



LMP SH-IP & HRNL-25W REST API REFERENCE

Public visual integration guide

DATASHEET

REST API

v1.3.0 RELEASE | BUILD 310

www.xichtee.com
office@xichtee.com
Company ID: 56695284
Tax ID / VAT: 2122403635



Document control

DOCUMENT	VALUE
Title	LMP SH-IP & HRNL-25W REST API Reference
Document revision	8.13
Firmware baseline	v1.3.0 · Release · build 310
Issued	2026-10-05 · Europe/Bratislava

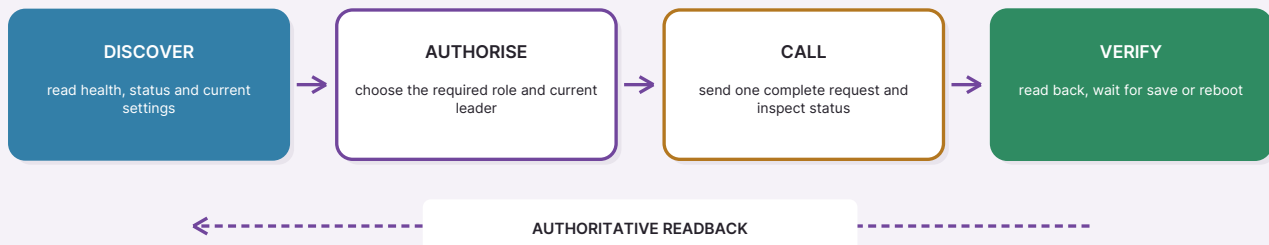
Purpose

This guide describes the public HTTP API for LMP SH-IP and HRNL-25W. Each endpoint lists its method and path, access requirements, parameters, response formats, save behaviour, retry guidance, and verification steps. It also identifies legacy endpoints that change state through GET.

NOTE Later firmware versions may add response fields. Ignore unknown JSON fields, handle the documented error codes, and check the live firmware/build through `/api/health` before using version-specific behaviour.

HOW TO USE THIS REFERENCE

The same external workflow applies to every endpoint family



A response confirms only the phase documented for that operation.



DATASHEET

LMP SH-IP & HRNL-25W

REST API REFERENCE

Contents

Document control	2
Contents	3
01 · Start here	4
02 · Conventions and lifecycle	7
03 · Endpoint directory	11
04 · System health and live status	13
05 · Rules, colour and scheduling	18
06 · Presets and Custom Effects	21
07 · Logic Matrix	25
08 · Device, segments and network	29
09 · Reading Cluster settings	33
10 · Updating Cluster settings	35
11 · Cluster setup and recovery	38
12 · Backup and restore	40
13 · Firmware update	45
14 · HTTP responses and errors	49
15 · Limits and security	51



01 • Start here

Base URL

```
http://${DEVICE_IP}:${HTTP_PORT}
# HTTP_PORT defaults to 80
```

IMPORTANT The device serves native HTTP. Use it only on an isolated trusted management LAN, or through a trusted external HTTPS boundary. HTTPS provides confidentiality, integrity and server authentication; native HTTP does not.

HTTP TRANSACTION ANATOMY

Exact readiness exchange; CR LF terminates every line

CLIENT TO DEVICE	90 BYTES		DEVICE TO CLIENT	90 BYTES
REQUEST LINE	25 B		STATUS LINE	25 B
GET /api/ready HTTP/1.1			HTTP/1.1 204 No Content	
HOST	18 B		CACHE	25 B
Host: 192.0.2.10			Cache-Control: no-store	
ACCEPT	26 B	REPLY →	CONNECTION	19 B
Accept: application/json			Connection: close	
CONNECTION	19 B		BODY LENGTH	19 B
Connection: close			Content-Length: 0	
HEADER TERMINATOR	2 B		HEADER TERMINATOR	2 B
CR LF			CR LF	

The blank line completes each 90-byte header block. This 204 response has no message body.

192.0.2.10 is a documentation-only address; replace it with the device address.

Authentication

Protected requests use HTTP Basic authentication on each call. There is no bearer-token API. Because the device serves plain HTTP, credentials are not confidential without an external trusted HTTPS boundary.

IMPORTANT Every operation marked **Authenticated**, **User/Admin** or **Administrator** requires credentials for an enabled account. A feature licence or device operating mode never authenticates a request or bypasses its role check. Integrations must send HTTP Basic credentials on every protected call.



DATASHEET

LMPSH-IP & HRNL-25W

REST API REFERENCE

METHOD	CONTRACT
HTTP Basic	Send Authorization: Basic base64(username:password) on every protected request.
Authorisation	The role associated with the supplied account determines whether User or Administrator operations are available.

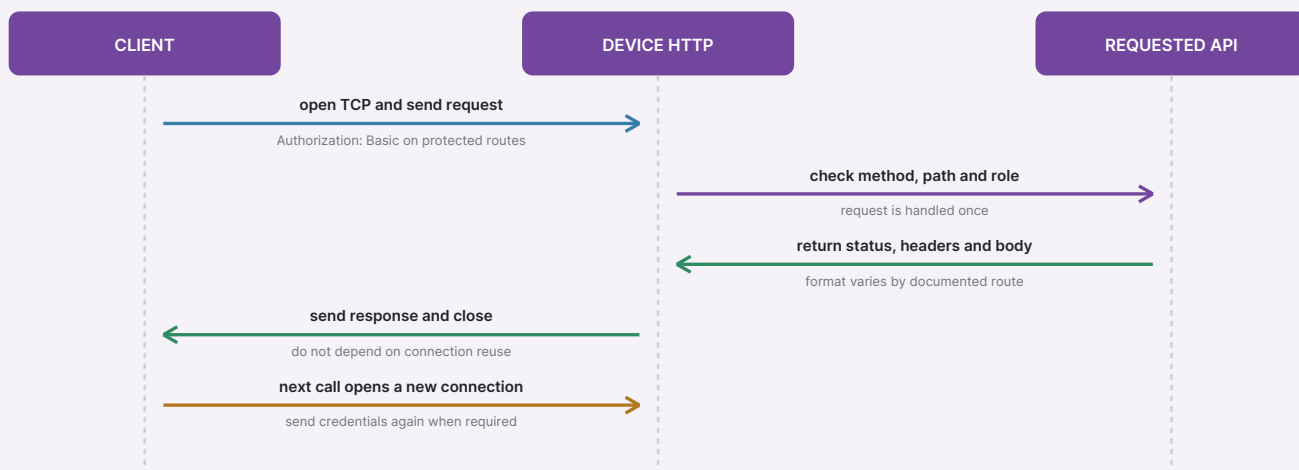
```
# curl prompts for the password; do not place it on the command line
curl --user "${USERNAME}" http://${DEVICE}/api/logic/config
```

IMPORTANT Authentication and authorisation failures are not uniform on all compatibility routes. Check the documented status, Content-Type and response format; never treat an unexpected HTML page as a successful API response.

ROLE / STATE	CAPABILITY
Public	Readiness, health and status are available without authentication.
Authenticated User	Rule, preset and colour controls plus Custom Effect and Logic reads.
Administrator	Persistent configuration, backup/restore, Cluster topology and firmware update.
Cluster Follower	A Follower cannot change the shared application configuration. Device-specific administrator settings remain available.
Backup standby	Read service remains available; writes are accepted only after the Backup has become the active leader and is ready.

PROTECTED REQUEST LIFECYCLE

HTTP Basic accompanies every protected call; there is no API token session



Never place a password in a URL or command line; let curl prompt or use protected credential storage.

Quick read

```
curl -s http://${DEVICE}/api/health
curl -s http://${DEVICE}/api/status
```



DATASHEET

LMPSH-IP & HRNL-25W

REST API REFERENCE

Quick authenticated read

```
# Safe first authenticated call; curl prompts for the password
curl --user "${USERNAME}:" \
  "http://${DEVICE}/api/custom_effect?idx=0"
```

IMPORTANT Some legacy endpoints use GET to change device state, although clients normally treat GET as read-only. For routes marked **LEGACY MUTATING GET**, disable prefetching, check the current state before retrying, and never include secrets in the URL.

BEFORE THE FIRST MUTATION

Treat examples as integration patterns; perform visible-output changes on an isolated bench

VALIDATE

LOCAL

Check strict decimal syntax, indexes, ranges and complete required bodies.

ROUTE

AUTHORITY

Use status to select the current ready Cluster leader before a shared write.

SEND ONCE

MUTATES

Disable prefetch and automatic replay for every state-changing GET.

VERIFY

READBACK

Read the authoritative state and follow the endpoint's save or reboot rule.

Maintained GPI/Logic ownership can override Rule Active; one-shot mappings release ownership after their edge.



02 · Conventions and lifecycle

Transport and representation

ITEM	CONTRACT
Connection	Firmware normally sends Connection: close. Use one request per connection; do not depend on connection reuse.
Request timing	Complete headers within 8 s and an ordinary request within 15 s total, measured from its first received bytes. Later progress does not restart either limit. An expired request is closed without a guaranteed HTTP error response.
JSON	UTF-8 JSON for most APIs. Some compatibility mutations return text, HTML or JSON without a uniform envelope.
Forms	Legacy writes and restore/custom-effect endpoints use URL-encoded query/form fields.
Non-OTA POST framing	Follow the Content-Length rules below. The complete request (headers + body) may be at most 16,381 bytes. A valid positive length that exceeds this request limit returns 413. TCP fragments may split the method, path, headers or body; processing waits for the complete body.
POST Content-Length	Send exactly one Content-Length header. The header name is case-insensitive. Its value must contain decimal digits with a value from 1 to 2,147,483,647; leading zeroes and surrounding spaces or tabs are accepted. Signs, fractions and other trailing characters are not accepted. Only the HTTP header field supplies this length. Endpoint and request-size limits still apply.
Invalid request framing	A missing, zero, invalid, out-of-range or repeated Content-Length is rejected with 411. Transfer-Encoding and folded header lines are also rejected with 411; request-side chunked transfer is not supported.
Cluster body	POST /api/cluster_settings requires Content-Type: application/json and rejects unknown/duplicate fields.
OTA body	POST /api/fw_upload requires a raw, non-multipart UF2 body plus Content-Length. application/octet-stream is the expected media type, but v1.3.0 does not enforce Content-Type.
Indexing	Segment, rule, preset, slot and bank indexes are zero-based unless stated otherwise.
Time	Names ending _ms use milliseconds. uptime_ms is 64-bit; sequence and age counters should be treated as unsigned.
IPv4	Dotted-decimal IPv4. Cluster peers must be usable unicast addresses and satisfy role/IP relationships.

