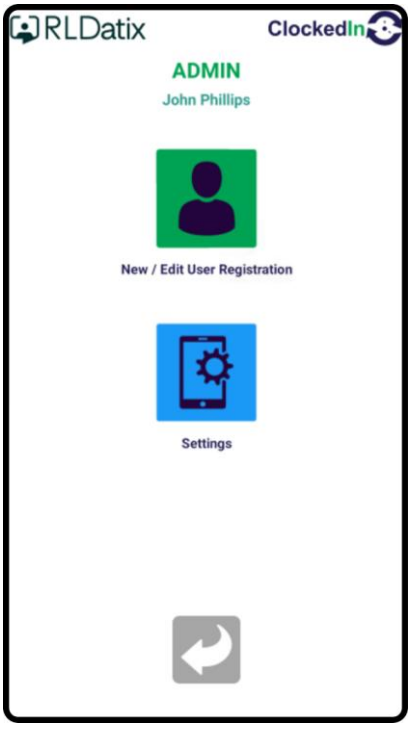


Figure 4 — the Admin menu

Two options

The name of the signed-in administrator appears under the **ADMIN** heading, so it is always clear who is making a change.

New / Edit User Registration (green) registers a palm, a PIN or a fob against an employee. See 4.

Settings (blue) opens Device Settings, which control which methods the terminal offers and how registrations default. See 5.

3.3 Super administrator access

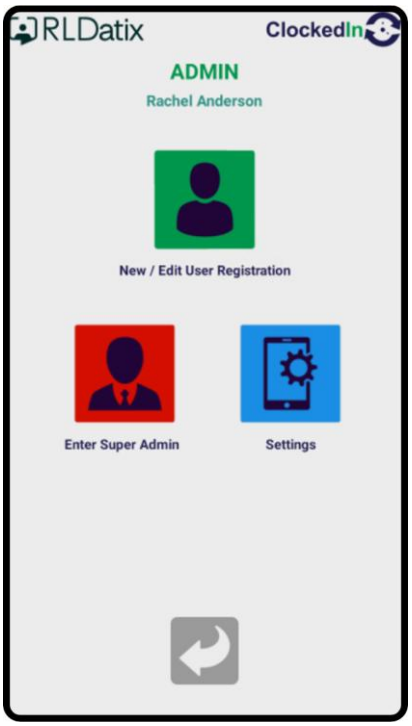


Figure 5 — the Admin menu with elevated access

A third option

An administrator with elevated rights sees an extra red tile, **Enter Super Admin**.

Behind it are the terminal's identity and mode settings — the things that are set once during installation and then left alone. See 6.

Red is used throughout OnTime for the elevated path, in the same way it is used for **CLOCK OUT**.

4. Registering employees

Registration is how an employee's palm, PIN or fob becomes something the terminal recognises. It is done once per employee per method, at the terminal, by an administrator.

> **Employees are not created here**
>
> The employee list comes from your rostering system, which sends across the staff who are enabled for time and attendance. This screen registers **how** an employee identifies themselves — it does not create the employee.
>
> If someone cannot be found by the search in 4.3, they have not yet reached the terminal. Check that they are enabled for time and attendance in the rostering system rather than trying to add them here.

4.1 Opening the registration screen

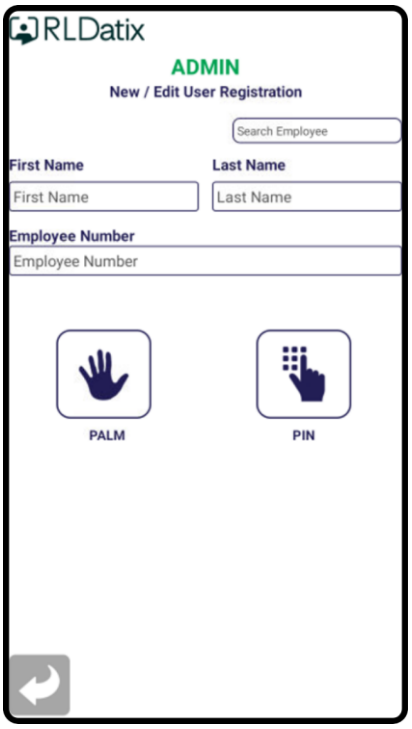


Figure 6 — the registration screen, before an employee is chosen

An empty form

From the Admin menu, tap **New / Edit User Registration**.

The form opens empty, with **PALM** and **PIN** shown in navy. Navy means *not registered*; green means *registered*.

The remaining controls — the location settings, the NFC option and the green save button — appear only once an employee has been chosen.

4.2 Finding the employee



Figure 7 — searching for an employee

Choosing who to register

1. Tap **Search Employee** and type part of the name, or the employee's timeclock ID. The keyboard appears.
2. Matching employees are listed as employee number followed by name.
3. Tap the right one.

First Name, **Last Name** and **Employee Number** fill in by themselves. Check the employee number before going further — names repeat, numbers do not.

4.3 Registering a palm



Figure 8 — an employee record with the palm registered

Reading the tiles

With an employee loaded, tap the **PALM** tile and follow the reader prompt, holding the hand steady and flat until the terminal responds.

A registered method turns green — here **PALM** is green and **PIN** is still navy.

A small red cross appears on the corner of a registered tile. Tapping it removes that registration; see 4.7.

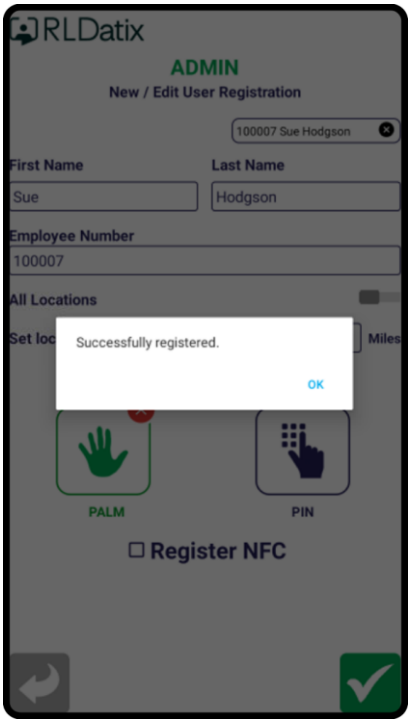


Figure 9 — registration confirmed

The confirmation

The terminal reports **Successfully registered.**

Tap **OK**, then press the green tick at the bottom right to save the registration.

The employee can use the palm reader as soon as the record is saved. If the reader does not respond, or the same hand fails repeatedly, see 12.

4.4 Registering a PIN

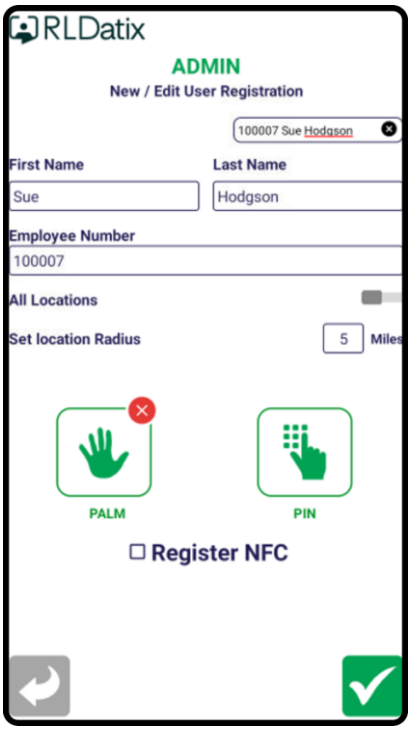


Figure 10 — palm and PIN both registered

Adding a PIN

Tap the **PIN** tile and set the number. Both tiles are then green, as shown.

