



Technical Reference

Installation, network and service

Version 1.1.0 · 2026

Contents

1. About this document

- 1.1 What RiNGY is
- 1.2 What RiNGY is not
- 1.3 Principle of operation

2. Hardware

- 2.1 Controller
- 2.2 The bell output
- 2.3 Behaviour across a restart
- 2.4 The backup cell

3. Network

- 3.1 What the device needs
- 3.2 Addressing
- 3.3 Outbound connections
- 3.4 Concurrency

4. Security

- 4.1 Two ways in, two different credentials
- 4.2 Accounts and roles
- 4.3 Sessions
- 4.4 What is never exposed

5. Time

- 5.1 Where the time comes from
- 5.2 The trust ladder

6. Certificates

- 6.1 What is installed by default
- 6.2 The browser warning
- 6.3 Tamper detection

7. Storage and data

- 7.1 Flash layout
- 7.2 The schedule file
- 7.3 What a factory reset erases
- 7.4 There is no configuration backup
- 7.5 Fault log

8. Software updates

- 8.1 The bundle
- 8.2 How an update proceeds
- 8.3 Rules that matter in practice
- 8.4 If an update goes wrong

9. Diagnostics

- 9.1 First questions
- 9.2 The fault state
- 9.3 What to send with a support request

10. Specifications and limits

- 10.1 Schedule
- 10.2 Factory schedule
- 10.3 Access
- 10.4 Network and update
- 10.5 Time

11. Integration

1. About this document

This is the reference for whoever installs, connects and services a RiNGY unit - the electrician who wires it, the school's IT contact who puts it on the network, and support staff diagnosing a fault.

It does not repeat the User Manual. Anything a teacher or secretary does - building a timetable, declaring a day off, importing holidays - is there, and only there. This document covers what is underneath.

1.1 What RiNGY is

RiNGY switches your school's existing bell circuit on a schedule. It is a controller and a switch: it closes a contact for a few seconds at each bell time, and the school's own bell, horn or siren does the sounding.

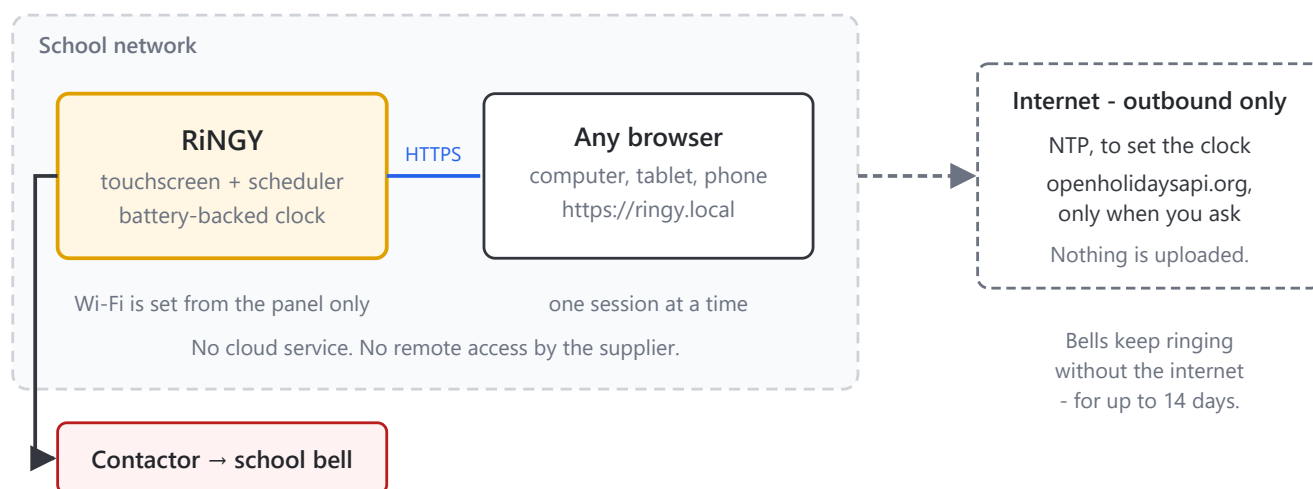
1.2 What RiNGY is not

There is no sound hardware. No speaker, no amplifier, no audio files, no melodies, no SD card. RiNGY has no way to produce a tone. If your school needs different sounds, that is a property of the bell you connect, not of RiNGY.

There is no cloud service. The device is administered directly over the school network. It reaches the internet only to set its clock and, once a year if you ask it to, to fetch the official holiday calendar. Nothing is uploaded anywhere.