IMPORTANT For legacy GET queries, an empty or malformed integer can become 0, while a missing field normally becomes -1. Validate strict decimal syntax and the documented range before sending the request; do not rely on a 400 response. A malformed request can otherwise target item 0, clear a runtime value or set black RGB.

When an accepted request is not yet saved

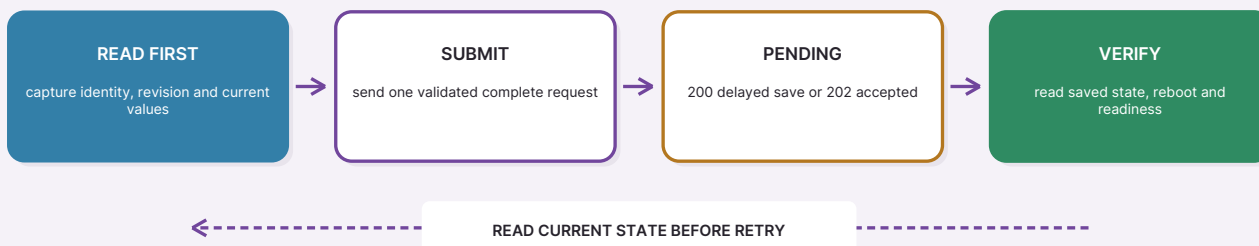
A 202 Accepted response means the device accepted or queued the request. The change may still need to be saved or followed by a reboot. Use the verification steps listed for that endpoint.

PHASE	WHAT THE CLIENT KNOWS	NEXT ACTION
Request accepted	202 or storage=queued	Stop sending writes and read the state back.
Applied in memory	A current GET may show the new values	Do not consider the change saved while pending is true.
Settings saved	Saved settings match the readback	For changes that require a reboot, wait for it.
Device ready	Expected identity, build, topology and ready state are visible	Resume normal traffic.



ACCEPTED IS NOT COMPLETE

A safe client follows every asynchronous operation to an observable finish



Do not send a second write merely because the requested value is already visible in RAM.

Some 200 responses are saved later

The legacy Rule configuration, Rule NTP, Preset, colour/mode and update_config routes return 200 after changing the running configuration. The device saves those configuration changes after the 30-second Web delay. Rule key=0 Active follows the separate automatic retention policy below. Ordinary readback confirms the running value, not that an individual request has been saved. For configuration writes, serialize changes, retain the health save-counter baseline, wait for the quiet period, and require a later successful save with no latched verification fault before relying on the change.

Rule Active retention

Rule Active states are saved automatically and restored at startup from the last verified save. This includes accepted manual, protocol, input and Cluster changes. A maintained GPI or Logic input can replace the restored state with its current result, and an authoritative Cluster master can replace it with current live state.

After an idle period, an Active state that remains unchanged is normally saved after about 30 seconds. Further background Active saves are spaced at least 120 seconds apart. If states keep changing, the device takes a save opportunity after about 120 seconds of unsaved changes. Busy traffic or another save, update or recovery operation can delay saving. These times do not guarantee that a power cut retains every recent change. A configuration save or controlled restart can save the state sooner.

A successful command or current-state readback confirms the running value, not that this particular change has already been saved. The configuration save counters are not a receipt for an individual Active change, and waiting a fixed 30 or 120 seconds is not proof of saving. Reconnect after restart and verify the effective Rule state and physical output. Keep the controller's intended state and refresh it after reconnect or failover when required by the installation.

Controlled restart and power interruption

A controlled restart saves and verifies the Rule Active state captured for that restart before continuing. Stop sending changes once a restart is requested; later changes are not part of that saved snapshot. If saving cannot finish, the restart can remain pending. Sudden power loss or an unexpected reset restores the last verified save, which can be older than the last displayed state. Current maintained inputs and Cluster authority still apply after restart.

IMPORTANT A restore can change the live state before a later save error, and the runtime values may not roll back automatically. Keep authenticated recovery access and a protected backup. After an error, reapply the intended settings or restart the device to restore the last saved configuration before attempting another save.



Retrying requests

When the device returns 503 Service Unavailable with Retry-After: 1, wait at least the advertised interval, then repeat only if the operation is safe to retry in its documented state. HTTP may be temporarily unavailable while configuration persistence or firmware update processing completes. After a connection closes without a complete response, reconnect and read the current state before retrying a state-changing request.

Short API responses allow normal control and monitoring to continue while data is sent. They can end after five seconds without progress or 30 seconds overall. Treat a truncated response as incomplete. Retry a read after a brief pause. If a state-changing request loses its reply, read back the affected settings or operation state before repeating it; the change may already have been accepted.

Web monitor downloads

The Pro-Bel, Ember+ and OSC web monitors return the history captured when a download is accepted. Later traffic does not alter that response. Device control continues while the history is sent.

A history download can return 503 with Retry-After: 1 when another download is active or available capacity is insufficient. Finish or cancel the other download, wait at least one second and retry.

Each monitor history response has a 30-second total transfer limit; continued progress does not extend it. If the connection closes before the complete JSON arrives, discard the partial response and request a new download.

IMPORTANT While Cluster settings are being saved, an API request can return 503 with Retry-After: 1 and `{"error":"cluster_persistence_pending","retry_after_ms":1000}`. The requested operation was not executed; wait, read the relevant state again and retry only when safe.

IMPORTANT A protected state-changing request can return 503 before execution while the device is saving settings. The response includes Retry-After: 1 and may have an empty body; no change was made. Re-read the current state before retrying.



DATASHEET

LMP5H-IP & HRNL-25W

REST API REFERENCE

CLIENT DECISION AFTER A RESPONSE

The HTTP status selects the next safe action; the response body supplies detail

200 SUCCESS

FOLLOW UP

Use the endpoint's save rule; some legacy changes still need 30 seconds.

202 ACCEPTED

PENDING

Stop writing, read pending state and wait for save or reboot.

409 CONFLICT

RECONCILE

Re-read authority, identity, revision and effective values before deciding.

503 BUSY

WAIT

The request was not executed. Honour Retry-After, then re-read before retrying.

A closed or partial response is an unknown outcome: discard partial data and inspect current state.

Cluster authority

IMPORTANT A peer shown as online is not necessarily the active leader. Use `cluster_leader`, `cluster_ready`, and the `Primary/Backup age` fields from `/api/status` when deciding where to send writes.

If this device is not the active Cluster leader, the following public routes return 409 cluster_remote_managed: GET `/api/set_rule`, `/api/set_rule_ntp`, `/api/set_preset`, `/api/set_color` and `/api/update_config`; and POST `/api/custom_effect`, `/api/custom_effect_preview`, `/api/logic/apply`, `/api/restore_leds` and `/api/restore_rules`. Other administrator settings remain available on that device.



03 · Endpoint directory

PUBLIC ENDPOINT LANDSCAPE

Every method and path below is retained in the detailed directory

PUBLIC MONITORING

3 ROUTES

GET /api/ready
GET /api/health
GET /api/status

RULES / COLOUR

3 ROUTES

GET /api/set_rule
GET /api/set_rule_ntp
GET /api/set_color

PRESETS / EFFECTS

4 ROUTES

GET /api/set_preset
GET /api/custom_effect
POST /api/custom_effect
POST /api/custom_effect_preview

LOGIC / DEVICE / NETWORK

7 ROUTES

GET /api/logic/config
GET /api/logic/status
POST /api/logic/apply
GET /api/update_config
GET /set_config
POST /api/ember_consumer/browse
GET /api/ember_consumer/browse

CLUSTER

2 ROUTES

GET /api/cluster_settings
POST /api/cluster_settings

BACKUP / RESTORE

5 ROUTES

GET /api/backup
POST /api/restore_net
POST /api/restore_leds
POST /api/restore_rules
POST /api/restore_special

FIRMWARE

4 ROUTES

GET /api/fw_status
POST /api/fw_upload
GET /api/fw_apply
GET /api/fw_invalidate

Use the directory table for access role, mutation, save/reboot and purpose details.

METHOD	PATH	ACCESS	MUTATES	ASYNC / REBOOT	PURPOSE
GET	/api/ready	Public	No	No	HTTP readiness probe
GET	/api/health	Public	No	No	Versioned health and boot telemetry
GET	/api/status	Public	No	No	Live device, LED and Cluster status
GET	/api/set_rule	User/Admin	Yes	By key*	Mutate one rule property



DATASHEET

LMPSH-IP & HRNL-25W

REST API REFERENCE

METHOD	PATH	ACCESS	MUTATES	ASYNC / REBOOT	PURPOSE
GET	/api/set_rule_ntp	User/Admin	Yes	30 s	Mutate one Rule NTP slot
GET	/api/set_preset	User/Admin	Yes	30 s	Mutate preset/effect fields
GET	/api/set_color	User/Admin	Yes	30 s	Set mode/segment RGB
GET	/api/custom_effect	User/Admin	No	No	Read Custom Effect slot
POST	/api/custom_effect	Admin	Yes	202	Queue Custom Effect save
POST	/api/custom_effect_preview	Admin	Runtime	No	Set/clear live preview
GET	/api/logic/config	User/Admin	No	No	Read Logic configuration
GET	/api/logic/status	User/Admin	No	No	Read Logic live state
POST	/api/logic/apply	Admin	Yes	Queued	Atomically replace one Logic bank
GET	/api/update_config	Admin	Yes	30 s	LED and device-label configuration
GET	/set_config	Admin	Yes	Save/reboot	Network settings and Ember+ consumer
POST	/api/ember_consumer/browse	Admin	No	202/job	Start or cancel a provider browse job
GET	/api/ember_consumer/browse	Admin	No	No	Poll a provider browse job
GET	/api/cluster_settings	Admin	No	No	Read Cluster settings
POST	/api/cluster_settings	Admin	Yes	202/reboot	Validate or replace topology
GET	/api/backup	Admin	No	Stream	Download application backup
POST	/api/restore_net	Admin	Yes	202	Restore network section
POST	/api/restore_leds	Admin	Yes	202	Restore LEDs/presets/legacy timelines
POST	/api/restore_rules	Admin	Yes	202	Restore rules/NTP/Logic
POST	/api/restore_special	Admin	Yes	202/reboot	Restore auxiliary modes
GET	/api/fw_status	Admin	No	No	Read firmware-update state
POST	/api/fw_upload	Admin	Flash	No	Upload firmware image
GET	/api/fw_apply	Admin	Yes	Yes	Apply staged image
GET	/api/fw_invalidate	Admin	Yes	No	Discard staged image

* User/Admin means an enabled User or Administrator authenticated with HTTP Basic. A 30 s entry means the device normally saves configuration changes after the 30-second Web delay; a 200 response does not confirm that the change is saved. For /api/set_rule, key=0 Active follows Rule Active retention in section 02, while keys 1..11 use the configuration delay.