A PIN can also arrive from the rostering system, in which case it is already set and does not need doing here.

Enter Pin can be hidden in Device Settings (5). While it is hidden, staff cannot clock with a PIN even where one is registered.

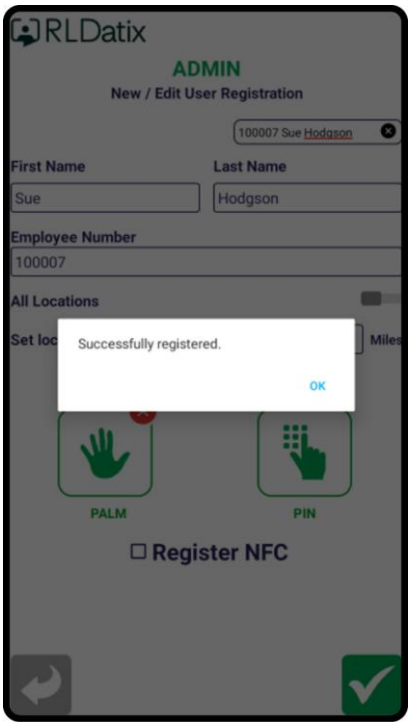


Figure 11 — PIN registration confirmed

The confirmation

The same **Successfully registered.** message appears. Tap **OK**, then press the green tick to save the PIN to the system.

4.5 Registering a fob or card

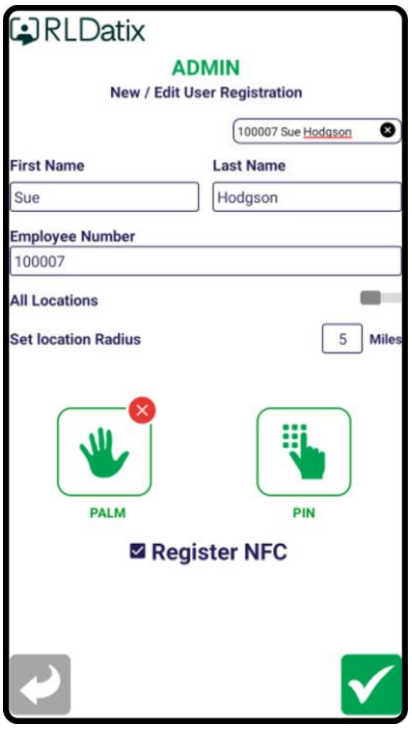


Figure 12 — the Register NFC option ticked

Arming the reader

1. Tick **Register NFC**, below the tiles.

The tick box arms the reader for one registration. It reads **Update NFC** once a fob has been registered, and is used the same way to replace one.

A fob can be registered in the same pass as a palm or a PIN: tick **Register NFC** *before* tapping the **PALM** or **PIN** tile, and the terminal asks for the fob once that registration is done.

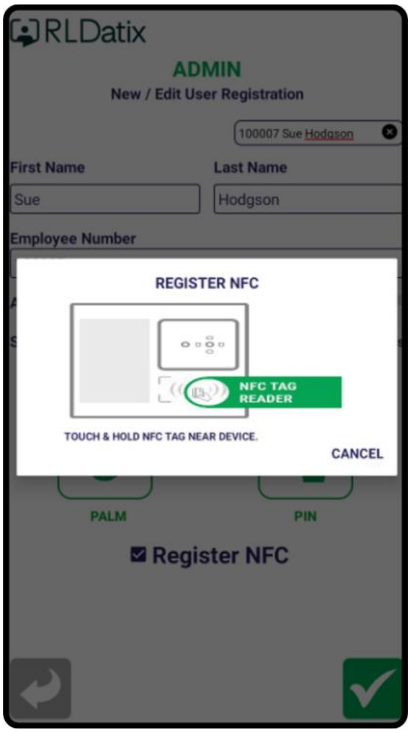


Figure 13 — where to present the fob

Presenting the fob

1. The terminal shows **TOUCH & HOLD NFC TAG NEAR DEVICE.** and marks where the reader sits.
2. Hold the fob or card against that part of the terminal until the terminal responds.

CANCEL abandons the registration and leaves any existing fob in place.

Fobs and cards must be unencrypted and operate at 13.56 MHz. See 11.2 before ordering or reusing existing cards.

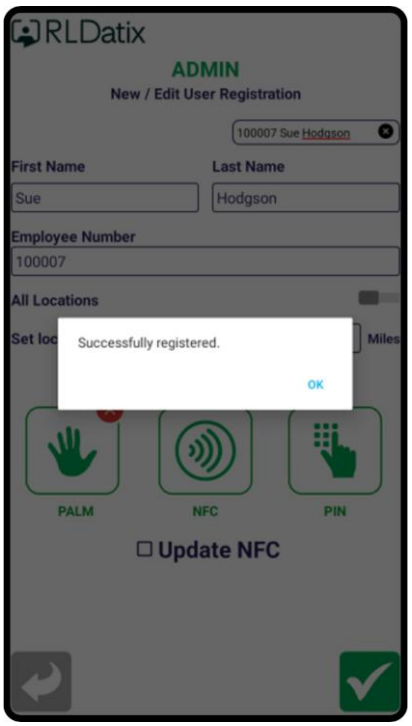


Figure 14 — fob registration confirmed

The confirmation

Successfully registered. appears, and a third tile — **NFC** — takes its place between **PALM** and **PIN**.

Tap **OK**.

4.6 Checking and saving the record

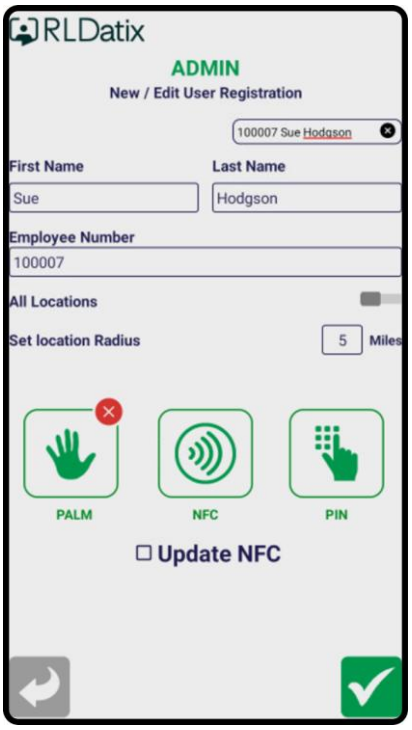


Figure 15 — all three methods registered

Before you leave the screen

Three green tiles — **PALM**, **NFC** and **PIN** — mean the employee can use any of the three.

Tap the green tick at the bottom right to save the record.

Leaving by the grey arrow at the bottom left does not save. Get into the habit of finishing on the tick.

4.7 Replacing or removing a registration

- **To replace a palm or a PIN**, tap its tile again and register afresh. The new reading replaces the old one.