There is no remote access by the supplier. No tunnel, no relay, no backdoor account that reaches in from outside. Support happens on site or over the school's own network.

1.3 Principle of operation



A scheduler task wakes once per second, compares the current minute against the bell list resolved for today, and on a match asks the bell task to close the relay for the configured duration. The clock is held by a

battery-backed real-time clock and corrected over the network. If the clock cannot be trusted, RiNGY stops ringing rather than ring at the wrong time - see chapter 5.

2. Hardware

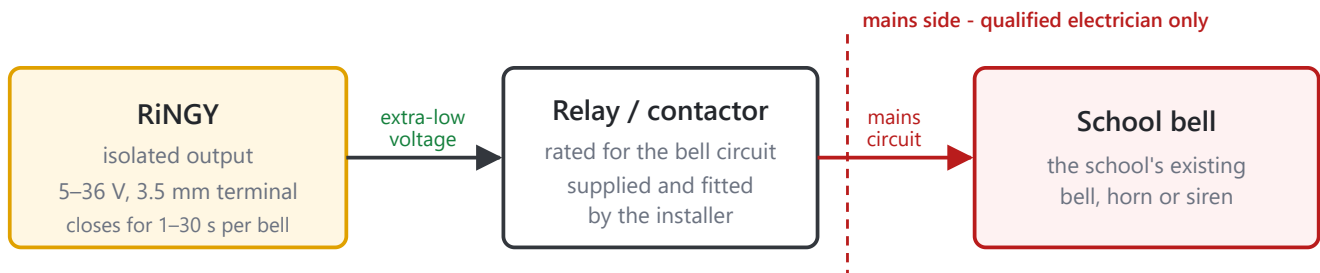
2.1 Controller

Module	ESP32-S3-WROOM-1
CPU	Xtensa LX7 dual core, up to 240 MHz
Flash	16 MB
PSRAM	8 MB octal
Board	Waveshare / Spotpear ESP32-S3-Touch-LCD-4.3B
Display	4.3 in, 800 × 480, 65 K colour, RGB interface
Touch	GT911 capacitive, 5-point, I ² C
Real-time clock	PCF85063 with CR927 backup cell
I/O expander	CH422G
Wireless	2.4 GHz Wi-Fi 802.11 b/g/n

The full board schematic and the component datasheets are published by the board vendor at spotpear.com and files.waveshare.com.

2.2 The bell output

The bell is driven from an **isolated digital output** on the carrier board, rated by the vendor for **5–36 V**, presented on a 3.5 mm screw terminal. Firmware drives it through the CH422G expander as an open-drain output, active low.



RiNGY never carries the bell current.

It closes a low-voltage contact. The relay or contactor between it and the bell circuit does the switching, and must be rated for that circuit and installed to local regulations.

THE OUTPUT IS A SWITCH, NOT A SUPPLY

The isolated output switches a circuit; it does not power one. It must not be connected directly to a mains bell. Between RiNGY and a mains bell circuit there must be a relay or contactor rated for that circuit, installed by a qualified electrician and in accordance with local regulations.

INSTALLATION DATA NOT COVERED HERE

The supply voltage, current draw, contactor rating, terminal labelling, enclosure dimensions and any CE marking are properties of the assembled RiNGY product rather than of the controller board, and are supplied separately by CulTech. This chapter documents the interface, not the installed assembly.

Front-panel manual override

The assembled product adds two controls that the firmware neither reads nor knows about:

Control	Function
AUTO ON/OFF rotary selector	Chooses whether the firmware's output or the manual button drives the bell circuit
Red push-button	Rings the bell directly while pressed

In the **OFF** position the firmware continues to run the schedule normally - the scheduler task fires, the log records the ring, `GET /api/bell/status` reports it - but the output does not reach the bell. **Nothing in the API, the log or the UI reflects the selector position**, because the firmware has no sense line for it. A support call reporting "the schedule stopped working, but the screen looks fine" should establish the selector position before anything else is investigated.

This is deliberate: the manual path stays available when the controller is wedged, mid-update or unpowered at the logic side, which is precisely when a school still needs to ring periods.

2.3 Behaviour across a restart

A reboot - whether from a software update, a manual restart or a watchdog - does not power-cycle the I/O expander. A device that restarted mid-ring would come back with the contact still closed, so the first hardware action of every boot is to force the bell output off, before the display, the network or anything else is brought up.