04 · System health and live status

THREE PUBLIC MONITORING SURFACES

Choose the smallest response that answers the monitoring question

/API/READY

ROUTER

204 proves that the HTTP router can answer now; it contains no device state.

/API/HEALTH

HEALTH

Versioned boot, deployment, network, runtime and save evidence.

/API/STATUS

STATE

Live application, segment, auxiliary input and Cluster state.

A complete response is a snapshot. Discard a partial streamed JSON body after a transport close.

Readiness probe

GET`/api/ready`

Public · SAFE · NO-STORE

Use this endpoint to confirm that the device HTTP API is responding. A successful response has no body.

Responses

STATUS	BODY / MEANING	CALLER ACTION
204	No Content	Device HTTP router is responsive.

Health status

GET`/api/health`

Public · SAFE · STREAMED JSON

Returns versioned health data for monitoring and deployment checks.

Public response fields

The fields below are supported for client integrations. Later firmware may add other fields; ignore any that are not listed here.

FIELD	TYPE / MEANING
schema_version	uint32, exactly 1.
uptime_ms	uint64 milliseconds.
fw_version / fw_release_type	Firmware version and release-type strings.
fw_build_number / fw_build_date	uint32 build number / YYYY-MM-DD string.
boot_count / boot_attempts / boot_loop	uint32 / uint32 / Boolean reboot state.
last_reset_code / last_reset	uint32 code / matching reset label.
current_slot / ready_slot / pending_slot	String A or B, or JSON null.



DATASHEET

LMPSH-IP & HRNL-25W

REST API REFERENCE

FIELD		TYPE / MEANING
forensics_degraded / boot_confirmation_degraded		Boolean degraded post-boot evidence states.
bootloader_version / bootloader_build_date		Bootloader identity strings.
bootloader_metadata_valid / bootloader_legacy		Boolean metadata validity / legacy fallback state.
bootloader_metadata_status		String valid, missing or corrupt.
bootloader_build / bootloader_capabilities / bootloader_hardened		uint32 build / capability mask / Boolean.
last_reset_code	last_reset LABEL	
0 / 1 / 2 / 3	Unknown / Power On / Run Pin / Debug	
4 / 5 / 6 / 7	Watchdog / Software Reset / OTA Apply / BOOTSEL	
8 / 9 / 10	Out Of Memory / HardFault / Network Fault	
11 / 12	Factory Reset / Panic	

Operational state

FIELD	TYPE / MEANING
dhcp_bound	Boolean; a DHCP lease is active.
heap_free / heap_min	uint32 current/minimum free memory bytes.
oom / previous_oom	uint32 out-of-memory event counts for this and the previous run.
temp_c	Number in degrees Celsius with one decimal.
cpu0_pct / cpu1_pct	Integer utilisation percentages.
net_w5500_ok / net_w5500_link_up	Boolean network-controller and physical-link state.
net_w5500_speed_mbps / net_w5500_full_duplex	10 or 100 / Boolean.
led_core1_active / led_output_enabled	Boolean renderer and output state.
led_configured_count	uint32 configured LED total.
storage_save_attempts / storage_save_successes / storage_save_failures	uint32 device-global save counters.
storage_save_last_completed_ms	uint32 uptime timestamp of the latest completed save attempt.
storage_save_last_result	uint32: 0 none, 1 success, 2 busy, 3 too large, 4 overlap, 5 no safe slot, 6 verify failed, 7 queued, 8 waiting, 9 aborted.
storage_verify_retry_count / storage_verify_retry_after_ms	uint32 retry count / remaining backoff milliseconds.
storage_verify_fault_latched	Boolean; true means automatic persistence retries have stopped.

NOTE An erased legacy bootloader metadata page reports version 1.0, date 2025-12-20 and status missing. Present but invalid or executable-mismatched metadata reports unknown and corrupt; never treat that as the legacy identity.



DATASHEET

LMP5H-IP & HRNL-25W

REST API REFERENCE

Responses

STATUS	BODY / MEANING	CALLER ACTION
200	Complete JSON response	Check the firmware version and build number, then read the fields you need.
503	Temporary busy response, possibly with Retry-After: 1	Wait for the advertised interval and retry the complete request.
closed	No response or incomplete JSON	Discard the partial body and retry after service returns.

IMPORTANT Save counters are device-global, not request identifiers. Serialize changes and compare a before/after health snapshot. If storage_verify_fault_latched is true, automatic retries have stopped: treat the write as failed, preserve recovery access and correct the cause before retrying.

Live application and Cluster status

GET	/api/status	Public · SAFE · STREAMED JSON
-----	-------------	-------------------------------

Returns the current LED configuration, application state, auxiliary inputs and Cluster status.

Public response fields

The fields below are supported for client integrations. Later firmware may add other fields; ignore any that are not listed here. Auxiliary values and the Ember+ consumer age explicitly marked below can be JSON null.

IDENTITY / STATE FIELD	TYPE / MEANING
dev_name / dev_type_name	Device name and family strings.
dev_type	Integer: 0 LMP5H-IP, 1 HRNL-25W.
mode / hrnl_view	Integer operating and HRNL display modes.
seg_hw / seg_lic / seg_active / probe_targets	Integer hardware, licensed, active-segment, and Pro-Bel target counts.
cpu0 / cpu1 / ram / fls	Integer percentages.
temp	Number in degrees Celsius with one decimal.
last_reset / last_reset_code	Reset label / uint32 code.
boot_attempts / boot_loop	uint32 / Boolean.

Network and auxiliary state

FIELD	TYPE / MEANING
mode1_kind / mode2_kind	String gpi or sensor.
mode1_gpi_state / mode2_gpi_state	Boolean in GPI mode; otherwise JSON null.
mode1_temp_c / mode2_temp_c	Number °C when sensor status is ok; otherwise JSON null.
mode1_temp_status / mode2_temp_status	disabled, starting, ok, disconnected, crc_error, invalid or stale.
dhcp / ip	Boolean configured DHCP mode / live IPv4 string.
time / date / ntp_ok	Local time string / date string / synchronisation Boolean.
mqtt_lic / mqtt_en / mqtt_ok	Boolean licence, configured, and connection state.
mqtt_ip / mqtt_port	Broker host string / integer port.
mgmt_en / mgmt_port	Management service Boolean / integer port.



Outbound Ember+ consumer status

ember_consumer FIELD	TYPE / MEANING
state	disabled, backoff, opening, connecting, browsing or monitoring.
error	none or a stable lower-case reason such as not_configured, not_licensed, not_authoritative, no_socket, connection_lost, protocol_error, streaming_unsupported, value_unsupported or value_stale.
enabled / configured / socket_allocated / licensed	Boolean configuration, validity, allocation and feature state.
socket	Integer network-socket index; -1 when none is allocated.
authoritative / connected / monitoring	Boolean local-control, TCP and active-monitoring state.
available / stale / online	Boolean value usability, freshness and inherited remote online state.
value_type	none, boolean, integer or real. The public status response deliberately omits the monitored value.
age_ms	uint32 milliseconds since the last accepted value, or JSON null before any value.
reconnects / protocol_errors	uint32 counters.

Cluster authority and presence

FIELD	TYPE / MEANING
cluster_lic / cluster_en	Boolean licensed / configured enabled.
cluster_role / cluster_role_name	0 Off, 1 Primary, 2 Backup, 3 Follower / matching label.
cluster_leader	String none, primary or backup.
cluster_ready / cluster_transfer	Boolean readiness / synchronisation-in-progress state.
cluster_peers / cluster_hash / cluster_live_seq	Configured peer count / uint32 configuration hash / live sequence.
cluster_primary_age_ms / cluster_backup_age_ms	uint32 authoritative ages; unseen is 4294967295.
cluster_primary_health_age_ms / cluster_backup_health_age_ms	uint32 monitoring ages; unseen is 4294967295.
cluster_primary_seen / cluster_backup_seen	Boolean peer presence observed from accepted authoritative or HEALTH traffic; never authority proof.
cluster_primary_online / cluster_backup_online	Boolean recent authoritative-or-monitoring presence; never use alone as authority.
cluster_peer_seen_mask / cluster_peer_online_mask	uint32 follower bitmasks.
cluster_peer_ready_mask / cluster_peer_sync_mask	uint32 follower bitmasks.
cluster_peer_primary_leader_mask / cluster_peer_backup_leader_mask	uint32 follower-leader bitmasks.
cluster_failovers	uint32 runtime count of witnessed Primary-to-Backup authority promotions. One promotion counts once whether cluster_leader changes directly from primary to backup or briefly reports none. Startup or reinitialisation with only Backup available does not count.
cluster_sync_started / cluster_sync_completed / cluster_sync_aborted	uint32 synchronisation counters.

Nested application state

ARRAY	SHAPE
segments	Length seg_lic. Each object: n name; c LED count; h effective #RRGGBB; r effective 'R,G,B'; hc configured #RRGGBB.
presets	Fixed length 10. Each object: r,g,b integers; n string; sa,sd,st; ea,ed,et; ca,cd,ct,ct2 integers; ctx string; amch,amch2,amt1,amt2 integers; amc1,amc2,amc3 #RRGGBB strings.
rules	Outer length seg_lic; five objects per segment. Each object: a 0 1; p; ti (-1 disables); tb; o string; om; on,ox numbers; os string; gi 0 Disabled, 1 GPI1, 2 GPI2, 3..12 Logic1..10; ip,im 0 1.



NOTE On a Primary or Backup, bit i in each peer mask represents followers[i]. Follower devices return zero masks. Do not use online presence alone to choose the leader.