- **To replace a fob**, tick **Update NFC** and present the new fob. This is the step to use when someone loses a fob.
- **To remove a registration**, tap the small red cross on the corner of its tile. The tile returns to navy.

Removing a registration stops that method working for that employee and nothing else. A leaver is removed through the rostering system, which withdraws them from every terminal.

4.8 Locations and radius

Two controls sit above the tiles once an employee is loaded, and they govern which terminals the new registration reaches.

Control	What it does
All Locations	Off by default. Switched on, the registration is offered to every location rather than to those within the radius below.
Set location Radius	A distance in miles, **5** by default. Terminals within that distance of this one receive the registration, so an employee registers once and can then clock at any of them.

Registrations are distributed between terminals automatically; there is nothing to send by hand. Defaults for both controls are set in Device Settings (5).

4.9 Registering while the terminal is offline

Distributing a registration to other terminals needs a network connection, because the registration travels from the terminal it was made on. Registering with no connection still works on that terminal, and clocking events are held until the connection returns.

> **An offline registration is lost if the terminal restarts**
>
> While the terminal is offline the registration exists only in its local database. Fully closing OnTime, or powering the terminal down, clears that database; it is then rebuilt from AirStack, and a registration that has not yet reached AirStack does not come back.
>
> So where an employee has been registered offline, leave the terminal running until it has a connection again, and check the registration afterwards. If it has gone, register them once more.

5. Device Settings

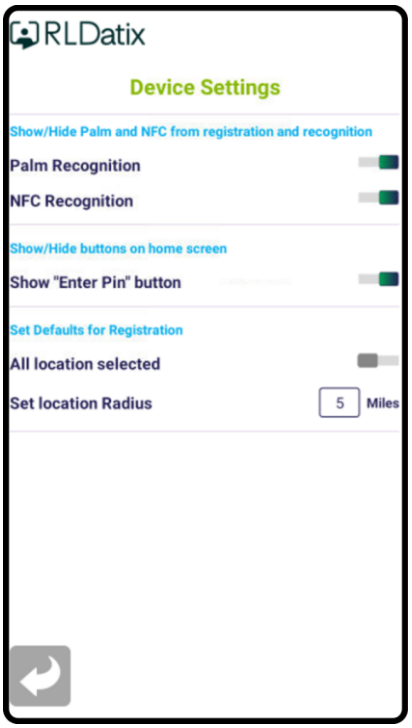


Figure 16 — Device Settings

Where to find it

From the Admin menu, tap **Settings**.

These settings govern what the terminal offers, and how new registrations default. They apply to this terminal.

A grey switch is off. A green switch is on.

Setting	What it controls	Normally
Palm Recognition	Whether the palm reader is offered, both for clocking and during registration. Switched off, the **PALM** tile disappears from the registration screen.	On
NFC Recognition	Whether fobs and cards are offered, in the same way.	On
Show "Enter Pin" button	Whether **Enter Pin** appears on the home screen. Switched off, staff cannot clock with a PIN even where one is registered.	On
All location selected	The default for the **All Locations** control on the registration screen (4.8).	Off

Setting	What it controls	Normally
Set location Radius	The default radius, in miles, for new registrations.	5

> **Switching a method off hides it everywhere**
> Turning off **Palm Recognition** or **NFC Recognition** removes that method from the clocking screen *and* from the registration screen. If a tile you expect is missing when registering an employee, this is the first place to look.

6. Super Admin Settings

This screen holds the terminal's identity, its clocking mode, and the route out to the Android screen. Reaching it requires an administrator with elevated rights.



Figure 17 — Super Admin Settings

Where to find it

From the Admin menu, tap **Enter Super Admin**. The tile appears only for an administrator with elevated rights (3.3).

6.1 How the terminal is identified

The fields across the top of the screen identify the terminal to the wider system.

Field	What it holds
Organization	The organisation the terminal belongs to.
Unique Identifier	The terminal's own identifier. This is the value that appears at the foot of the home screen and the one support will ask for.
Location	The site or department.
LatLng	The terminal's position, used with the radius settings in 4.8.

Field	What it holds
Postcode	The postcode of the site.

> **These fields are read-only**
>
> All five are held and maintained by ClockedIn. The terminal displays them so that you can check them and quote them to support; they cannot be edited here.
>
> If any of them is wrong, or needs changing because the terminal has been moved to another site, contact ClockedIn support and it will be corrected centrally.

6.2 Clock In/Out or Swipe And Go

The first switch chooses how an event is recorded once an employee has been recognised.

- **Clock In/Out** shows the two buttons in Figure 2 and asks the employee to choose. It is the clearer of the two, and the usual setting.
- **Swipe And Go** records the event on recognition alone, without a choice. It suits a single busy entrance where queueing matters more than the distinction.

6.3 Enable Pin or Disable Pin

The second switch turns PIN clocking on or off for the terminal as a whole. It sits above the **Show "Enter Pin" button** setting in 5: with PINs disabled here, showing the button achieves nothing.

6.4 Mobile Mode

The green **Mobile Mode** button at the top of the screen is how you leave OnTime and reach the Android screen. Tapping it brings up the prompt described in 7.1.

This is the only route to the Android screen, and it is behind super administrator access — which is what keeps Android out of reach of anyone using the terminal normally.

6.5 Export DB

Export DB writes out the terminal's local database. It is a diagnostic tool: use it when ClockedIn support asks for it, and send them the resulting file.

7. Reaching the Android screen

The network settings and the kiosk lock are both in Android rather than in OnTime, so both start from here.

7.1 Leaving OnTime

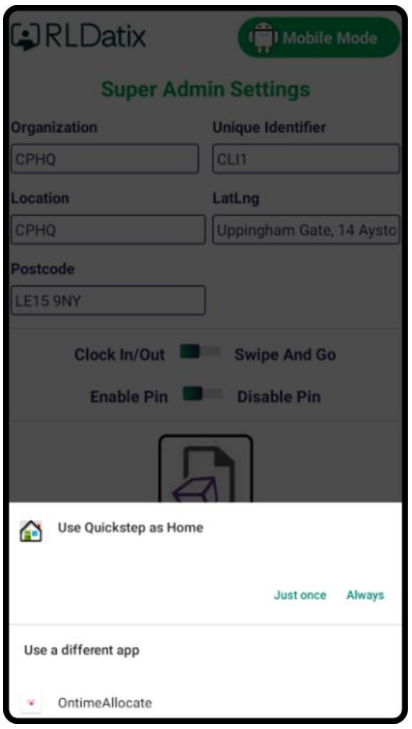


Figure 18 — the prompt shown on leaving OnTime

Getting out to Android

1. Tap **Admin Access** on the OnTime home screen and sign in as an administrator with elevated rights.
2. Tap **Enter Super Admin**, then the green **Mobile Mode** button (6.4).
3. Android asks which application should act as Home. Tap **Just once**.

Just once hands control to the Android screen for this occasion and leaves OnTime as the permanent home application.

Always makes the Android screen permanent — it undoes the kiosk lock, and the terminal will then need re-locking as described in 9.1. Tap **Just once** for any routine piece of work.