2.4 The backup cell

A CR927 3 V lithium cell keeps the real-time clock running while the unit is unpowered. RiNGY judges the cell's health from evidence rather than voltage: at each cold boot it checks whether the clock actually held the time across the outage.

State	Meaning
unknown	Not yet assessed
unverified	No cold-boot evidence observed yet
ok	The cell demonstrably held time across a real power cut
service_due	Past its replace-by date; still working
failed	Proven not to hold time; sticky until the cell is replaced

`service_due` is informational - nothing stops working. `failed` means that after a power cut the device will come up with no idea of the time and will not ring until the network gives it one.

3. Network

3.1 What the device needs

A 2.4 GHz Wi-Fi network with internet access. RiNGY takes an address by DHCP. It does not support 5 GHz, WPA-Enterprise, or captive portals.

Wi-Fi is configured only from the touchscreen. There is no web endpoint for it and no access-point mode, by design: a device that could be re-pointed at another network over the network would be a device an attacker could take away from you.

Credentials are written to storage only after the device has successfully associated *and* received an IP address, so a mistyped password can never destroy working credentials.

3.2 Addressing

Name	<code>ringy.local</code> , advertised by mDNS
Protocol	HTTPS on port 443 by default
Port 80	Redirects to HTTPS with a 301
Fallback	HTTP on port 80 if no valid certificate exists

The Info screen shows the current IP address alongside the name. If `ringy.local` does not resolve - some networks block mDNS, and some Android versions do not implement it - use the address directly. Reserving a fixed lease for the device on the school's DHCP server is worth doing for exactly this reason.

3.3 Outbound connections

Destination	Purpose	Frequency
<code>pool.ntp.org</code> , <code>time.google.com</code> , <code>time.cloudflare.com</code> (UDP 123)	Clock synchronisation	Periodic
<code>openholidaysapi.org</code> (TCP 443)	Official Bulgarian holiday calendar	Only when requested, plus once on 1 December

Nothing else leaves the device. If the school firewall blocks NTP, the clock will drift out of trust within 14 days and the bells will stop - see 5.2.

3.4 Concurrency

The device serves **four TLS sockets**. Under load it answers `503 Service Unavailable`, which is a normal operating condition and not a fault; the web interface retries on its own. This matters if you plan to poll the device from a monitoring system: keep it to one request at a time.

4. Security

4.1 Two ways in, two different credentials

Surface	Credential	Protects
Touchscreen	PIN, 4–6 digits	Schedule changes, Wi-Fi, settings
Web interface	Username and password	Everything the account's role allows

Stopping a ringing bell and triggering the emergency mode deliberately need **no** PIN. Everything else on the panel does. Three wrong PIN entries lock the keypad for 30 seconds.

4.2 Accounts and roles

Role	Who	Can
<code>client</code>	The school	Everything in day-to-day operation and scheduling
<code>service</code>	CulTech support	The above, plus firmware updates, certificates, logs, user management and factory reset

The school account is created by **claiming**: the first person to reach the web interface of an unclaimed device sets the username and password. After that the claim screen disappears. An unclaimed device on a school network is claimable by anyone on that network, so claim it during installation, not later.

4.3 Sessions

Mechanism	HttpOnly session cookie, <code>SameSite=Strict</code>
Concurrent sessions	One
Lifetime	1 hour
Storage	RAM only - every session ends at a restart
Login rate limit	5 attempts per 60 seconds, then <code>429</code>

One session at a time is a real constraint, not a rounding. A second successful login evicts the first. If two people administer the device at once, one of them will be signed out without warning.

4.4 What is never exposed

The PIN, account passwords and the TLS private key are never returned by any endpoint, in any form. Passwords and PINs are stored hashed. Log output routes untrusted values through a sanitiser so that a password typed into the wrong field cannot end up in the log.

5. Time

5.1 Where the time comes from

At boot RiNGY reads the battery-backed clock, then corrects it from the network. Both are needed: the network gives accuracy, the backup cell gives continuity across a power cut.

The time zone is a POSIX specification, factory-set to `EET-2EEST,M3.5.0/3,M10.5.0/4` - Bulgarian time with automatic summer-time changeover. Changing it takes effect immediately, and a malformed string is rejected with HTTP 400 rather than accepted: the C library treats an unparseable zone as UTC without reporting an error, which on this device would mean every bell ringing two or three hours out with nothing in the log to say why.

Summer and winter time

The backup clock holds **UTC only**, and the scheduler asks the C library for local civil time once a second. The offset is therefore re-derived continuously from the zone rules, and a changeover needs no restart and no reconfiguration. Bell times are stored as local wall clock, so 08:00 stays 08:00 on both sides of a transition.