Responses

STATUS	BODY / MEANING	CALLER ACTION
200	Complete JSON response; no-cache	Read the complete object and ignore unknown fields.
503	STATUS_SNAPSHOT_BUSY or another temporary busy response	Follow Retry-After: 1 and retry the complete request.
closed	No response or partial JSON	Discard the body and retry after service returns.

READING CLUSTER STATUS CORRECTLY

Presence helps monitoring; leadership and readiness route control writes

CURRENT LEADER

AUTHORITY

cluster_leader names primary, backup or none. It is the first routing signal.

READY

CONTROL

cluster_ready must be true and cluster_transfer false before normal writes resume.

AUTHORITATIVE AGE

LEASE

Primary/Backup age fields show recent accepted control traffic.

SEEN / ONLINE

MONITOR

Can include HEALTH-only presence. Useful for display, never sufficient for authority.

On masters, follower-mask bit i maps to followers[i]; Follower devices return zero masks.

Authority expiry

Remote authority expires after 1.5 seconds without accepted LIVE or valid configuration traffic, including valid retries. Rejected malformed or stale configuration packets do not postpone failover. It remains expired until fresh traffic from the configured master is accepted; monitoring presence alone does not restore authority. A Backup must be ready and wait at least 1.5 seconds after Cluster service starts before takeover.

Backup recovery during synchronisation

A Backup reports ready only after the complete application configuration and Custom Effects are verified. If synchronisation is interrupted, it restores the last complete verified configuration and Custom Effects before takeover. The restored configuration can be older than the Primary's latest change.

During recovery, the device can remain online for monitoring while cluster_ready=false. Incoming traffic changes neither readiness nor accepted live values. Management reads remain available; synchronisation can retry after recovery.

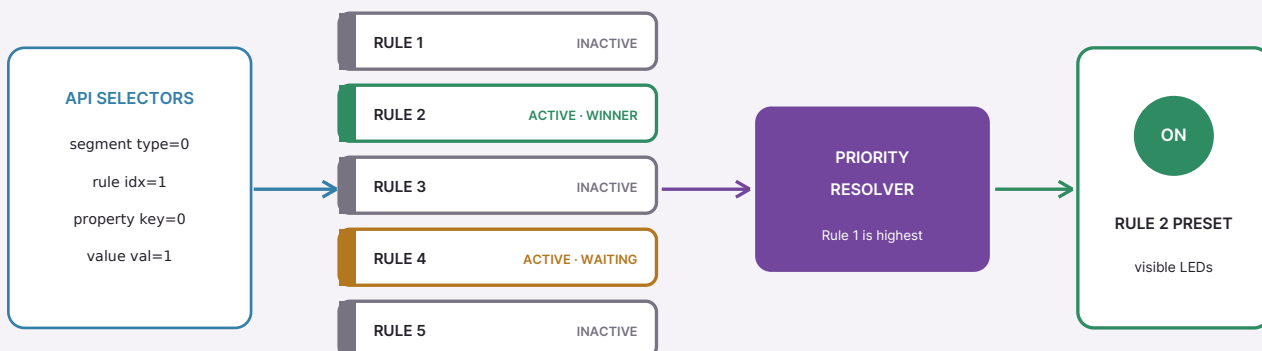
Do not treat cluster_transfer=false or an online indication as completion. Read cluster_leader, cluster_ready and cluster_hash together. Require the intended hash before considering the latest configuration replicated.

IMPORTANT If the saved recovery configuration cannot be verified, the device remains unready and does not accept control writes or become the Cluster leader. Check storage_verify_fault_latched in /api/health, preserve available backups and seek technical assistance.

05 · Rules, colour and scheduling

RULE CONTROL AND VISIBLE OUTPUT

Example: Rules 2 and 4 are active; the lower-numbered Rule 2 wins



Changing Active updates runtime state. Keys 1–11 change configuration and use the Web save delay.

A maintained GPI/Logic input may own Active; always confirm the authoritative readback.

Set one Rule property

GET

/api/set_rule

Authenticated · LEGACY MUTATING GET · CLUSTER-GATED

Changes one Rule property. The endpoint returns plain text OK even if an out-of-range index prevents the change, so validate indexes before sending the request. Active (key 0) follows the automatic retention policy in section 02; configuration keys 1..11 are saved after the 30-second Web delay.

Parameters

NAME / LOCATION	TYPE · REQUIRED	RULES / MEANING
type · query	integer · required	Zero-based segment; must be within licensed maximum.
idx · query	integer · required	Rule index 0..4.
key · query	integer · required	Property selector below.
val · query	string/number · required	Value interpreted by key; percent-encode strings.

IMPORTANT If type, idx, key, or numeric val is present but empty or malformed, the device interprets it as 0. A malformed selector can therefore target segment 0 / Rule 0 / key 0 and clear Active. Enforce strict decimal syntax and endpoint ranges before sending.

KEY	PROPERTY	VALUE / CONSTRAINT
0	active	0/1; saved automatically under the section 02 retention policy. Rejected with 409 when the Cluster master owns live rules; a maintained GPI or Logic input may override this value.



DATASHEET

LMPSH-IP & HRNL-25W

REST API REFERENCE

KEY	PROPERTY	VALUE / CONSTRAINT
1	preset_id	Preset slot 0..9; any other value becomes 0.
2 / 3	tsl_index / tsl_bit	Stored index -1 (disabled)..9999, clamped at ends; bit 0..3. TSL 3.1 input addresses only 0..126, so larger indexes cannot match a received TSL 3.1 message.
4	osc_path	Decoded string, maximum 63 bytes.
5	osc_match_mode	0 Trigger (>0.001), 1 Exact numeric A, 2 Range A..B, 3 String; invalid becomes 0.
6 / 7	osc_arg_min / osc_arg_max	Float. Malformed/missing val becomes 0.0 for key 6 and 1.0 for key 7.
8	osc_arg_str	Decoded string, max 31 bytes.
9	input source	0 disabled, 1 GPI1, 2 GPI2, 3..12 Logic outputs 1..10.
10 / 11	inverted / one-shot	1 enables the behaviour; other values disable it.

Responses

STATUS	BODY / MEANING	CALLER ACTION
200	text/plain OK	Read /api/status for the effective running state. For Active, follow section 02; this is not a saving acknowledgement. For keys 1..11, wait for the configuration delay and verify saving.
403	license_required	Address only licensed segments.
409	cluster_remote_managed	Send the live write to the active Cluster master.

Configure one scheduled Rule action

GET	/api/set_rule_ntp	Authenticated · LEGACY MUTATING GET · CLUSTER-GATED · 30-S SAVE
-----	-------------------	---

Updates the supplied fields for one of the two schedule slots. The device validates all schedule values and immediately re-evaluates the current local time.

Parameters

NAME / LOCATION	TYPE · REQUIRED	RULES / MEANING
seg (or type) · query	integer · required	Zero-based licensed segment.
idx · query	integer · required	Rule 0..4.
slot · query	integer · required	0 or 1; exactly two action slots exist.
mode · query	integer · optional	0 Disabled, 1 Once, 2 Daily, 3 Weekly; a value above 3 becomes Disabled.
action · query	integer · optional	0 Set FALSE/OFF, 1 Set TRUE/ON; >1 becomes slot default (slot 0 true, slot 1 false).
days · query	integer · optional	0..127 Weekly mask: bits 0..6 Monday..Sunday; higher bits stripped. Zero never fires.
minute · query	integer · optional	Local minute-of-day 0..1439 (00:00..23:59); >1439 becomes 0.
date · query	integer · optional	Once date as decimal YYYYMMDD; valid years 1970..9999. Omitted stays current; an invalid value becomes 0 and never fires.

Each value field is optional. Omitted or negative values leave the setting unchanged; an invalid supplied value is interpreted as 0. Scheduling uses NTP time and the configured time zone. After a valid request, the device checks both slots. Defaults are both Disabled; slot 0 action true, slot 1 false; days=127; minute=0; date=0. Send only values within the documented ranges.



Responses

STATUS	BODY / MEANING	CALLER ACTION
200	text/plain OK	A 200 response does not prove valid or saved schedule values. An Administrator may verify them through a securely handled backup; v1.3.0 has no User-accessible REST schedule readback.
403	license_required	Use a licensed segment.
409	cluster_remote_managed	Send the configuration change to the ready leader.

Set LED mode and segment colour

GET	/api/set_color	Authenticated · LEGACY MUTATING GET · CLUSTER-GATED · 30-S SAVE
-----	----------------	---

To change either the mode or a segment colour, send all three r, g and b parameters. If any value is missing, the endpoint makes no change.

Parameters

NAME / LOCATION	TYPE · REQUIRED	RULES / MEANING
r, g, b · query	integer · required for any change	Supply all three. The supported range is 0..255; values are not clamped. An empty or malformed supplied component is interpreted as 0.
mode · query	integer · optional after RGB	Zero-based active segment mode; changed only when licensed and valid. A malformed supplied mode is interpreted as 0.
seg · query	integer · optional after RGB	Zero-based segment; a malformed supplied seg is interpreted as 0.

Responses

STATUS	BODY / MEANING	CALLER ACTION
200	text/plain OK, including when no value changed	Read /api/status, wait for the save delay and verify the configuration.
403	license_required	Use a licensed mode or segment.
409	cluster_remote_managed	Send the change to the ready leader.



06 · Presets and Custom Effects

PRESET BEHAVIOUR ANATOMY

Each of ten presets combines colour with start, constant and stop behaviour

BASE RGB

COLOUR

The segment colour copied by apply-style controls and used by the preset.

START PHASE

ENTRY

Effect, direction and duration used when the preset becomes visible.

CONSTANT PHASE

VISIBLE

Static, looped, Morse, Audio Monitor or Custom Effect behaviour.

STOP PHASE

EXIT

Effect, direction and duration used when the preset loses priority.

Preset slot indexes are 0–9. Custom Effect modes map to values 10–19.

Update a preset

GET /api/set_preset

Authenticated · LEGACY MUTATING GET · CLUSTER-GATED · 30-S SAVE

Updates the supplied fields in preset slot 0..9. Omitted fields are unchanged; accepted changes are saved after the 30-second delay.