7.2 The Android screen

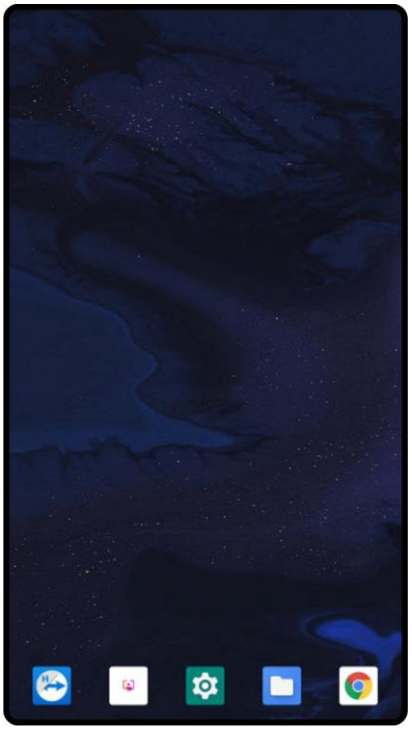


Figure 19 — the Android screen

Five applications

A row of five icons sits along the bottom of the screen. None of them is labelled, so they are identified by appearance, left to right:

TeamViewer Host — blue, first. Remote support; see 10.

OntimeAllocate — white with a pink mark, second. This is OnTime.

Settings — green with a cog, third. Network settings (8) and the kiosk lock (9).

Files — blue with a folder, fourth.

Chrome — white with a coloured swirl, fifth.

7.3 Returning to OnTime



Figure 20 — back at the OnTime home screen

Finishing up

Tap the **OntimeAllocate** icon, second in the row.

The terminal returns to the clocking screen and is ready for staff again.

Always finish an admin visit here. A terminal left sitting on the Android screen is not recording anything.

8. Connecting the terminal to a network

This section covers both networks that are joined with a password alone, and networks that also require a username. It lists the information you may need to obtain from whoever manages your network before installation.

8.1 What you will need

Collect the following before starting. The terminal will not save a wireless profile until every required field is completed.

For all networks

- The network name (SSID), exactly as it is broadcast, including capitalisation.
- Confirmation that the network is available on 2.4 GHz.
- Physical access to the terminal screen.

If the network is joined with a password only

- The wireless password (also called the pre-shared key, PSK, or network key).

If the network also requires a username

- A username and password valid for the wireless network. This must be an account the authentication server will accept — a standard staff login may not work if the network is restricted to registered devices.
- The hostname held in the authentication (RADIUS) server certificate — its Common Name (CN) or a DNS entry from its Subject Alternative Name (SAN). This is required for the **Domain** field.
- The Certificate Authority (CA) certificate file, if the server certificate was issued by an internal CA rather than a public one.

> **If you do not have these details**
> 8.7 contains wording you can forward to whoever manages your wireless network. They should be able to supply all three items.

8.2 Wi-Fi or Ethernet

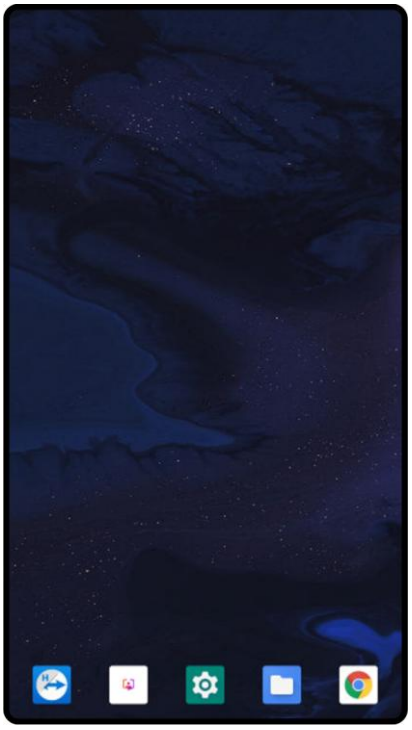


Figure 21 — the Android screen

Step 1 — open Settings

1. Leave OnTime as described in 7.1.
2. On the Android screen, tap **Settings** — the green icon with a cog, third in the row.

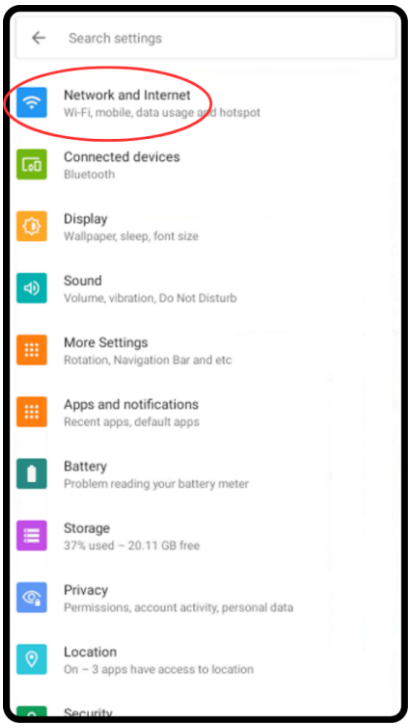


Figure 22 — the Android Settings list

Step 2 — open Network and Internet

1. Tap **Network and Internet**, at the top of the list.



Figure 23 — Network and Internet

Choosing the connection

Wi-Fi shows the network currently joined, with a switch to turn wireless on and off. Tap the row itself to reach the network list.

Ethernet is the wired alternative. A wired connection needs no configuration on a network using automatic addressing: connect the cable and the terminal takes an address.

Aeroplane mode should be off. **Mobile network** is unavailable on this model.

Where both are connected, the wired connection is used. A wireless profile can be left configured as a fallback.

> **The wired and wireless MAC addresses are different**
>
> Where MAC addresses have to be approved before a device is allowed onto the network, make sure the right one is registered — approving the Wi-Fi MAC will not admit a terminal connected by cable, or the other way round.
>
> The **Ethernet** MAC address is shown by tapping **Ethernet** on this screen. The **Wi-Fi** MAC address is in the Android system settings.

8.3 Which type of wireless network do you have?

Check this before you start, as it determines which of the next two sections to follow. The quickest test is to think about what someone is asked for when they join the network on a phone or laptop.

To join the network you are asked for	Shown on the terminal as	Follow
A password only	WPA2-Personal or WPA3-Personal	8.4
A username and a password	WPA2-Enterprise or WPA3-Enterprise	8.5
Nothing at all	Open or unsecured	8.4, leaving the password blank

You can also confirm this on the terminal itself. Tap the network name and look at the **Security** line. "Personal" means a password alone; "Enterprise" means a username and password. If the line ends in "-Enterprise", follow 8.5.

8.4 Connecting with a password only

Use this section for a network joined with a password and nothing else. This is what the terminal calls a WPA2-Personal or WPA3-Personal network, and it is what most sites use.

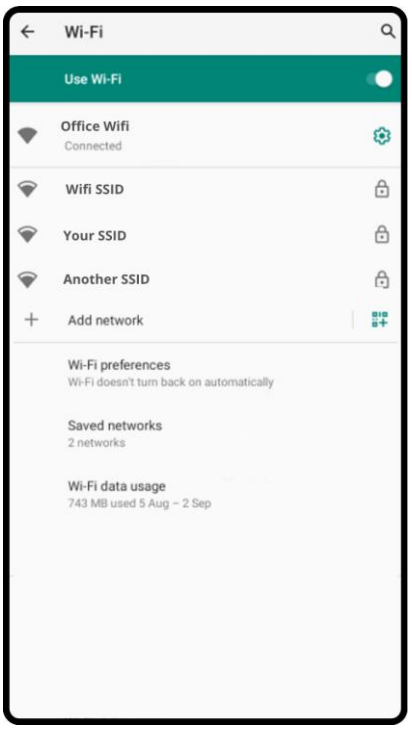


Figure 24 — the Wi-Fi network list

Opening the Wi-Fi list

1. Check that **Use Wi-Fi** is switched on.
2. Wait a few seconds for the list of networks to populate.
3. Tap the name of your network.

