Site Sign In — Administrator Guide

Oct 4, 2026 · @Jess

A plain-language guide to the Site Sign In admin console: checking who is on site, fixing a stuck sign-in, keeping hosts and sites current, and getting badge printing going again. No command line needed for anything in here.

Getting in

The console lives at `https://<your server>:8443/admin`, and you open it from a staff machine. The kiosk deliberately has no link to it — a kiosk is a public terminal, so administration does not belong on it.

Sign in with your own email address and password. At your first sign in you will be asked to set a real password and to scan a QR code into an authenticator app (Google Authenticator, Authy, 1Password and Bitwarden all work). **Save the eight recovery codes somewhere you can get to without your phone** — each works once.

Two roles:

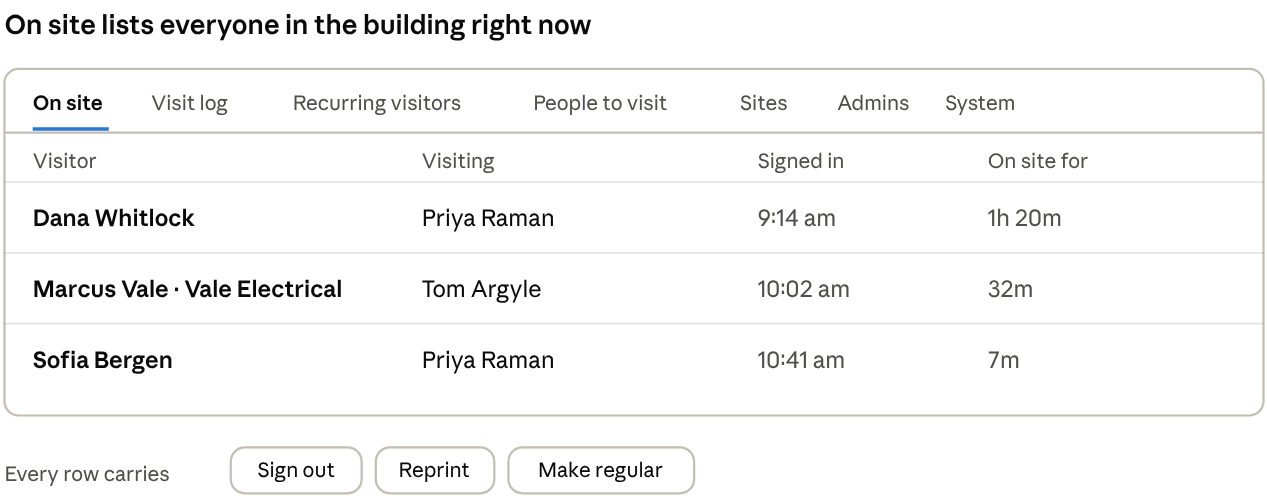
Role	Can do
Owner	Everything, including adding admins and sites
Admin	Day-to-day work; can be limited to a single site, and then sees only that site's visitors, staff list and log

If you are locked out, six wrong passwords locks that email address for 15 minutes. An owner can reset another admin's password (a temporary one appears on screen) or clear their two-factor so they can re-enrol on a new phone.

A browser certificate warning means that machine does not yet trust the local authority. Install it from **System → Certificate**, or browse to `http://<your server>:8080/ca.crt`.

Who is on site right now

On site is the tab you will live in. It lists everyone currently signed in, with their host, the time they arrived and how long they have been here.



the On site tab · placeholder visitors

Three things you can do from each row:

- **Sign out** — for the visitor who walked out without touching the kiosk.
- **Reprint the badge** — for a jam, a mis-feed, or a badge left on a desk.
- **Make regular** — turns a guest into a recurring visitor. It takes their name, company, mobile, email and check details straight from the visit, issues a PIN and opens the printable card. Their sign-in photo is kept as their profile photo, so from the next visit the kiosk skips the camera. The button only appears for someone who gave a mobile number.

The matching offsite copy is the **On site now** tab of the Google Sheet. It is rewritten in full every time anyone signs in or out, so it holds current occupants only, never history. The top row shows the head count and the time it was last updated — if that time is stale, the writes are queuing.

Visit log holds the complete history: searchable (it matches on company, so you can pull up every visit from one contractor) and downloadable as CSV. That history stays in the application and is never sent to Google.

Anyone still showing as on site at `AUTO_SIGNOUT_TIME` is closed off automatically overnight.