Parameters

NAME / LOCATION	TYPE · REQUIRED	RULES / MEANING
idx (or id) · query	integer · required	Preset slot 0..9; idx takes precedence.
r, g, b	integer · optional	Preset RGB; supported range 0..255.
name	string · optional	Decoded name, max 31 bytes; empty does not clear through this route.
sa, ea	mode · optional	Start/stop: 0 Instant, 1 Wipe, 2 Blink, 3 Fade, 4 Breathing, 5 Strobe, 6 Chase, 7 Phone Ring, 10..19 Custom Effect 1..10.
ca	mode · optional	Constant: 0 Static, 1 Wipe Loop, 2 Blink Loop, 3 Fade Loop, 4 Breathing, 5 Strobe Loop, 6 Chase Loop, 7 Phone Ring Loop, 8 Morse, 9 Audio Monitor, 10..19 Custom Effects.
sd, ed	direction · optional	0 left-to-right, 1 right-to-left.
cd	direction · optional	0 left-to-right, 1 right-to-left, 2 Center Out (2CH).
st, et, ct, ct2	milliseconds · optional	Start, stop, loop primary and loop secondary durations.
ctx	string · optional	Morse text: A-Z, 0-9 and spaces; lower-case letters are converted to upper case; max 64 bytes.
amch, amch2	integer · optional	Audio monitor channels; clamped 1..32.
amt1, amt2	integer · optional	Values are limited to 0..100; the device swaps them if necessary so the lower threshold comes first.
amc1, amc2, amc3	#RRGGBB · optional	Low/mid/high colours; malformed colours are ignored.



Send only the supported values above and verify the resulting configuration after a successful response.

Responses

STATUS	BODY / MEANING	CALLER ACTION
200	text/plain OK	A missing or out-of-range idx may make no change; a malformed supplied idx/id is interpreted as slot 0. Read the value back, then wait for the save delay.
409	cluster_remote_managed	Send the change to the ready leader.

Read Custom Effect slot

GET	/api/custom_effect	Authenticated · SAFE · JSON
-----	--------------------	-----------------------------

Returns a snapshot of Custom Effect slot 0..9, including whether a save was pending when the request was accepted. Later changes do not alter an active response.

Parameters

NAME / LOCATION	TYPE · REQUIRED	RULES / MEANING
idx · query	integer · required	Custom Effect slot 0..9. Missing/out-of-range returns 400; present empty/malformed parses as slot 0, so validate locally.

Response fields

LEVEL	EXACT FIELDS / TYPES
Effect	ok/storagePending Boolean; idx integer; name string; len uint32 ms; count/outCount uint8; style/band uint8; c2/c3 uppercase #RRGGBB strings; keyframes/okeyframes arrays.
keyframes[]	t uint32 ms; pq/sq uint16 Q8; tr/soft/rep/repc/gap uint8; gapc #RRGGBB; r/g/b/br uint8; e easing uint8; f motion-property mask; rf repeat-lane mask.
okeyframes[]	t uint16 ms; style/band/e/f uint8; c2/c3 uppercase #RRGGBB strings.

IMPORTANT For reliable JSON readback in v1.3.0, use Custom Effect names made from printable characters excluding quotation marks and backslashes. Clients must enforce this interoperability rule before saving a name.

Responses

STATUS	BODY / MEANING	CALLER ACTION
200	Complete JSON slot	Repeat the GET until storagePending=false, then compare every field to confirm the saved result.
400	{"ok":false,"err":"bad_idx"}	idx is missing or its parsed value is outside 0..9. If idx is supplied but empty or malformed, the device interprets it as 0.
503	Temporarily busy; Retry-After: 1	Read one slot at a time. Finish or cancel another active web download, wait one second, then retry the complete GET.
closed	No response or incomplete JSON	Discard the partial response and retry the complete GET; never combine partial slot responses.



Queue Custom Effect save

POST /api/custom_effect

Administrator · MUTATING · 202 ASYNC

Updates only the name, or replaces the complete timeline. Timeline changes are queued for saving and verification.

IMPORTANT Timeline fields cannot be updated individually. If any of len, data, odata, style, band, c2 or c3 is present, the endpoint treats the request as a complete timeline replacement: omitted len becomes 4000 ms and omitted data/odata become empty lists. Send the complete intended timeline, or send only idx and name for a name-only edit.

Parameters

NAME / LOCATION	TYPE · REQUIRED	RULES / MEANING
idx · form	integer · client-required	Slot 0..9. The device interprets a missing, empty, or malformed idx as 0. Clients must validate idx to avoid overwriting slot 0.
name · form	string · optional	Name, max 31 bytes. For interoperable JSON readback in this firmware baseline, clients must exclude quotation marks, backslashes and control characters. For a name-only change, send idx and a non-empty name, then omit all timeline fields.
len · form	uint32 · full mode	100..60,000 ms. Below 100 (including omitted/zero) becomes 4000; above 60,000 clamps.
data · form	string · full mode	Decoded form value at most 8,191 bytes. At least one valid motion record is required unless data and odata are both intentionally blank; odata-only is rejected as no_keyframes.
odata · form	string · full mode	Decoded form value at most 4,095 bytes. Motion plus output keyframes are normalised to at most 96 combined frames; excess records are truncated.
style · form	integer · optional	0 solid, 1 gradient, 2 bands; an invalid value becomes solid.
band · form	integer · optional	1..120; zero/out-of-range becomes 1.
c2, c3 · form	#RRGGBB · optional	Secondary/tertiary colours; malformed value leaves the prior global colour.
CSV	PREFERRED FIELD ORDER	
data (18)	t,pos_q8,size_q8,trail,soft,repeat,repeat_count,gap,gap_r,gap_g,gap_b,r,g,b,brightness,easing,flags,repeat_lane_flags	
odata (10/11)	t,style,c2r,c2g,c2b,c3r,c3g,c3b,band,easing[,flags]	
easing	0 linear, 1 hold, 2 ease-in, 3 ease-out, 4 ease-in-out; an invalid value becomes linear.	
motion flags	0x01 position, 0x02 size, 0x04 colour, 0x08 brightness, 0x10 trail, 0x20 feather, 0x40 repeat, 0x80 repeat-count.	
output flags	For odata only: 0x01 mode, 0x02 accent A, 0x04 accent B, 0x08 band; 0 enables all flags (0x0F).	
repeat lane	0x01 count, 0x02 gap, 0x04 gap colour.	

Responses

STATUS	BODY / MEANING	CALLER ACTION
202	{"ok":true,"queued":true,"verification":"pending"}	Call GET /api/custom_effect until storagePending=false, then compare the complete slot.
400	missing_body, bad_idx, no_keyframes	Correct the request.
409	cluster_remote_managed	Send the change to the ready leader.
503	storage_queue_rejected + Retry-After: 1	The rejected request does not change or save the effect. Wait at least one second, read the slot and retry only if needed.
500	overlay_verify_failed	The requested values may already be pending. Inspect /api/health and read back the slot before deciding whether to retry.



NOTE A busy rejection does not cancel an earlier accepted save. Save one effect at a time: after 202, wait for storagePending=false and compare the complete slot before sending the next save. A visible value while storagePending=true is not proof that it has been saved.

Set or clear Custom Effect preview

POST

/api/custom_effect_preview

Administrator · MUTATING RUNTIME

Shows a live preview without saving the effect.

Parameters

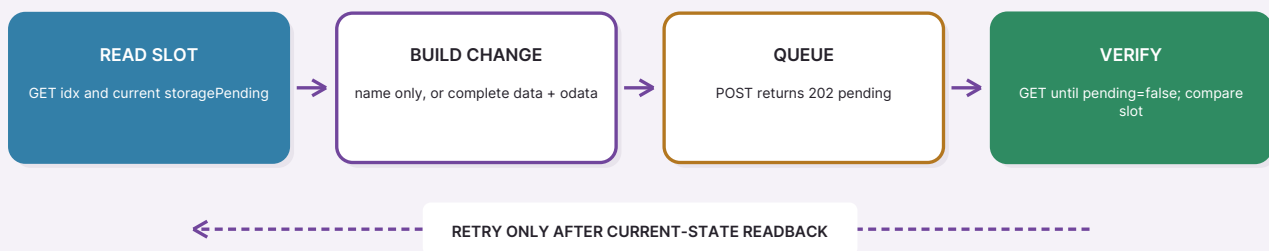
NAME / LOCATION	TYPE · REQUIRED	RULES / MEANING
idx · form	integer · client-required	Slot 0..9. The device interprets a missing, empty, or malformed idx as 0. Clients must validate idx locally.
enabled · form	literal 1 to enable	A missing or malformed enabled value, or any value other than 1, clears the preview.
len, data, odata	as save · when enabled	At least one valid motion record is needed to enable. If no valid motion records remain, the device clears the preview.
style, band, c2, c3	optional	Preview output style.
timeline · form	0/1 · optional	Enable timeline-mode preview.
playhead · form	uint32 · optional	Milliseconds, clamped to len.

Responses

STATUS	BODY / MEANING	CALLER ACTION
200	{"ok":true,"preview":false}	Preview was cleared: enabled was not literal 1 or no valid motion frame remained.
200	{"ok":true,"preview":true,"idx":0,"count":1}	Runtime preview is active; it is not persisted.
400	missing_body or bad_idx	Send a URL-encoded body within the documented size limit and an explicit idx from 0 to 9.
409	cluster_remote_managed	Send the runtime preview request to the ready leader.

CUSTOM EFFECT SAVE AND PREVIEW

A name-only edit and a complete timeline replacement are distinct operations



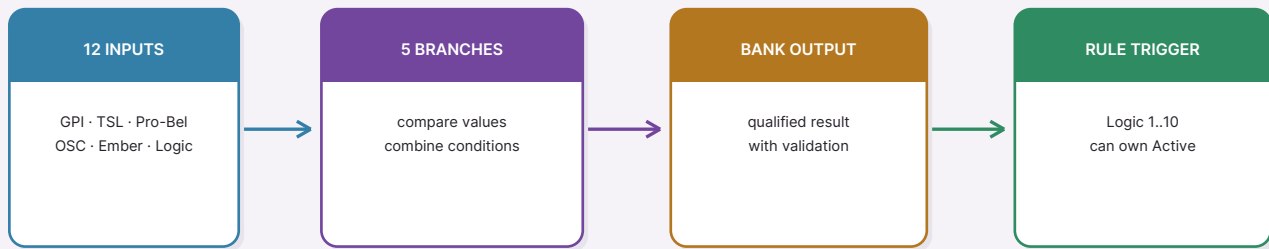
Preview is runtime-only and does not replace the queued-save verification flow.