If your network does not appear, it is either out of range, not broadcasting its name, or not available on 2.4 GHz. Tap **Add network** to enter a hidden network name manually.

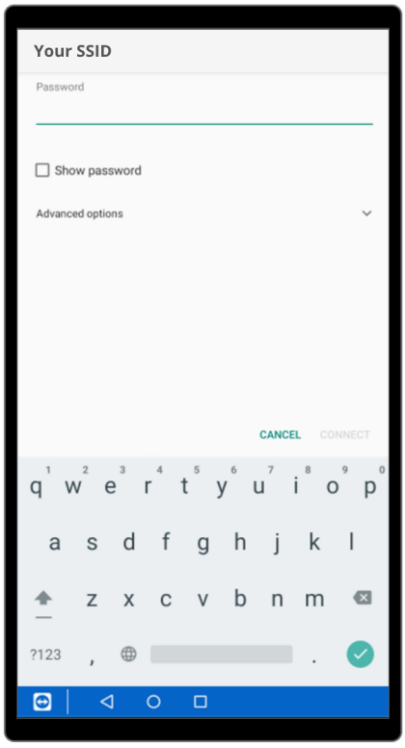


Figure 25 — entering the network password

Entering the password

1. Type the wireless password into the **Password** field.
2. Tick **Show password** and check it character by character. Passwords are case-sensitive and this is the single most common cause of failure.
3. Tap **CONNECT**.

The terminal will show Connecting, then Connected. This normally takes under fifteen seconds.

Leave **Advanced options** alone unless your network requires a fixed IP address or a proxy — see 8.6.

8.5 Connecting with a username and password

Use this section for a network that requires a username as well as a password. This is what the terminal calls a WPA2-Enterprise or WPA3-Enterprise network. There are more fields to complete, and the terminal will not let you save the network until the required ones are filled in.

Begin as in 8.4: open **Settings**, then **Wi-Fi**, and tap your network name. The terminal will then show the longer form below.

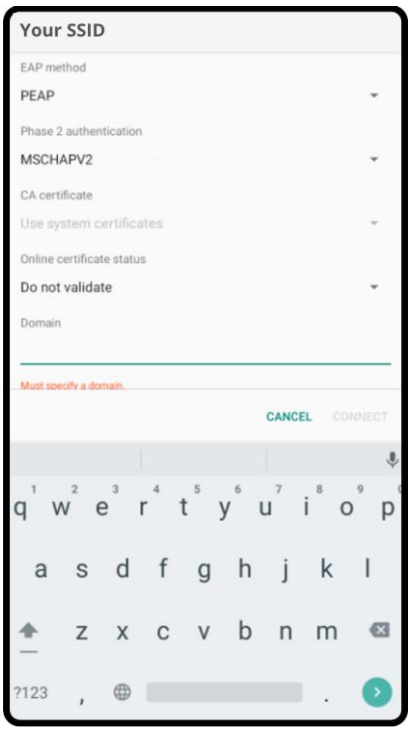


Figure 26 — EAP method, certificate and Domain fields

Certificate and method settings

1. **EAP method** — set to **PEAP** unless your network administrator has specified TTLS or TLS.
2. **Phase 2 authentication** — set to **MSCHAPV2**.
3. **CA certificate** — select the certificate supplied by your network administrator. If they have confirmed that certificate validation is not required, select **Do not validate** here.
4. **Online certificate status** — leave as **Do not validate**.
5. **Domain** — enter the hostname from the authentication server certificate, for example radius.yourcompany.co.uk. It is not your website address and not the name of the wireless network.

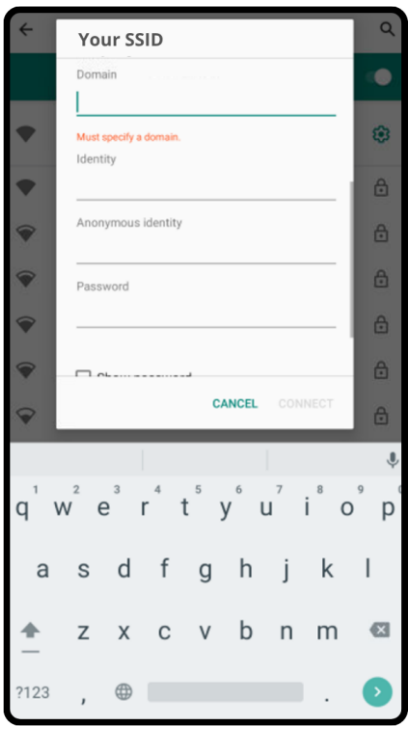


Figure 27 — Identity, Anonymous identity and Password

Credentials

1. **Identity** — the username supplied for the terminal.
2. **Anonymous identity** — leave blank unless your network administrator has specified a value.
3. **Password** — the password for that username. Tick **Show password** and verify it before continuing.

CONNECT becomes available once all mandatory fields are complete. Tap it to join the network.

> **"Must specify a domain" and a greyed-out CONNECT button**
>
> These are two separate dropdowns and they are easily confused. **Online certificate status** controls only revocation checking; it does not switch validation off.
>
> While **CA certificate** is set to **Use system certificates**, the **Domain** field is mandatory and the profile cannot be saved without it.
>
> Either enter the correct hostname in **Domain**, or set the **CA certificate** dropdown itself to **Do not validate** — the **Domain** field then disappears.
>
> If **Do not validate** is not offered in the **CA certificate** list, a **Domain** value must be supplied. Request it using the questions in 8.7.

8.6 Advanced options

Most installations need nothing from this section. Use it only if you have been told the terminal requires a fixed IP address, or that traffic must pass through a proxy server.

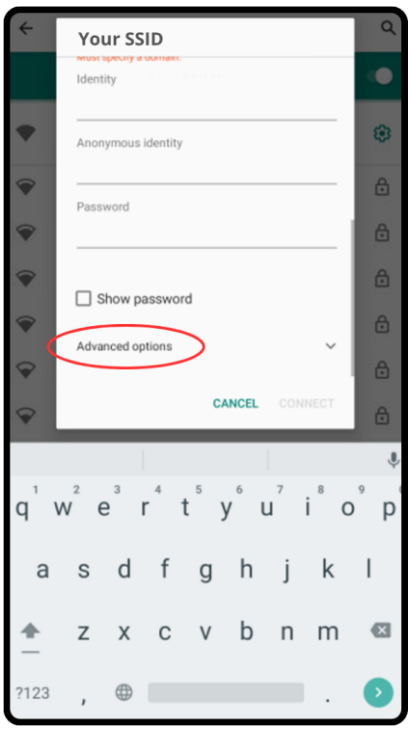


Figure 28 — the Advanced options link

Opening advanced options

1. Scroll to the bottom of the network form and tap **Advanced options** to expand the section.

Everything in here is optional. If the site uses standard automatic addressing, leave all three settings at their defaults.

