

Technical Architecture

OnTime, AirStack and HealthRoster Interaction

Architecture, Connectivity, Protocols, Security and Resilience

Document Control	
Prepared by	Cube Purple Limited
Version	1.0
Date	21 August 2026

1. Purpose and Scope

This document is the standing technical reference for how OnTime, AirStack and HealthRoster interact. It covers the architecture and the data exchanged across each interface, site connectivity, hosting and boundaries, the protocols and integration method used, security controls and encryption in transit, and resilience and failure handling.

It is intended to be shared with any organisation using ClockedIn products alongside HealthRoster.

► A note on naming

- ClockedIn is the time and attendance brand owned by Cube Purple Ltd. OnTime and AirStack are its customer-facing products.
- The RLDatix workforce system is referred to here as HealthRoster, the name used throughout the system's own configuration. Organisations that refer to it internally as Optima should read the two names as interchangeable.

2. System Overview

Three systems exchange data to deliver time and attendance: OnTime (the clocking application running on ClockedIn SmartHub devices on site), AirStack (the ClockedIn middleware), and HealthRoster (RLDatix's workforce system). A fourth system, CPAir, manages the device software only and carries no customer data — see 2.2.

The architecture and the data passed across each interface are shown in Figure 1 on the following page.

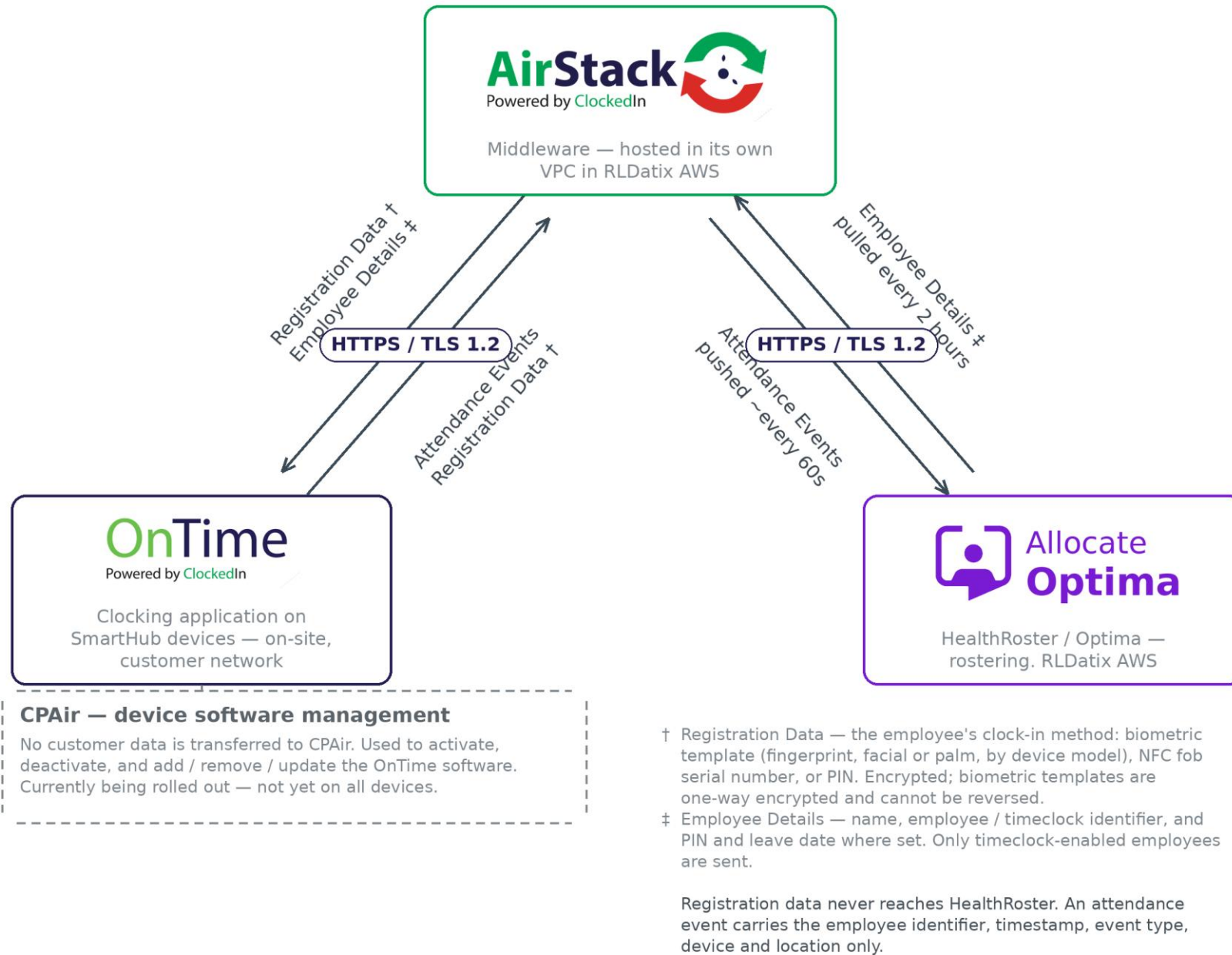


Figure 1 — OnTime / AirStack / HealthRoster architecture, data flow and transport.

2.1 Component summary

Where each component is hosted is set out in 5.1.

Component	Role
OnTime	Clocking application running in locked kiosk mode on ClockedIn SmartHub hardware. Supports biometric, NFC fob and PIN clocking.
AirStack	Middleware: receives attendance events and registration data from OnTime devices, provides the admin and reporting web portal, and exchanges data with HealthRoster. Master record for attendance events. Each organisation has its own installation — see 5.4.
HealthRoster	RLDatix workforce system. Master record for employee identity; consumer of attendance events.
CPAir	Cube Purple's device software management platform — see 2.2. No customer data.

2.2 CPAir

No customer data is transferred to CPAir. It is used to manage the OnTime software on the device — CPAir can activate and deactivate the software, and add, remove or update it entirely.

CPAir is being rolled out progressively and is not yet present on all devices in the field.

3. Data Exchanged Between the Systems

This section sets out precisely what data crosses each interface, since the labels on the diagram are necessarily brief.

3.1 Employee details — HealthRoster → AirStack → OnTime

HealthRoster is the master record for employee identity. It sends AirStack only those employees who are timeclock enabled — that is, employees who have a unique timeclock identifier recorded against them. Employees without one are not passed to AirStack at all.