07 • Logic Matrix

LOGIC MATRIX SIGNAL PATH

Each of ten banks evaluates up to 12 inputs through five branches



READ /api/logic/config describes the bank; /api/logic/status reports live values.

CHANGE POST /api/logic/apply replaces one complete bank atomically.

Invalid references or cycles are rejected; read configuration and runtime status after an accepted change.

LIMIT	VALUE
Banks / outputs	10
Inputs per bank	12
Branches per bank	5
Maximum on-delay	3,600,000 ms
TSL ID / bit	0..126 / 0..3

Read Logic configuration

GET /api/logic/config

Authenticated User/Admin · SAFE · NO-STORE

Returns a snapshot of the complete version 2 configuration. Later changes do not alter an active response. editable is true only for an Administrator.

Shape excerpt — one bank, one input and one output

The real response always contains ten banks; each bank contains twelve inputs and five outputs. The shortened valid JSON below illustrates nesting only.

```
{ "ok":true,"version":2,"editable":true,"banks":[{"name":"Logic 1","enabled":true,"inputs":[{"type":0,"cmp":0,"index":0,"aux":0,"id":0,"delay":0,"a":0,"b":0}], "outputs":[{"enabled":true,"mode":0,"threshold":1,"cells":"120000000000"}]}}
```



LEVEL	CONTENTS
root	ok Boolean true; version integer 2; editable Boolean; banks fixed length 10.
banks[]	name string; enabled Boolean; inputs fixed length 12; outputs fixed length 5.
inputs[]	type, cmp, index, aux, id, delay, a, b: integers. delay is ms; a/b are signed threshold x1000.
outputs[]	enabled Boolean; mode integer; threshold integer; cells string of exactly 12 digits 0,1,2.

Responses

STATUS	BODY / MEANING	CALLER ACTION
200	Complete application/json; no-store	Treat the arrays as one complete version-2 configuration snapshot.
503	Temporarily busy; Retry-After: 1	Finish or cancel another active web download, wait at least one second, then retry the complete GET.
closed	No response or incomplete JSON	Discard the partial response and retry the complete GET; never combine partial Logic configurations.
500	{"ok":false,"err":"missing_state"}	Device state was unavailable; do not attempt an apply.

Device control continues while the configuration is sent. The response can end after five seconds without progress or 30 seconds overall; continued progress does not extend the total limit. Request one large web download at a time.

Read Logic runtime status

GET	/api/logic/status	Authenticated User/Admin · SAFE · NO-STORE
-----	-------------------	--

Returns the current input, branch and output states together with validation details.

Response

FIELD	TYPE / FORMAT
ok	Boolean true.
raw / qualified / pending / available	Each is an array of 10 strings; every string has 12 '0'/'1' characters, one per input.
branches / branch_valid	Each is an array of 10 strings; every string has 5 '0'/'1' characters, one per branch.
output / valid	Strings of 10 '0'/'1' characters, one per Logic bank.
sums / connected	Each is a 10×5 matrix of non-negative integer active/connected input counts.
validation	Object code, logic, input, branch, related: uint8 integers. Index fields use 255 when not applicable.
validation.code	0 OK, 1 bad header, 2 bad source type, 3 bad comparator, 4 bad source reference, 5 bad aggregate, 6 bad threshold, 7 bad matrix cell, 8 bad Rule source, 9 cycle.



DATASHEET

LMPH-IP & HRNL-25W

REST API REFERENCE

ember_consumer object

FIELD	TYPE / MEANING
state / error	Same stable runtime strings described for /api/status.
enabled / configured / connected / monitoring	Boolean.
available / stale / online	Boolean value usability, freshness and inherited remote online state.
socket	Integer network-socket index; -1 when none is allocated.
kind	none, boolean, integer or real.
age_ms	uint32 milliseconds, or JSON null before a value.
value	Boolean, integer or finite JSON number matching kind; JSON null when unavailable.
endpoint	Configured provider as IPv4:port, or an empty string when state is unavailable.
path	Configured dot-separated numeric Glow path, or an empty string.
reconnects / protocol_errors	uint32 counters.

NOTE Unlike public /api/status, this authenticated Logic response includes the monitored value and configured endpoint/path because they are needed to commission the selected Logic source.

Responses

STATUS	BODY / MEANING	CALLER ACTION
200	application/json; no-store	Use validation plus valid bit strings before trusting outputs.

Atomically apply one Logic bank

POST /api/logic/apply

Administrator · MUTATING · STORAGE QUEUED

Replaces one Logic bank using a URL-encoded body. Other banks remain unchanged. Cyclic or invalid nested references are rejected.

Parameters

NAME / LOCATION	TYPE · REQUIRED	RULES / MEANING
v · form	integer · required	Exactly 2.
bank · form	integer · required	0..9.
name · form	string · required	1..23 bytes; no ASCII control characters or DEL.
enabled · form	0/1 · required	Bank state.
i0..i11 · form	8-int CSV · required	type,cmp,index,aux,id,delay_ms,threshold_a_x1000,threshold_b_x1000. Delay 0..3,600,000; thresholds signed int32 fixed-point (20.5 => 20500).
o0..o4 · form	3-int CSV · required	enabled 0/1, aggregate_mode 0..4, threshold 0..12.
c0..c4 · form	12 digits · required	Per-input cell: 0 off, 1 direct, 2 inverted.
ENUM	VALUES	
source type	0 disabled, 1 GPI, 2 TSL, 3 local parameter, 4 rule state, 5 Logic output, 6 Remote Ember+	
comparator	0 true, 1 false, 2 EQ, 3 NE, 4 GT, 5 GTE, 6 LT, 7 LTE, 8 between	
aggregate	0 any, 1 all, 2 at least, 3 exactly, 4 at most	



DATASHEET

LMPH-IP & HRNL-25W

REST API REFERENCE

SOURCE	TUPLE RULES
0 Disabled	Use zero for every tuple value; the general integer limits still apply.
1 GPI	index 0..1; comparator only 0 TRUE or 1 FALSE.
2 TSL	id 0..126, aux tally bit 0..3; comparator TRUE/FALSE.
3 Parameter	id/index/aux identify the provider value; numeric comparators 0..8 are allowed.
4 Rule state	index segment 0..44, aux rule 0..4; comparator TRUE/FALSE.
5 Logic output	index bank 0..9; comparator TRUE/FALSE; cyclic references are rejected.
6 Remote Ember+	index, aux and id must all be 0. The one device-local monitored value is selected; Boolean or signed-x1000 numeric comparisons follow its current type.

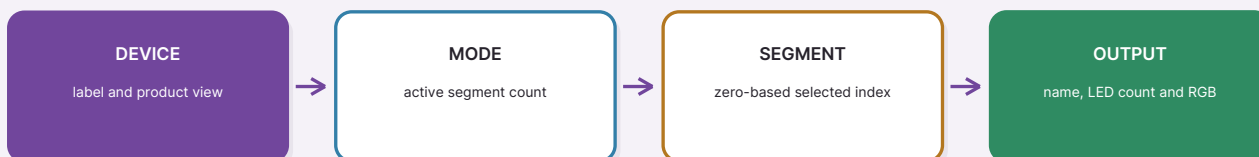
Responses

STATUS	BODY / MEANING	CALLER ACTION
200	applied/storage=queued or unchanged/storage=current pending	Read the complete configuration. An applied value is current in RAM; use a serialized health counter advance and no verification fault as later save evidence.
400	missing_body, unsupported_version, invalid_payload, invalid_bank, invalid_name, invalid_bank_state, invalid_input/output/matrix/config, logic_cycle	Correct the complete bank payload.
409	cluster_remote_managed	Send the complete bank change to the ready leader.
413	scratch_exhausted	Check the request size and encoding, then send the complete request again.
503	storage_writer_busy or storage_queue_rejected + Retry-After	Wait, read the current configuration, then retry if the change is still needed.

08 · Device, segments and network

DEVICE-TO-OUTPUT HIERARCHY

The request selects the active layout before changing one segment



Swap changes the two-segment display order. Firmware range: 1-120 LEDs per active segment; HRNL-25W maximum: 120 LEDs total.

Update device label and LED segments

GET

/api/update_config

Administrator · LEGACY MUTATING GET · CLUSTER-GATED · 30-S SAVE

Updates the device label, LED counts, segment names, segment order and HRNL view. Accepted changes are saved after the 30-second delay.

Parameters

NAME / LOCATION	TYPE · REQUIRED	RULES / MEANING
dev_name · query	string · optional	Non-empty decoded label, max 31 bytes.
leds · query	integer · optional	Legacy Segment 0 count.
cN · query	integer · optional	Segment N LED count. Software range: 1..120 per active segment, with a 5,400-LED firmware total ceiling. HRNL-25W hardware: maximum 120 LEDs total across all segments.
nN · query	string · optional	Segment N name, non-empty, max 31 bytes.
swap · query	0/1 · optional	Physical two-segment order flag.
hrnl_view · query	0/1 · optional	HRNL only: 0 strip, 1 rack 42U.

HRNL-25W has a 25 W PoE power supply and a maximum of 120 LEDs in total across all segments. Keep the sum of its active segment counts at 120 or fewer. Software acceptance of a count or an Extended Segments licence does not increase this hardware limit.

Responses

STATUS	BODY / MEANING	CALLER ACTION
200	{"status":"ok"}	Read /api/status, wait for the save delay and verify the configuration.
403	license_required	Do not address unlicensed HRNL segments.
409	cluster_remote_managed	Send the change to the ready leader.



Configure the outbound Ember+ consumer

GET /set_config

Administrator · LEGACY MUTATING GET · DEVICE-LOCAL ·
SAVE/REBOOT

Updates the complete device-local lazy-consumer settings, saves the network section and restarts the device. This public subset covers only the compact consumer fields below; omit unrelated Network Config fields when changing only the consumer.