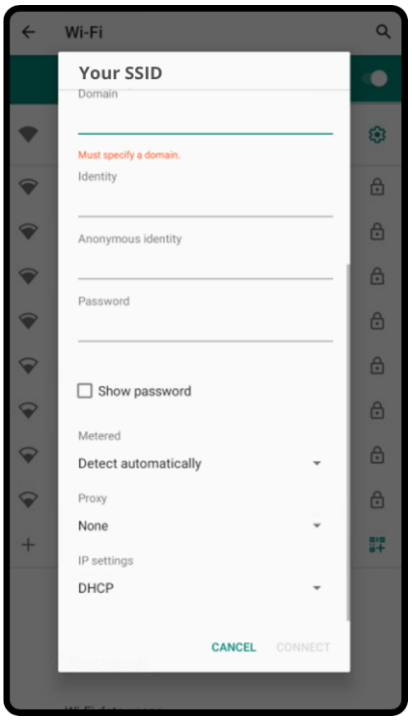


Figure 29 — Metered, Proxy and IP settings

Metered, Proxy and IP settings

1. **Metered** — leave as **Detect automatically**.
2. **Proxy** — leave as **None** unless the site uses a proxy server, in which case select **Manual** and enter the hostname, port and any bypass list you have been given.
3. **IP settings** — leave as **DHCP** so the terminal is assigned an address automatically. Select **Static** only if a fixed address has been reserved for the terminal, and then enter the address, gateway, network prefix length and DNS servers exactly as provided.

An incorrect static configuration will let the terminal join the wireless network but leave it unable to reach the server. If in doubt, use **DHCP**.

8.7 Information to request from your network administrator

If your network requires a username and password, the wording below can be forwarded to whoever manages it. All three items are needed before the terminal can be set up.

Suggested wording

We are installing a wall-mounted ClockedIn time and attendance terminal that needs to join the wireless network. The terminal runs Android and supports WPA2 and WPA3, on the 2.4 GHz band only. To connect it to an 802.1X network using PEAP with MSCHAPv2, please could you provide:

1. The hostname in the RADIUS server certificate — the Common Name, or a DNS entry from the Subject Alternative Name. The terminal requires this in its Domain field and will not save the wireless profile without it.

2. The CA certificate that issued that server certificate, as a .crt or .cer file, if it was issued by an internal Certificate Authority.

3. A username and password the terminal can authenticate with, if an account has not already been created for it.

Alternatively, if it is simpler at your end, a dedicated 2.4 GHz WPA2-Personal network for devices of this kind would avoid the certificate requirement entirely. We are happy to work with either approach.

A note on username-and-password networks

Networks of this kind work well for laptops and phones, which can prompt someone when a certificate expires or a password changes. A wall-mounted terminal cannot do this. It simply stops connecting, and the only visible symptom is an authentication message on screen.

For this reason many sites place terminals, printers and similar fixed devices on a separate 2.4 GHz network secured with WPA2-Personal, isolated on its own VLAN. This is usually a short change for the network administrator and removes an ongoing maintenance burden. It is worth raising as an option rather than a fallback.

9. Locking the terminal to OnTime

Terminals are delivered and installed with OnTime already locked to kiosk mode: the terminal starts in OnTime, and the home button returns to OnTime. Nothing needs doing to put a new terminal into this state.

The lock is undone by choosing **Always** rather than **Just once** at the prompt in 7.1. Where that has happened, use this section to put it back.

9.1 Re-locking the terminal



Figure 30 — the App info shortcut

Step 1 — open App info

1. From the Android screen, press and hold the **OntimeAllocate** icon — the white icon with a pink mark, second in the row.
2. Tap **App info** in the small panel that appears.

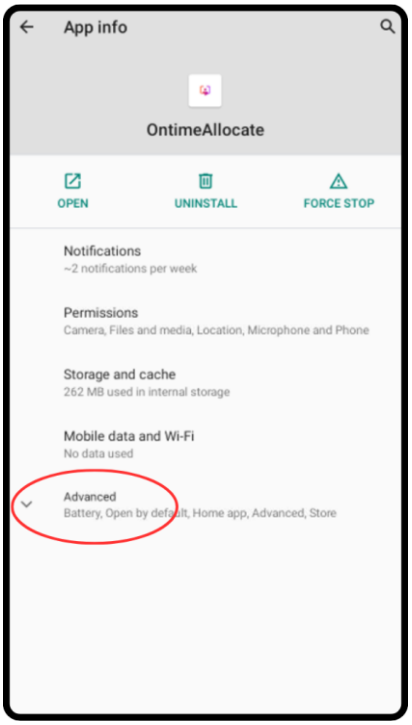


Figure 31 — the App info page

Step 2 — expand Advanced

1. Tap **Advanced**, at the foot of the list.

Its summary line reads *Battery, Open by default, Home app, Advanced, Store*, which is how to recognise the right row.

Take care not to tap **UNINSTALL** or **FORCE STOP** near the top of this page.

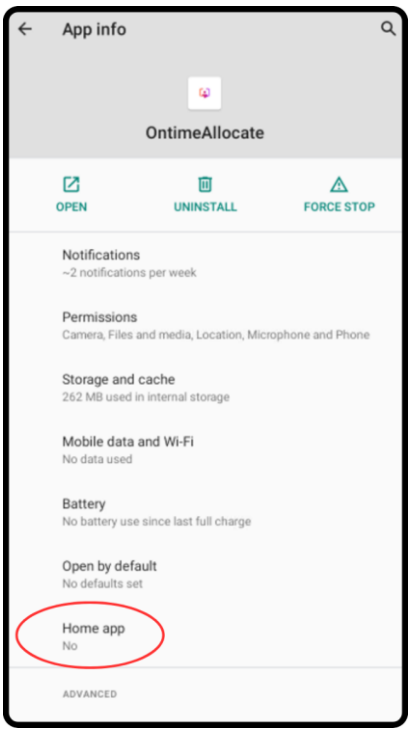


Figure 32 — the Home app setting

Step 3 — open Home app

1. Find **Home app** in the expanded list. It reads **No**.
2. Tap it.



Figure 33 — the Default home app picker

Step 4 — choose OntimeAllocate

1. Tap **OntimeAllocate**, moving the selection away from **Quickstep**.

The change takes effect immediately — there is nothing to save and no confirmation.

Press the home button to check. The terminal should go straight to the OnTime clocking screen.

9.2 Working on a locked terminal

The lock does not put Android out of an administrator's reach — it puts it behind super administrator access. The Android screen is reached only through **Mobile Mode** in Super Admin Settings, which brings up the prompt described in 7.1; there is no other way to it from a locked terminal. That is what keeps the browser, the file manager and the settings away from anyone using the terminal to clock in.

10. Remote support

Terminals are supported remotely using TeamViewer. It allows the service desk to take full control of a terminal to diagnose faults, and it is also how software updates are applied — neither requires anyone to be on site.