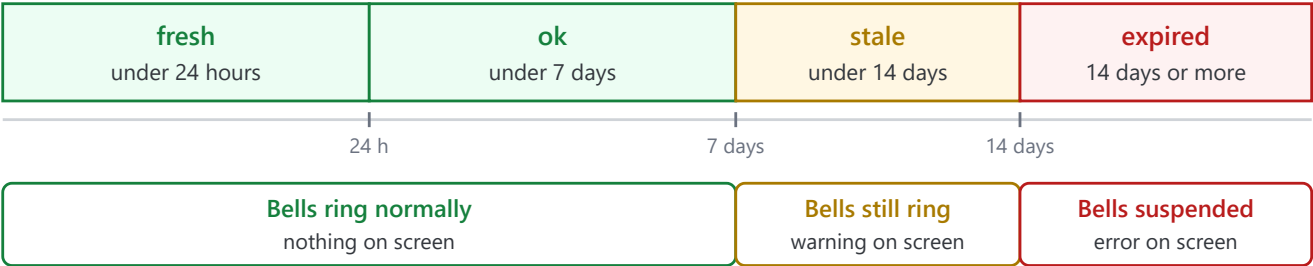
Two consequences follow from a changeover, both by design and both on a Sunday:

Transition	Effect
Last Sunday in March, 03:00 → 04:00	Local 03:00–03:59 does not occur, so a bell scheduled inside that hour does not ring. There is no catch-up: a bell fires in its own minute or not at all
Last Sunday in October, 04:00 → 03:00	Local 03:00–03:59 occurs twice. The fired-minute bitmap is keyed on minute-of-day and is cleared only when the day number changes, so the second pass is suppressed and no bell rings twice

Neither is configurable, and neither has ever mattered in practice: both fall on a Sunday, in the small hours, and a school day contains no bells at that time.

5.2 The trust ladder

Time since the clock was last confirmed against the network



Losing Wi-Fi does not stop the bells. Losing it for a fortnight does.
A bell at the wrong time disrupts every lesson in the building; a bell that does not ring gets reported.

RiNGY tracks how long it has been since the clock was last confirmed against the network, and lets that govern whether it is willing to ring.

Level	Age of last synchronisation	Scheduled bells
fresh	under 24 hours	Ring normally
ok	under 7 days	Ring normally
stale	under 14 days	Ring, with a warning on screen
expired	14 days or more	Suspended
unconfirmed	Clock never confirmed this boot	Suspended
none	No usable clock at all	Suspended

This is deliberate. A school bell that rings at the wrong time is worse than one that does not ring: the first disrupts every lesson in the building, the second is noticed and reported. The device announces the condition on screen well before it stops.

Losing Wi-Fi does not stop the bells. Losing Wi-Fi *for a fortnight* does.

6. Certificates

6.1 What is installed by default

On first boot the device generates its own certificate and keeps it in a dedicated storage area, separate from the rest of its settings.

Algorithm	ECDSA P-256, self-signed
Validity	10 years
Subject alternative name	Includes <code>ringy.local</code>
Basic constraints	<code>CA:TRUE</code> , so it can be installed as a trusted root
Private key	Never leaves the device

6.2 The browser warning

Because the certificate is self-signed, browsers cannot verify it and will warn on every first visit. The connection is still encrypted; what the browser cannot do is prove the device's identity.

Three ways to resolve it, in order of preference:

1. **Install the device certificate as trusted** on the machines that administer RiNGY. Download it from Settings → Security, then install it into the operating system or browser trust store. The warning disappears permanently.
2. **Upload your own certificate**, if the school already runs an internal certificate authority. Settings → Security accepts a certificate and key in PEM form.
3. **Accept the warning each time.** Workable, and teaches staff to click through security warnings, which is a habit worth not teaching.

`Strict-Transport-Security` is deliberately sent with `max-age=0` . With a self-signed certificate, HSTS would remove the user's ability to click through - and would lock the school out of its own device the day the certificate is rotated.

6.3 Tamper detection

A fingerprint of the certificate is recorded separately from the certificate itself. If the two stop matching, the device reports a suspected tamper in Settings → Security rather than carrying on quietly.