Parameters

NAME / LOCATION	TYPE · REQUIRED	RULES / MEANING
ec · query	Boolean text · recommended	1, true or on enables. Any other value, or omission while another consumer field is supplied, disables.
ecip · query	IPv4 · optional	Remote provider; omission retains the stored address. When enabled, use a usable unicast address; unspecified, loopback and multicast addresses are rejected.
ecp · query	integer · optional	Remote TCP port 1..65535; omission retains the stored port; default 9000.
ecpath · query	numeric path · optional	Empty saves an awaiting-selection state. A non-empty path has one to six dot-separated non-negative components, each 0..2147483647; omission retains the stored path.
ecstale · query	integer ms · optional	1,000..3,600,000 in 100 ms steps; omission retains the stored value; default 5,000.

```
# Mutating request: curl prompts for the Administrator password
curl --user "${USERNAME}" \
"http://${DEVICE}/set_config?ec=1&ecip=192.0.2.20&ecp=9000&ecpath=1.70.1200.710.7000&ecstale=5000"
```

IMPORTANT This route is intended for the browser Network Config form and restarts after a successful save. Do not automatically replay it after a transport interruption. Reconnect, read `/api/status` and authenticated `/api/logic/status`, and verify the exact endpoint/path and monitoring state.

Responses

STATUS	BODY / MEANING	CALLER ACTION
200	HTML restart/redirect page	Wait for restart, reconnect and verify consumer status. The effective Ember provider client count may be reduced by one.
400	text/plain invalid Ember+ Consumer configuration	Correct IPv4, port, stale timeout or a malformed non-empty path; an empty path is the valid awaiting-selection state. No consumer setting is changed.
403	Forbidden	Use an enabled Administrator account.
409	text/plain Save failed. Device was not rebooted.	Treat the update as unsaved and inspect current settings before retrying.
closed	No complete response	Outcome is unknown. Reconnect and read current state before deciding whether to retry.

NOTE Send the complete five-field set for a deterministic integration update. An enabled Consumer with an empty path is saved as awaiting selection and does not start monitoring or reserve a runtime socket. A configured enabled Consumer uses one outbound network socket. If four provider clients were requested, the saved provider allocation is reduced to three. On a configured Cluster Follower the input-only consumer is suppressed and does not reduce provider capacity.

Start, verify or cancel an Ember+ provider browse job

POST /api/ember_consumer/browse

Administrator · READ-ONLY · JSON · ASYNCHRONOUS

Starts one read-only directory-list or Parameter-verification job, or cancels the current job. This route never saves Consumer settings and never writes the remote provider.

Parameters

NAME / LOCATION	TYPE · REQUIRED	RULES / MEANING
Content-Type · header	application/json · required	Any other content type returns 415.
schema_version · JSON	integer 1 · required	Only schema version 1 is supported.
op · JSON	start_list start_verify cancel · required	Selects directory listing, Parameter verification, or cancellation.
provider_ip / provider_port · JSON	IPv4 / integer · start only	Usable unicast IPv4 address and TCP port 1..65535.
path · JSON	integer array · start only	start_list accepts Root [] or up to 16 non-negative signed-32-bit components. start_verify requires one to 16 components.
offset / limit · JSON	integer · start_list	offset 0..65535 and limit 1..8 are required. The first page has offset 0.
after · JSON	integer · continuation only	For a non-zero offset, send the last numeric child number from the preceding page. It is not allowed on the first page.
generation · JSON	non-zero integer · cancel only	Identifies the active job to cancel.

```
{ "schema_version": 1, "op": "start_list", "provider_ip": "192.0.2.20",
  "provider_port": 9000, "path": [], "offset": 0, "limit": 8 }
```

NOTE Only one browse job is active at a time. Start returns a generation token; poll it until terminal, then cancel it if the operator closes the browser before completion. A job is bounded to 30 seconds overall; an individual response phase expires after 10 seconds without completion.

Responses

STATUS	BODY / MEANING	CALLER ACTION
202	{ "schema_version": 1, "ok": true, "generation": N, "state": "opening" }	Poll the returned generation with GET.
200	schema-v1 cancellation response	Cancellation was accepted; poll until the job closes if needed.
400	schema-v1 error object	Correct JSON schema, operation, endpoint, path or page fields; nothing was started.
413	payload_too_large	The JSON body exceeds 768 bytes; reduce it and send the complete request again.
409	browser_busy, browser_not_allowed or generation_conflict	Wait for the active job to finish, use the current device state, or read the active generation again.
415	unsupported_media_type	Send application/json.
500	internal_error or response_overflow	Treat the start as failed; read the current generation before deciding whether to retry.
503	browser_unavailable, socket_busy or buffer_unavailable; Retry-After: 1	Wait, free required capacity if needed, then start a new job.



Poll an Ember+ provider browse job

GET /api/ember_consumer/browse

Administrator · SAFE · NO-STORE

Returns current progress or the completed direct-child page for one generation. It is a no-store read and does not change Consumer configuration.

Parameters

NAME / LOCATION	TYPE · REQUIRED	RULES / MEANING
generation · query	non-zero integer · required	The only accepted query parameter. It must match the current job generation.

Response fields

FIELD	TYPE / MEANING
schema_version / ok / generation / operation	Schema 1, success flag, job token and list or verify operation.
state / error / active / terminal / connected / closing / elapsed_ms	Lifecycle state, optional stable error, lifecycle flags and elapsed milliseconds.
path / offset / limit / seen / more	Listed parent path, returned page position, page size, observed direct-child count and whether a continuation may be requested.
verified / node_parameter_only	Whether verification completed and whether entries are limited to Node and Parameter kinds.
entries	At most eight direct children. Each includes number, kind, identifier, identifier_truncated, declared_type, stream_identifier, value_type, value, online, selectable and compatible.

Responses

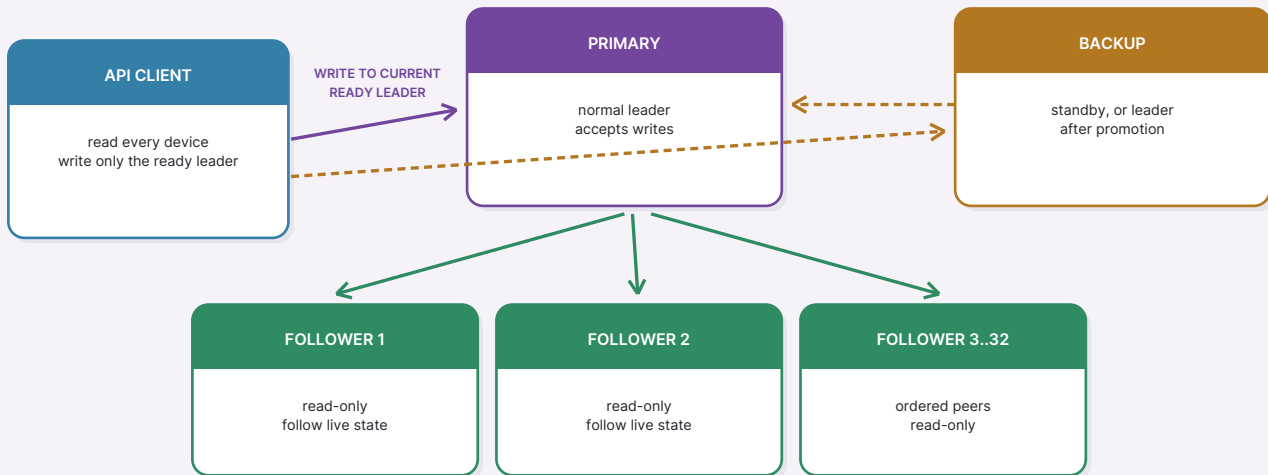
STATUS	BODY / MEANING	CALLER ACTION
200	schema-v1 status/page object	Continue polling while active. Open a returned Node or verify a returned compatible Parameter.
400	schema-v1 error object	Provide exactly one non-zero generation query parameter.
409	generation_conflict	The token is stale or belongs to another job; start a new browse operation.
503	state_unavailable; Retry-After: 1	Retry the same poll after the stated delay.

NOTE The response path is the directory being displayed; an empty array means Root. Filter and page controls in Network Config operate only on this returned direct-child page. A verified compatible path is copied into the form by the browser and takes effect only after the normal Network Config save and restart.

09 · Reading Cluster settings

CLUSTER TOPOLOGY AND WRITE AUTHORITY

Monitoring presence and control authority are separate signals



Use cluster_leader and cluster_ready for writes. Online/HEALTH presence alone is never authority.

Read Cluster settings

GET /api/cluster_settings

Administrator · SAFE · SENSITIVE · NO-STORE

Returns the device's Cluster topology, revision token, reboot status and last verified saved settings.

FIELD	TYPE / MEANING
schema_version	integer 1.
revision	Eight-hex-character token for the complete current configured or staged record, including Group ID and follower order. Treat it as opaque.
reboot_pending	Boolean: a change that requires a reboot is still being saved.
supersede_pending_supported	Boolean; true means this firmware supports supersede_pending.
pending_owner	none, cluster, or other.
durable_available / settings_durable	durable_available is true when a verified saved record exists. settings_durable is true when the pending settings match it.
durable_revision / durable_settings	Verified 8-hex token / complete object, or JSON null when unavailable.
durable_settings object	schema_version, licensed, enabled, role, role_name, primary, backup, backup_configured, group_id, follower_count and ordered followers.
boot_count / uptime_ms	uint32 / uint64 reboot information for monitoring.



DATASHEET

LMPH-IP & HRNL-25W

REST API REFERENCE

FIELD	TYPE / MEANING
last_reset_code / last_reset / boot_attempts / boot_loop	Reset/boot diagnostics.
serial / mac	Persistent device identity. mac is normalised to 12 hexadecimal digits.
licensed / enabled	Runtime Cluster licence and whether Cluster mode is enabled in the settings.
role / role_name	0 Off, 1 Primary Master, 2 Backup Master, 3 Follower.
primary / backup / backup_configured	Primary and Backup IPv4 addresses; backup_configured shows whether a Backup address is set.
group_id	Sensitive eight-hex-digit shared identifier.
follower_count / followers	Ordered 0..32 list; ordering defines peer-mask bits.