10.1 Checking the connection

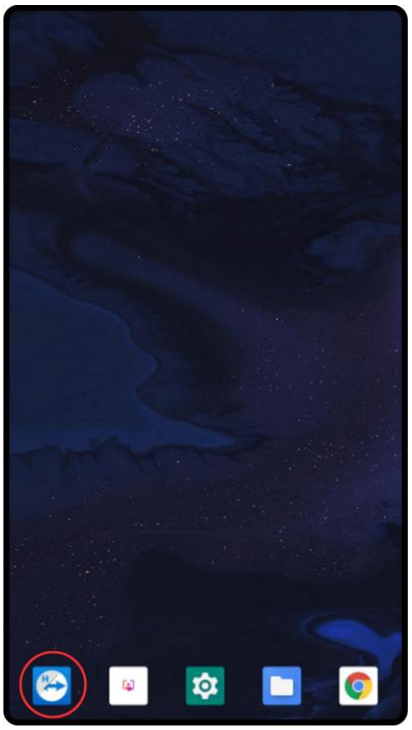


Figure 34 — the TeamViewer Host icon

Opening TeamViewer Host

1. From the Android screen, tap the blue **TeamViewer Host** icon, first in the row.

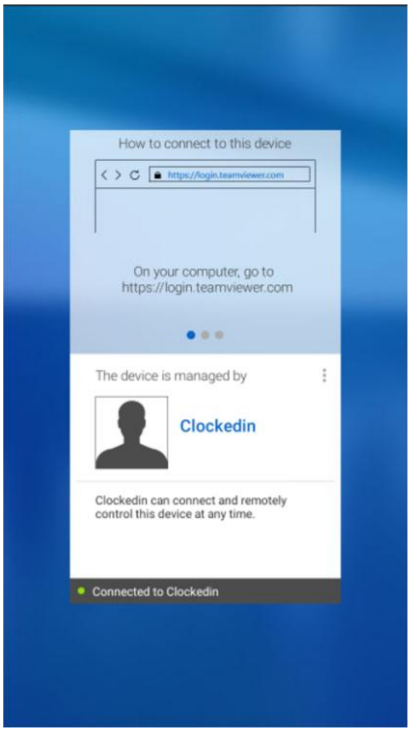


Figure 35 — TeamViewer Host, connected

What a healthy terminal shows

The strip along the bottom of the card is the part that matters. **Connected to Clockedin** beside a green dot means the terminal is reachable for remote support.

Anything else — a red or amber indicator, or a message that the device is not reachable — means the terminal cannot get out to the internet. Check the network connection (8) before raising a fault.

This check is worth doing before you leave site, and before reporting any problem. A terminal that cannot be reached remotely takes considerably longer to support.

10.2 Network requirements

It is strongly recommended that customer firewalls allow full outbound internet access for the terminal. This prevents communication and syncing problems in both directions, for both attendance events and employee registration templates. Remote support needs outbound access of its own, primarily on port 5938.

The full network requirements — ports, destinations and the traffic the terminal depends on — are set out in the ClockedIn technical architecture document. Ask your ClockedIn contact for a copy if you do not have one.

11. Looking after the terminal

11.1 Cleaning the reader

The scanning surface has a silicone layer. Repeated use of industrial cleaning solvents, particularly alcohol-based ones, damages that layer, and the damage shows up as reduced capture sensitivity — the reader becomes gradually less willing to recognise people.

For everyday marks, wipe with a dry cloth. For something sticky, spray a small amount of a mild ammonia-based cleaner such as Windex onto a **cloth**, blot or gently wipe the affected area, then blot dry.

Two things to avoid

Do not spray any cleaner directly onto the scanning surface.

Do not use paper towels: they leave paper particles on the silicone layer.

11.2 Fobs and cards

If you already issue ID cards and would like to reuse them, send samples to ClockedIn through your account manager and we will confirm whether they can be read. Where they cannot, ClockedIn can supply compatible cards or keyring fobs in any quantity. Compatibility requirements are in 1.1.

11.3 Power and siting

The terminal has no internal battery, so it stops when its power does and restarts when power returns. Events already recorded are held on the terminal and are not lost. To restart the terminal deliberately, see 11.4.

Where a terminal repeatedly loses its network, the position of the terminal relative to the nearest access point is the usual cause. See 12.

11.4 Restarting the terminal

The terminal is restarted from Android's navigation bar, the strip of buttons along the foot of the screen. On the SmartHub Pro2 the bar is kept hidden so that it cannot be brought up over OnTime. Restarting means showing it for long enough to reach its power button, then hiding it again. Reaching the setting takes super administrator access (7.1).

A restart loses any registration made while offline

Restarting clears OnTime’s local database in the same way as powering the terminal down (4.9). If anyone has been registered while the terminal was offline, wait until it is connected again before restarting.

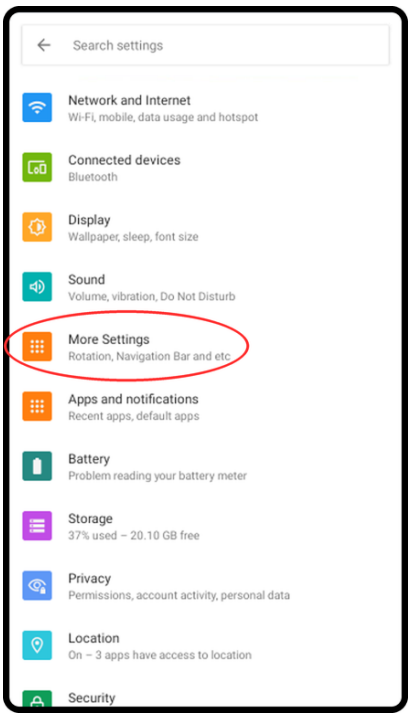


Figure 36 — More Settings in the Android Settings list

Step 1 — open More Settings

1. Leave OnTime as described in 7.1, and tap **Settings** on the Android screen.
2. Tap **More Settings**.

Its summary line reads Rotation, Navigation Bar and etc, which is how to recognise the right row.

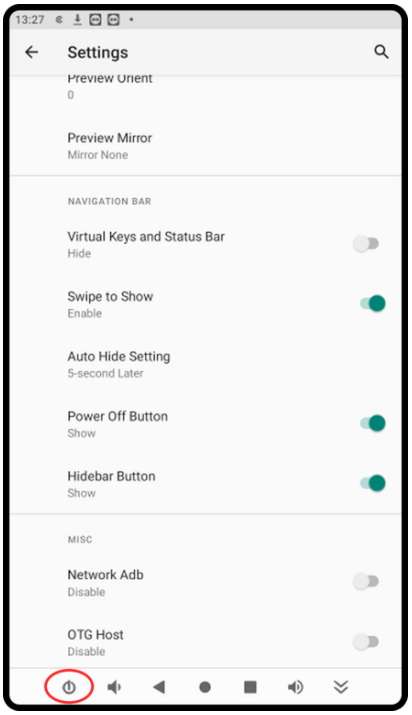


Figure 37 — the Navigation Bar settings, with the navigation bar showing

Step 2 — show the navigation bar

1. Under **Navigation Bar**, check that **Power Off Button** and **Hidebar Button** are both switched on, reading Show. Switch on either one that is not.
2. Switch on **Swipe to Show**. A message appears at the foot of the screen.
3. Wait for the message to clear, then swipe up from the bottom edge of the screen. The navigation bar appears along the foot of the screen.