Keeping the lists current

Two lists need an eye kept on them: the people a visitor can ask for, and the regulars who sign in with a PIN.

People to visit. Pick a site, then paste or upload your staff CSV (`docs/hosts-sample.csv` shows the shape). This is the list the kiosk offers a visitor, so a departed staff member left on it is the usual cause of a badge naming the wrong host.

Recurring visitors. Each saved person is one record, and their mobile number, email address and PIN must all be unique. The mobile number is the username; the PIN is four digits.

To do this	Use this
Issue a fresh random PIN	**New PIN** on the list
Set a specific PIN, or read back the current one	**Edit** — leave the PIN box blank to keep the current one
Stop someone signing in, but keep their record	Untick **Active** in Edit
Delete them for good	**Remove** — the PIN stops working and the stored photo goes
Stop the kiosk asking them to pose	Add a photo in Edit, from the camera or a file

Removing someone keeps their visit history: visits store the name, contact details and host in their own columns. It does **not** sign them out if they are currently on site — the confirmation says so, and their visit can still be closed at the kiosk with their last name and mobile number.

Five wrong PINs locks that mobile number for 15 minutes. Saving the record clears the lockout, under both the old and the new number.

WWCC and VIT expiry. Give a recurring visitor an expiry date and the console watches it. Inside 28 days the row turns amber; past the date it turns red, a count appears on the **Recurring visitors** tab, and a banner sits across the top of every screen. Nothing is blocked automatically — an expired check is a conversation at the desk, not a door the software slams.

Expiry colours the row: amber inside 28 days, red once it has passed

1 check has expired and 1 expires soon

Visitor	Mobile	PIN	Check	Expires	Warning
Jenna Pike	0412 555 109	4821	WWCC	14 Mar 2027	
Rob Castellan	0403 221 784	7390	VIT	19 Oct 2026	15 days
Amy Thorne	0431 908 552	1264	WWCC	2 Sep 2026	**expired**

Nothing is blocked automatically — the colour is a prompt to have a word at the desk.

recurring visitors · one expiring, one expired

Settings worth knowing

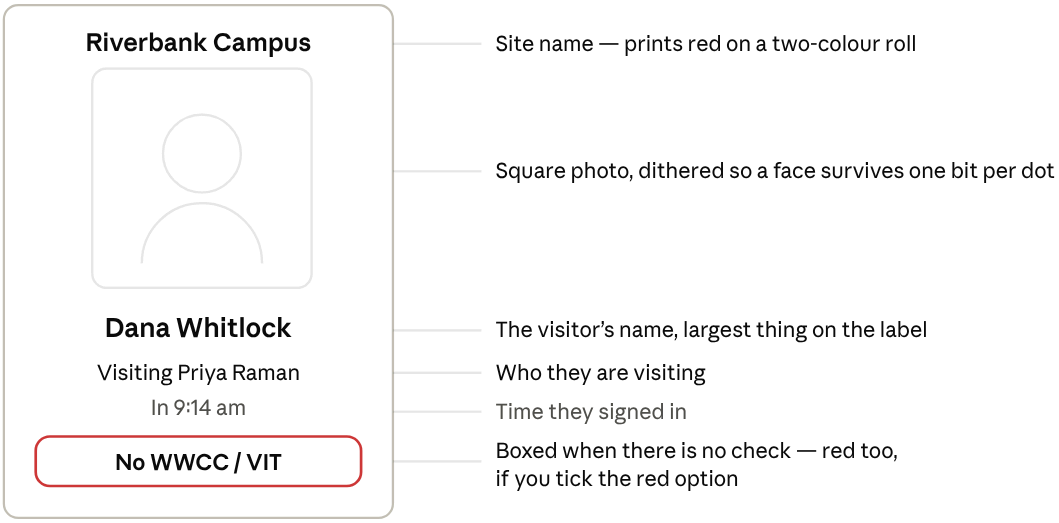
Almost everything a site needs sits under **Sites → Edit**. Each site has its own staff list, its own badge settings and its own look.