For each of those employees, the fields exchanged are:

- Name.
- Employee timeclock identifier — the unique identifier that makes them timeclock enabled.
- PIN, where one has been set — optional.
- Leave date, where one has been set — see 7.2. Where the field is empty, nothing is transferred in its place.

No other information forms any part of this exchange. AirStack pulls only what has changed since the last synchronisation rather than requesting the full employee list each time. Every record received is tagged within AirStack as having originated from HealthRoster, so its provenance remains traceable.

AirStack passes the employee's name, identifier and PIN (where set) on to OnTime.

3.2 Registration and distribution of clock-in methods

An employee can clock using a PIN, an NFC fob or a biometric.

- PIN — created in HealthRoster or in OnTime.
- NFC fob — the fob's serial number. Registered in OnTime.
- Biometric template — fingerprint, facial or palm, depending on the device model. Registered in OnTime.

Where a method is registered at a device, it is sent from that device to AirStack over HTTPS/TLS 1.2, encrypted to AES 256. AirStack then distributes it to other timeclocks, according to the configured radius and distribution settings, so the employee can clock at those devices without having to register again.

3.3 Attendance events

AirStack is the master record for clock events. An event is captured at the device and sent to AirStack, where it is stored the moment it arrives. A background process then forwards new events to HealthRoster approximately every minute.

Only the essentials travel with each event:

- Employee identifier.
- Timestamp.
- Event type — clock in or clock out.
- Device and location.

3.4 What never reaches HealthRoster

Registration data does not cross into HealthRoster. Biometric templates and fob serial numbers are held between the OnTime devices and AirStack only; an attendance event identifies the employee by their identifier alone (see 3.3).

4. Site Connectivity — How the Devices Connect

4.1 Network options

The ClockedIn SmartHub devices are Android-based industrial tablets running OnTime in locked kiosk mode. Each device connects to a network chosen by the organisation — Cube Purple does not provide or manage a dedicated network for the devices.

Depending on the device model and the site, connectivity is provided by one of the following:

- Wi-Fi — the most common method; the device connects to the organisation's nominated wireless network.
- Wired Ethernet — where the device model has an Ethernet port.
- Micro wireless access point (WAP) — some models have no Ethernet port. Where a wired connection to the network is preferred or required, a micro WAP is installed locally to bridge the device onto that connection.
- Mobile data SIM — some models support a data SIM, used where no suitable network is available at the installation point.

Whichever method is used, the chosen network must permit the outbound destinations and ports set out in 6.1.