Step 3 — restart

1. Tap the power button, at the left-hand end of the navigation bar.
2. Tap **Restart**. Do not choose **Power off**, which shuts the terminal down and leaves it off.

The bar hides itself again after a few seconds (**Auto Hide Setting**, 5-second Later). If it goes before you reach the power button, swipe up again.

The terminal shuts down and starts again in OnTime.

Step 4 — hide the navigation bar again

1. Leave OnTime again (7.1) and go back to **Settings**, then **More Settings**.
2. Switch **Swipe to Show** off. Leave every other setting on the screen as it is.
3. Return to OnTime as described in 7.3.

> **Why Swipe to Show goes back off**
>
> While it is on, anyone at the terminal can swipe up over OnTime and bring up the navigation bar, with its power, volume and navigation buttons. Switched off, the bar stays out of sight while OnTime is running.

12. Troubleshooting

Work down the relevant table. Where a symptom has more than one possible cause, they are listed in the order worth checking.

12.1 Clocking and recognition

Symptom	Likely cause	Action
A palm is not recognised, or is recognised inconsistently	The employee is presenting the hand they did not register. The reader needs cleaning.	Ask them to use the hand they registered with. If they need to use either hand, register the second one as well (4.7). Clean the scanning surface as described in 11.1.
One employee is never recognised, whatever they present	No registration exists on this terminal. They were registered while the terminal was offline, and it has since restarted. This terminal is outside the radius of the terminal they registered at.	Open their record (4.2) and check for green tiles. Register them again — see 4.9. Register them at this terminal, or widen the radius (4.8).
A fob is not detected, and no fob works	The fob reader has stopped responding.	As a super administrator, exit OnTime and close it from the recent-applications view; the reader is detected again when OnTime returns to the foreground. The recent-applications button is on the navigation bar: show it as in 11.4, steps 1 and 2, and switch Swipe to Show off again afterwards. Closing OnTime clears any registration made while offline (4.9). As an administrator, open **Settings**, switch the fob slider off, select **NFC** and switch NFC off, then go back to OnTime and repeat the steps to switch it back on.
A fob is not detected, but other fobs work	The fob is not 13.56 MHz, or is encrypted. The fob is not registered to that employee.	Check compatibility — see 1.1 and 11.2. Tick **Update NFC** and present the fob again (4.5).
A registration was made but has disappeared	It was made while the terminal was offline, and OnTime was closed or the terminal was powered down before the connection returned.	Register the employee again with the terminal connected — see 4.9.

Symptom	Likely cause	Action
Enter Pin is missing from the home screen	**Show "Enter Pin" button** is switched off. PINs are disabled for the terminal.	Switch it on in Device Settings (5). Set the switch to **Enable Pin** in Super Admin Settings (6.3).
A **PALM** or **NFC** tile is missing when registering	That method is switched off for the terminal.	Switch **Palm Recognition** or **NFC Recognition** back on in Device Settings (5).
An employee cannot be found by the search	They have not reached the terminal from the rostering system.	Confirm they are enabled for time and attendance in the rostering system. Employees are not created at the terminal — see 4.

12.2 Network

Symptom	Likely cause	Action
The network does not appear in the list	The network is 5 GHz only. The network name is hidden. The signal does not reach the terminal.	Confirm the network is broadcast on 2.4 GHz. Use **Add network** to enter the name manually. Check signal strength at the terminal position.
"Must specify a domain" and **CONNECT** is greyed out	**CA certificate** is still set to **Use system certificates**, which makes **Domain** mandatory.	Enter the server certificate hostname in **Domain**, or set the **CA certificate** dropdown to **Do not validate**. Note this is a different dropdown from **Online certificate status**.
"Authentication problem"	A password alone has been entered on a network that also expects a username. Incorrect username or password. The account is not recognised by the authentication server.	Check the **Security** line for the network. If it ends in "-Enterprise", a username is required — follow 8.5. Re-enter both, using **Show password** to verify. Ask your network administrator to check the authentication log for the terminal.
Connects, then drops repeatedly	Marginal signal strength. Fast roaming or band steering interfering with the terminal.	Reposition the access point, or add one nearer the terminal. Ask your network administrator to disable fast roaming (802.11r) on the network the terminal uses, or to provide a dedicated network for it.

Symptom	Likely cause	Action
Shows as connected but the terminal cannot reach the server	A static IP configuration is incorrect. The terminal is on a network segment that blocks outbound access.	Set **IP settings** back to **DHCP** and retest. Ask your network administrator to confirm the network permits the required outbound traffic — see 10.2.
Worked previously, has now stopped	A wireless password or account password has been changed. A server or CA certificate has expired. The network security settings have been changed.	Re-enter the current credentials. Ask your network administrator to confirm certificate validity, and to supply a replacement CA certificate if it has been renewed. Confirm the network has not been changed to require a username.
TeamViewer does not show **Connected to Clockedin**	No network connection. The firewall blocks the outbound access TeamViewer needs.	Check the connection as in 8.2. Ask your network administrator to confirm the outbound access described in 10.2.

12.3 The terminal itself

Symptom	Likely cause	Action
Staff can reach the Android screen, the browser or Settings	**Always** was chosen at the prompt in 7.1, which undid the kiosk lock.	Re-lock the terminal as described in 9.1.
The terminal starts on the Android screen rather than OnTime	OnTime is no longer the home application.	Re-lock the terminal as described in 9.1.
Recognition works but no choice of Clock In or Clock Out appears	The terminal is set to **Swipe And Go**.	This is a setting, not a fault. Change it in Super Admin Settings if the choice is wanted — see 6.2.
The identity fields in Super Admin Settings are wrong	They are held centrally by ClockedIn and cannot be edited on the terminal.	Contact ClockedIn support with the terminal's unique identifier and what needs changing — see 6.1.
A bar of buttons appears when someone swipes up from the bottom of the screen	**Swipe to Show** was left on after a restart.	Switch it off in **More Settings** — see 11.4, step 4.
Nothing on screen	No mains power.	Check the supply. The terminal has no internal battery, and recorded events are not lost — see 11.3.

13. Getting help

If a problem persists after working through 12, contact support. Diagnosis is much faster with the following to hand.

- **The terminal's unique identifier**, from the foot of the OnTime home screen (2.1). Where more than one terminal is affected, the identifier of each.
- **What is wrong with each terminal**, described in full rather than summarised.
- **Whether each terminal is switched on and connected to the internet**, and whether its TeamViewer status shows as connected (10.1).
- **Whether power has been recycled** on the affected terminals.
- **Whether the problem affects everyone or only some people**, with examples where you have them.
- **A screenshot or a short video** of the problem, if it can be captured.
- **For a network problem**, the network name, the security type shown on the terminal, the exact wording of any message on screen, and — where a username is required — the reason recorded in your authentication server log.

Who to contact

Support for these terminals runs through RLDatix, and the route depends on which stage you are at.

Stage	Route
Within Project Implementations	Contact the relevant RLDatix Implementation Programme Representative by email, or use the Cube Purple Implementations portal.
Business as usual	Contact the RLDatix support team through their support portal.

> **ClockedIn**
>
> ClockedIn is owned and provided by Cube Purple Limited, Suite 6 Empingham House, Uppingham Gate, Uppingham, LE15 9NY
>
> Telephone 0203 865 0960 · etimeclocks.uk