7. Storage and data

7.1 Flash layout

16 MB, partitioned as follows.

Partition	Type	Size	Holds
<code>nvs</code>	NVS	24 KB	Wi-Fi credentials, PIN hash, time zone, language, account hashes, emergency-mode flag
<code>otadata</code>	OTA	8 KB	Which application slot boots
<code>phy_init</code>	PHY	4 KB	Radio calibration
<code>ota_0</code>	app	4 MB	Firmware slot A
<code>ota_1</code>	app	4 MB	Firmware slot B
<code>fatfs_react_0</code>	FAT	2 MB	Web interface, slot A
<code>fatfs_react_1</code>	FAT	2 MB	Web interface, slot B
<code>storage</code>	SPIFFS	1 MB	Schedule, settings, pending holidays, fault log
<code>coredump</code>	coredump	256 KB	Reserved
<code>certs_nvs</code>	NVS	64 KB	TLS certificate and private key

Firmware and web interface are held in **paired** slots and swapped together, so the two can never be mismatched after an update.

7.2 The schedule file

`schedule.json` and `settings.json` are written atomically: the new content is written to a temporary file, the previous version is kept as a backup, and only then is the new file put in place. An interrupted write - a power cut mid-save - leaves a recoverable state that is repaired at the next start.

7.3 What a factory reset erases

Factory reset is a **service-role** action. It restores the factory schedule and settings, resets the time zone, clears the record of the last clock synchronisation, clears the touchscreen setup flag, PIN and language, **deletes the school account**, clears the Wi-Fi credentials, returns the device to HTTP, and erases the certificate store.

The device then needs to be set up from scratch, including reclaiming the account, exactly as if it were new. It is not a troubleshooting step.

The same reset can also happen **by itself**. If the settings store is found to be corrupt at start-up, the device clears it and continues rather than refusing to start, and comes up in the setup wizard with no Wi-Fi, no account and no PIN. A unit that "came back blank" after a power event has almost certainly done this; the reason is recorded in the fault log once the unit is reachable again.

7.4 There is no configuration backup

RiNGY has no export or import of its configuration. What exists is a restore of the *factory* schedule, which preserves the time zone, working days and ring duration. A school that has built an elaborate timetable should keep its own record of it.

7.5 Fault log

A persistent log of warnings and errors is held in the storage partition, capped at approximately 64 KB across two rotating files. The logger stops writing rather than let the log fill the partition and prevent a schedule from being saved. It is readable and downloadable by the service role from Settings → System.

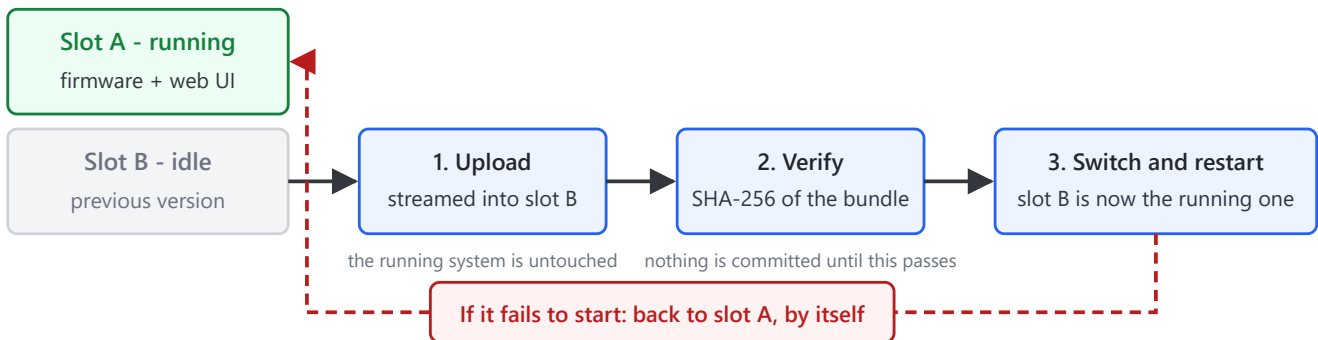
8. Software updates

8.1 The bundle

An update is a single `.sbu` file carrying both the firmware and the web interface, with a SHA-256 over the whole thing. Bundles are between 100 KB and 8 MB.

8.2 How an update proceeds

The device holds two complete copies. One runs; the other is written to.



Automatic rollback covers a firmware that will not start. A firmware that starts but misbehaves needs a manual rollback.

1. The bundle is uploaded through Settings → Software by a service-role session.
2. It is streamed directly into the **inactive** application and web slots. The running system is untouched.
3. Nothing is committed until the hash of the complete bundle verifies.
4. The boot selector is switched and the device restarts.
5. On the next boot the new firmware must complete its start-up. If it does not, the bootloader **automatically returns to the previous version**.