► Important — confirm network coverage before installation

- Network coverage must be checked at each proposed installation location before the devices are installed.
- A device positioned at the edge of Wi-Fi or mobile coverage is the most common cause of intermittent connectivity, and is best resolved at survey stage rather than after go-live.

4.2 Direction of connections

While data travels in both directions, every connection is opened by the device. Nothing on the internet — and nothing at Cube Purple or RLDatix — opens a connection to a timeclock.

Where an instruction needs to reach a device — an employee removal, a registration to distribute, a software change — it is held at AirStack or CPAir until the device next connects, and returned to the device in the reply. This is why an instruction issued while a device is offline is not delivered at the time it is issued, and is re-sent until the device confirms it (see 4.3).

Remote support works on the same principle: the device maintains an outbound connection to TeamViewer's servers, and a support engineer's session request is relayed down that existing connection rather than being made directly to the device.

4.3 Behaviour when the network is disrupted

A reliable and stable network connection gives the best result: with a constant connection, attendance events are sent to AirStack in almost real time.

If the network is disrupted, events are not lost. The device stores them locally and automatically transmits them once the connection is restored. Instructions travelling the other way are handled on the same principle — an employee-removal instruction issued while a device is offline is re-sent by AirStack every 24 hours until the device confirms it has been actioned.

5. Hosting, Infrastructure and Boundaries

5.1 Where each component sits

Layer	Location	Detail
OnTime devices	On-premises	ClockedIn SmartHub hardware on the organisation's chosen network (see 4).
AirStack	Cloud server	RLDatix AWS VPC.
HealthRoster	Cloud server	RLDatix AWS VPC.
CPAir	Cloud server	Cube Purple VPS. Device software management, entirely separate from the AirStack and HealthRoster hosting. No customer data (see 2.2).

AirStack and HealthRoster are hosted separately within RLDatix's AWS environment.

The network topology is shown in Figure 2 on the following page.