Setting	What to know
Badge printing	Turn it on per site. With *Print from the server* ticked, the server renders the badge and pushes it to the printer, so the kiosk tablet needs no driver and shows no print dialog
Roll loaded in the printer	Must match what is physically in the machine. This is the single most common cause of a refused job
Label stock	A shortcut that fills in size, roll type and colour option. It is not itself saved, which is why it can appear to revert
Rotation	0° lays the badge across the 62 mm width; 90° turns it for a label that hangs from its short edge. Check the bitmap preview — only one will suit how you hang them
Photo settings	Error diffusion is the default and much the best for faces. *Preview the photo settings* renders a real visitor photo at several settings side by side

Setting	What to know
Banner and colours	PNG with a transparent background, up to 2 MB. The editor shows the contrast ratio as you type — aim for 7:1 on a screen people read standing up

Before committing a new roll, use **Bitmap preview** (shows the exact image that will be sent) and **Test print** on the site card.

The badge: name and host large, check status unmissable



a 62 × 90 mm badge · placeholder visitor

The evacuation sheet

The Google Sheet exists for one job: so somebody standing in a car park can see who is in the building. Check it from **System → Test the sheet connection**, which also shows the service account address and the last successful write.

Bookmark the sheet on the phones that would actually be used in an evacuation, and confirm it loads **for them**, not just for you. Check it again occasionally — a revoked key or changed sharing queues rows silently, and the head count and *Updated* time in the first row are the giveaway.

When badges stop printing

First, the reassuring part: **sign in still completes**. The visitor is recorded, the kiosk falls back to its own browser print dialog, and the failure is shown against the site in **Sites** with the reason. You can reprint any badge from the **On site** list.

Work through these in order — the first two account for nearly every case.

1. **Does the roll setting match the roll?** Open **Sites → Edit → Printer** and compare *Roll loaded in the printer* with what is actually in the machine. A DK-22251 must be set as the black/red roll even when nothing on the badge is red. The printer's own message — *Black/Red on White paper is installed now. Change it to Monochrome media* — sounds like a driver setting but means swap the roll or fix this field.
2. **Continuous or die-cut?** `62` means a continuous roll cut to length; `62x100` means pre-cut labels. Sending one to the other kind is refused as a wrong roll.
3. **Can the printer be reached?** It needs a fixed IP — a DHCP lease change silently stops badges. Check the address under **Sites → Edit → Printer**.
4. **Press Test print** on the site card. A failed test shows the printer's own words rather than a summary, and **Diagnostics** shows exactly what would be sent.
5. **Ask the printer what it has loaded**, on the docker host:

   ```
   docker compose exec visitor-signin node scripts/printer-status.mjs
   ```

   The QL-820NWB is write-only over port 9100, so it often will not answer. When it doesn't, **Brother Status Monitor on a PC with the printer installed** gives the exact reason a job was refused — more than anything on the server can tell you.
6. **Still stuck?** `docker compose exec -it visitor-signin node scripts/print-probe.mjs` sends one label per roll id and asks you after each whether anything came out. The `-it` matters: it needs a terminal.

Everything else that goes wrong

What you see	What it means	What to do
Browser warns about the certificate	That device does not trust the local authority	Install it from **System → Certificate**. On iPad there is a second, separate step: Settings → General → About → Certificate Trust Settings
Sheet says *The caller does not have permission*	The spreadsheet was never shared with the service account	**System** shows the address. Share the sheet with it as **Editor**. This is the cause nine times in ten
Head count on the sheet looks stale	Writes are queuing	**System** shows the last successful write and any error. Rows retry every minute and are never lost
An admin cannot sign in	Six wrong passwords locks the address for 15 minutes	Wait, or have an owner reset the password
An admin lost their phone	Their authenticator is gone	An owner clears their two-factor; they re-enrol at next sign in
A regular's PIN is rejected	Five wrong attempts locks that mobile number for 15 minutes	Open their record and save it — that clears the lockout
The kiosk asks which site it is on	It was never pointed at one	Visit `http://<server>:8088/?site=<site-slug>` once; the tablet remembers
Someone is still on site who left hours ago	They never signed out	Sign them out from the **On site** list. `AUTO_SIGNOUT_TIME` catches the rest overnight

Two things to be careful with

Changing `APP_SECRET` makes every stored PIN unreadable. If it has to change, reissue PINs from the console afterwards.

Starting a new certificate authority means every kiosk device has to trust the new one. *Renew the server certificate* is the safe option and touches no devices.

If you edit `.env` on the host, bring the container back with `docker compose up -d`, not `docker compose restart` — restart reuses the old environment and the change appears to do nothing.

Created by: Jess Rogerson (yelling commands at Claude.AI)