An update can therefore fail safely at every stage. The version that was working is still present in the other slot throughout.

8.3 Rules that matter in practice

- **Update outside teaching hours.** The device restarts, and a restart during a scheduled bell is a missed bell.
- **One upload at a time.** A second concurrent upload is refused.
- **An upload stalls out.** If the connection dies mid-upload, the transfer is abandoned after 60 seconds of silence, or 11 minutes overall, and the device recovers on its own.
- **The device refuses a new upload while the current firmware is still unverified.** Let it finish booting and confirm itself first.

8.4 If an update goes wrong

The automatic rollback covers a firmware that fails to start. It does **not** cover a firmware that starts cleanly but misbehaves - nothing can detect that automatically. A manual rollback to the other slot exists for that case and is available to the service role. It is deliberately not exposed in the interface, because "go back one version" is not a decision to offer under a stress.

9. Diagnostics

9.1 First questions

Symptom	Where to look
No bell at a scheduled time	Day type on the dashboard; the day's bell list on the Schedule screen
Bells stopped entirely	Clock trust - see 5.2. Check Wi-Fi and NTP reachability
Status shows <code>fault</code>	9.2
Web interface unreachable	mDNS - try the IP from the Info screen. Then check port 443
Signed out unexpectedly	Someone else signed in. One session at a time - see 4.3
Time wrong by exactly one hour	Time zone, not the clock

9.2 The `fault` state

`fault` means the bell output could not be confirmed to have switched off after retrying for about a minute. It is reported as a distinct state precisely because reporting it as `idle` would be a lie - and one that could leave a bell ringing while the screen says everything is fine.

On seeing `fault` : check whether the bell is physically silent. If it is still sounding, cut power to the bell circuit at the distribution board and investigate the wiring and the contactor. A restart clears the state; it does not clear the cause.

9.3 What to send with a support request

- The firmware version, from Settings → Software or the Info screen
- The device's MAC address, from the Info screen
- The downloaded fault log, if the service role is available on site
- What the screen showed, and what the bell did
- Whether the clock was showing a warning

10. Specifications and limits

10.1 Schedule

Bells per day plan	60
Named day plans	5, plus the default plan
Dated exceptions	40
Ring duration	1–30 seconds, factory 5
Bell label length	63 characters
Exception label length	95 characters
Screen sleep	0 (never) to 3600 seconds, factory 60

10.2 Factory schedule

Seven 40-minute lessons from 07:30, 10-minute breaks except 15 minutes after the third lesson: 14 bells between 07:30 and 13:15, Monday to Friday, 5-second ring.

10.3 Access

PIN	4–6 digits; 3 attempts then a 30-second lockout
Web password	Minimum 8 characters
Username	Up to 31 characters
Concurrent sessions	1
Session lifetime	1 hour
Login rate limit	5 attempts per 60 seconds

10.4 Network and update

Wi-Fi	2.4 GHz 802.11 b/g/n, WPA/WPA2-PSK or open
Concurrent TLS connections	4
Networks listed per scan	40
Update bundle	100 KB – 8 MB
Upload idle timeout	60 seconds
Upload total budget	11 minutes

10.5 Time

Clock source	PCF85063 RTC, CR927 backup cell, corrected by NTP
Bells suspended after	14 days without synchronisation
Time zone	POSIX string, factory <code>EET-2EEST,M3.5.0/3,M10.5.0/4</code>

11. Integration

RiNGY serves a JSON API over the same HTTPS interface the web application uses, so a school that already runs a management system can read status and drive the bell from it.

The essentials:

Method and path	Purpose
<code>POST /api/login</code>	Sign in; returns a session cookie
<code>GET /api/status</code>	Version and network state; no session needed
<code>GET /api/bell/status</code>	Bell state, day type, clock trust, next bell
<code>POST /api/bell/test</code>	Ring once, for the configured duration
<code>POST /api/bell/panic</code>	Enable or disable the emergency mode
<code>GET /api/schedule/today</code>	The bell list in force today
<code>POST /api/schedule/today</code>	Override today: day off, or apply a plan

Three things will catch out a first integration:

- Every state-changing request needs both `Content-Type: application/json` and `X-Requested-With: XMLHttpRequest`. Without the second, the request is rejected as cross-site.
- `503` means busy, not broken. Retry.
- Signing in from a script signs out whoever is using the web interface.

The complete endpoint reference, with every request and response shape, is available from CulTech on request.