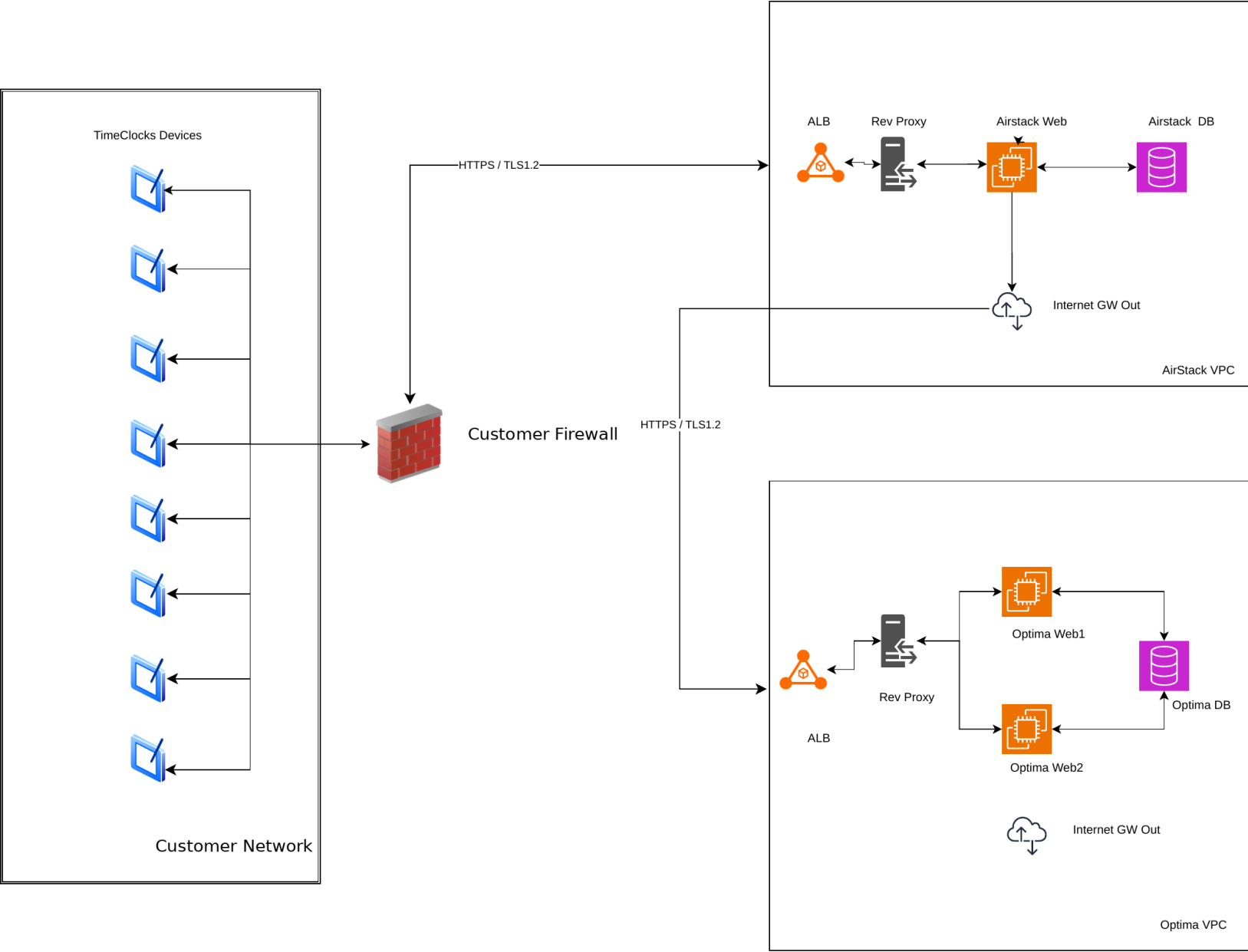


Figure 2 — AirStack and Optima AWS network topology. Source: RLDatix.

5.2 AWS infrastructure

The following is provided by RLDatix, who host and operate both environments.

- AirStack sits in its own VPC. Traffic arrives at an AWS Application Load Balancer, passes through an NGINX reverse proxy, and is directed to the correct AirStack installation by host header via the IIS bindings on the AirStack web server. The web server is backed by its own database.
- Access to the environment is controlled by AWS security groups.
- Outbound traffic from AirStack leaves through the VPC's internet gateway.
- HealthRoster sits in a separate Optima VPC, fronted by its own load balancer and reverse proxy, with two web servers and a database behind them.
- Patching of the AirStack server follows RLDatix's standard patching regime, in line with the HealthRoster servers.

5.3 Resilience of the hosted environment

Overnight snapshots of the AirStack server are taken. In the event of a failure the backup is restored and the server recreated, within the agreed service level.

5.4 Instance model, environments and updates

- Each organisation has its own AirStack installation, addressed by its own host header. Live and pre-production installations are hosted on the same RLDatix AirStack infrastructure.
- Updates are deployed only after approval from the organisation, ideally following user acceptance testing.
- A pre-production (PPD) AirStack instance is provided explicitly for UAT. Timeclock units can be configured to communicate with the PPD instance for testing purposes, so changes can be validated on real hardware before being approved for the live instance.

6. Protocols, Ports and Integration Method

6.1 OnTime device interfaces

The following outbound access is required from whichever network the devices are placed on.

Interface	Destination	Port(s) / protocol	Notes
OnTime ↔ AirStack	AirStack (RLDatix cloud) — attendance events, registration data, employee details	HTTPS / TLS 1.2	Requires unrestricted outbound access, or direct communication with AirStack where a fully open policy is not possible. Specific host/URL/IP requirements available from RLDatix Support.
OnTime → CPAir	https://cpair.uk/login (198.244.229.71)	TCP/443 (HTTPS)	Device software management only — no customer data (see 2.2).
OnTime → Google Play services	play.google.com, android.com, *.gstatic.com, *.ggpht.com, googleapis.com and related Google endpoints	TCP/443; TCP+UDP 5228–5230 (android.com)	Required for app registration/updates and the location-radius distribution of clock-in methods. Full host list in the OnTime Network Requirements document.
Remote support	TeamViewer master servers (*.teamviewer.com)	UDP/TCP 5938 (primary), falling back to TCP 443 then TCP 80	Used by the Cube Purple / RLDatix service desk for remote support and OnTime software deployment. Device-initiated outbound only (see 4.2).

6.2 AirStack ↔ HealthRoster

AirStack and HealthRoster are connected by a single secure web link over HTTPS, encrypted in transit using TLS 1.2. This is standard TLS, not mutual TLS: AirStack connects to the full external HealthRoster URL in the same way an end user would.

Authentication is session based. AirStack signs in to HealthRoster and is issued a temporary session pass, which it reuses for subsequent requests rather than authenticating on every call. If that session expires, AirStack signs in again automatically; no manual intervention is required.

What is exchanged, and in which direction, is set out in 3.1 and 3.3.

6.3 Synchronisation frequency

Data	Typical frequency	How it runs, and manual options
Attendance events	Approximately every 60 seconds, plus an automatic retry sweep every 10 minutes for anything that failed	Runs continuously as a background process. Individual events can be resent from within AirStack; bulk resends are handled by the Cube Purple development team.
Employee details	Every 2 hours	Runs automatically in the background. Can also be triggered manually within AirStack.

6.4 Delivery confirmation, retry and failure handling

Attendance events are delivered using a two-way handshake. When AirStack sends an event to HealthRoster, HealthRoster confirms back that it has been received, and the event is then displayed as received within AirStack. This gives a positive, auditable confirmation of delivery for every event rather than an assumed one.

- Events are stored in AirStack the moment they arrive, so a delivery problem delays data rather than losing it.
- Anything that fails to send is picked up automatically by the retry sweep that runs every 10 minutes.
- Every attempt, successful or not, is logged, giving a complete audit trail for any individual event.
- Outright rejections generate an email alert to staff, so a failure is never silent.
- Where intervention is needed, an individual event can be resent from within AirStack; bulk resends are handled by the Cube Purple development team.

7. Security, Encryption and Data Retention

7.1 OnTime devices and the OnTime ↔ AirStack interface

Registration data of every type — biometric templates, fob serial numbers and PINs — is encrypted, and traffic between the devices and AirStack is carried over HTTPS/TLS 1.2.

► Biometric templates are encrypted one way and cannot be reversed

- A biometric template is encrypted in one direction only. Cube Purple cannot decrypt a template or reverse it back to the original biometric.
- Matching is performed against the encrypted string itself, not against the biometric capture. The system compares encrypted values; it does not reconstruct or compare fingerprints, faces or palms.
- It is therefore not possible to recover an image of an employee's biometric from anything held on the device, in AirStack, or in transit between them.

The wider control set on the device and this interface is as follows:

- Android OS-level security: Linux kernel protections and secure inter-process communication between applications. Devices are unrooted, retaining the manufacturer's original security controls.
- Devices run in locked kiosk mode — only Super Admin access can exit the OnTime application — and are physically secured within a locked kiosk enclosure, mitigating access to physical ports.
- No inbound connections are accepted by the device; all traffic runs over sessions the device opens (see 4.2).
- Approximate payload sizes: an attendance event is 2–3KB; a biometric template is 20–25KB.
- Firewall policy on the chosen network remains the organisation's own.

7.2 Data retention in AirStack

AirStack does not hold time and attendance data indefinitely. All attendance data is removed automatically once a defined retention period has elapsed. That period is controlled by the organisation and configured within AirStack; the default is 3 months. A longer period is not generally required, because attendance events are passed to HealthRoster (see 3.3), which holds the record used for rostering and pay.

Employee data — including registration data of every type, role and historical clock data — is fully removed from AirStack and OnTime when an employee leaves. Removal is triggered automatically on the leave date set in HealthRoster, or can be carried out manually in AirStack. Both routes support UK GDPR compliance.

7.3 Hosted data

- Data held in the AWS-hosted environment is stored securely within a SQL database.
- Biometric information is encrypted using AES 256.
- Access to the hosted environment is restricted to an approved remote desktop gateway.

7.4 AirStack ↔ HealthRoster

Transport encryption and authentication for this interface are set out in 6.2. No biometric or registration data crosses it (see 3.4).

8. Resilience and Failure Handling

This section consolidates, for reference, the resilience behaviour described elsewhere in this document.

8.1 Resilience behaviour — summary

- Device to AirStack: events are stored locally on the device and sent automatically when the connection returns (4.3).
- AirStack to HealthRoster: every event is positively confirmed; failures are retried automatically every 10 minutes, all attempts are logged, and outright rejections raise an email alert (6.4).
- Instructions to a device: re-sent every 24 hours until the device confirms (4.3).
- Device unable to connect at all, and therefore unable to receive instructions: contact RLDatix Support.
- Change validation: a pre-production AirStack instance allows changes to be proven on real hardware before reaching live (5.4).
- Most common site-level cause of intermittent connectivity: marginal network coverage at the device location (4.1).
- Hosted environment: recovery is by restore from the overnight snapshot (see 5.3).

8.2 Single points of failure

The two points at which a fault stops data moving, rather than delaying it, are the site network and the AirStack server itself. Neither results in the loss of attendance events:

- Site network — events are held on the device and sent when the connection returns.
- AirStack server — restored from the overnight snapshot, with any events already held on the devices delivered once it is back in service.