Valid JSON shape excerpt

The complete response also contains the remaining fields in the table above. Placeholders represent values read from the device; do not log the Group ID.

```
{
  "schema_version": 1,
  "revision": "D0C0FFEE",
  "reboot_pending": false,
  "pending_owner": "none",
  "durable_available": true,
  "settings_durable": true,
  "durable_revision": "D0C0FFEE",
  "serial": "${SERIAL}",
  "mac": "${MAC12}",
  "licensed": true,
  "enabled": true,
  "role": 1,
  "role_name": "Primary Master",
  "primary": "192.0.2.10",
  "backup": "0.0.0.0",
  "group_id": "${GROUP_ID}",
  "followers": ["192.0.2.20"],
  "durable_settings": {
    "schema_version": 1,
    "licensed": true,
    "enabled": true,
    "role": 1,
    "role_name": "Primary Master",
    "primary": "192.0.2.10",
    "backup": "0.0.0.0",
    "backup_configured": false,
    "group_id": "${GROUP_ID}",
    "follower_count": 1,
    "followers": ["192.0.2.20"]
  }
}
```

Responses

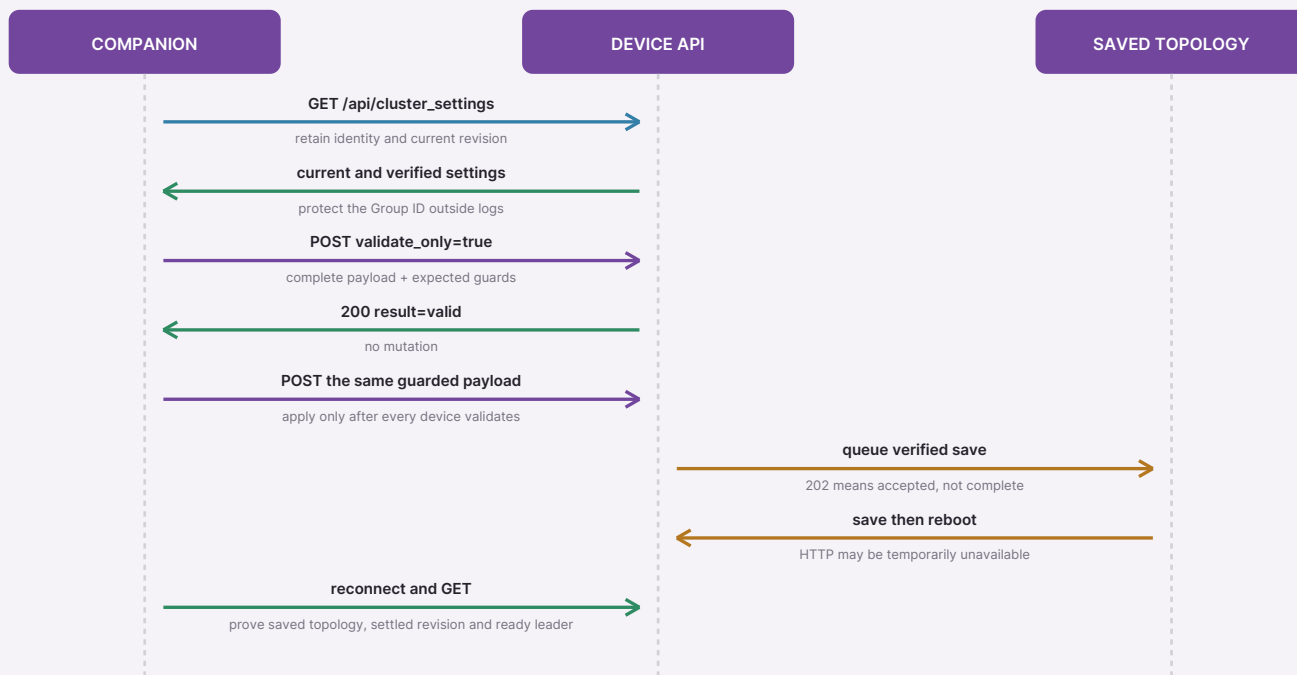
STATUS	BODY / MEANING	CALLER ACTION
200	application/json schema-v1 object; no-store	Store group_id securely and keep revision and device identity with the response.
503	identity_unavailable	The device identity could not be read. Do not submit a topology change.
500	cluster_settings_overflow	The device could not create the response. Update or recover the firmware before changing topology.



10 · Updating Cluster settings

SAFE TOPOLOGY REPLACEMENT

Identity and revision guards bind validation and apply to the intended device state



A revision conflict or identity mismatch is a stop-and-reconcile result, never an automatic overwrite.

Validate or replace complete topology

POST /api/cluster_settings

Administrator · MUTATING UNLESS validate_only · 202/REBOOT

Validates or replaces the complete version 1 topology. Identity and revision checks prevent changes from being applied to the wrong device or to stale settings.



DATASHEET

LMPSH-IP & HRNL-25W

REST API REFERENCE

Parameters

NAME / LOCATION	TYPE · REQUIRED	RULES / MEANING
Content-Type · header	application/json · required	Otherwise 415 unsupported_media_type.
schema_version · body	integer 1 · required	Only version 1.
role · body	integer 0..3 · required	Off, Primary, Backup, Follower.
primary · body	IPv4/empty · required	Empty or 0.0.0.0 means unconfigured.
backup · body	IPv4/empty · required	Backup role requires configured backup.
followers · body	array · required	Masters: 1..32 ordered addresses. Follower: no downstream list.
group_id · body	8 hex · required	Non-zero when enabled; sensitive.
expected_serial · body	string · required	Value returned by GET /api/cluster_settings.
expected_mac · body	12 hex · required	Value returned by GET /api/cluster_settings.
expected_revision · body	8 hex · optional	Recommended; required with supersede_pending.
validate_only · body	boolean · optional=false	Validates the payload without changing settings, saving, or rebooting.
supersede_pending · body	boolean · optional=false	With a matching revision, resume or replace a pending Cluster save.

```
{ "schema_version":1, "role":1, "primary":"192.0.2.10",  
  "backup":"","followers":["192.0.2.20"],  
  "group_id":"${GROUP_ID}", "expected_serial":"${SERIAL}",  
  "expected_mac":"${MAC12}", "expected_revision":"D0C0FFEE",  
  "validate_only":true, "supersede_pending":false }
```

IMPORTANT This is a shape example, not a replayable payload. Substitute identity and revision from the same device, keep the Group ID secret, and make the Primary or Backup address equal that device's live address when required by its role.

Validation rules

The device rejects unknown or duplicate fields, invalid or conflicting addresses, more than 32 followers, and an enabled topology with a zero Group ID. A Follower cannot have its own follower list. A Primary or Backup must have at least one follower, and a Backup role requires a backup address. Enabled roles require a usable live IPv4 address. The Primary or Backup address must match this device's live address; a Follower's address must differ from both master addresses. A Cluster licence is required unless the role is Off.

Success object

A successful response contains schema_version:1, ok:true, result:string, changed:Boolean, reboot_required:Boolean, and revision, current_revision and proposed_revision as opaque eight-hex-digit strings.



DATASHEET

LMPSH-IP & HRNL-25W

REST API REFERENCE

Responses

STATUS	BODY / MEANING	CALLER ACTION
200	result=valid or result=unchanged	After validation succeeds, send the same payload to apply it. Unchanged is final only when reboot_pending=false, settings_durable=true and revision=durable_revision.
202	result=applied, pending, or superseded; reboot_required=true	Stop further writes. Wait for save and reboot; a temporary unavailable response from another request does not change the accepted outcome. Reconnect and require expected identity/topology, reboot_pending=false, settings_durable=true, revision=durable_revision and matching durable_settings.
400	JSON error object: missing or invalid field, topology, or role/address mismatch	Correct the payload. Use code and field in client logic, and show message to users.
403	license_required	Install the Cluster licence or set role Off.
409	identity_mismatch, revision_conflict, reboot_pending, non_cluster_reboot_pending, supersede_busy or save_failed	Read the current state and follow the recovery for that code. If save_failed is returned, treat the change as unsaved.
415	unsupported_media_type	Send application/json.
500	canonicalization_failed or response_overflow	Do not assume the change succeeded. Update the firmware or use the supported recovery process before trying again.

Error envelope

```
{ "schema_version": 1, "ok": false,
  "error": { "code": "revision_conflict", "field": "expected_revision",
    "message": "Cluster settings changed after they were read",
    "current_revision": "A1B2C3D4" }
```

Errors returned after the JSON body has been parsed include current_revision. The earlier 400 missing_body and 415 unsupported_media_type responses omit it.

CLUSTER POST OUTCOMES

The result describes the next client action, not merely request parsing

VALID

200

Validation succeeded without mutation. Apply the same guarded payload only after every peer validates.

UNCHANGED

200

Final only when no reboot is pending and current revision equals the verified saved revision.

APPLIED / PENDING

202

Accepted for verified save and reboot. Stop writes; reconnect after any temporary unavailable response and prove completion.

CONFLICT

409

Identity, revision, pending owner or save state changed. Re-read and reconcile.

Never convert a 202 or 409 into success merely because staged RAM already resembles the requested topology.



11 • Cluster setup and recovery

AUTHORITY STATES DURING SETUP

Role, readiness and current leadership determine whether an application write is accepted

PRIMARY LEADER

WRITE

Normally ready and write-authoritative after the verified topology boots.

BACKUP STANDBY

READ

Readable, but application writes wait until a ready promotion.

BACKUP LEADER

WRITE

Accepts writes only while elected and ready after Primary expiry.

FOLLOWER

READ ONLY

Always read-only for shared application configuration.

Configure and verify Followers first, then Backup, then Primary; preserve recovery material before every wave.

IMPORTANT The hash, ready and no-transfer checks confirm the health of an existing Cluster. They are not required when first configuring a Cluster or recovering a broken one. Before the first write, save each device's current settings and identity.

STEP	REQUEST / CHECK	PASS CONDITION
1	GET health/status on every reachable device	The identity and build match expectations. For an existing topology, record whether the matching hash, ready state and absence of a transfer confirm that the Cluster is healthy. Do not require this when provisioning or recovering a Cluster.
2	Capture /api/backup plus each /api/cluster_settings	A secure backup and Cluster settings record exist for every device; the Group ID is not logged.
3	Retain serial, mac and revision per device	The identity check prevents an address change from redirecting the write to another device.
4	Construct every complete per-device topology	All devices use the same Primary, Backup and Group ID; each local role, address and follower order is correct.
5	POST every payload with validate_only=true	All reachable devices return 200 result=valid before any changes are applied.
6	POST the change with the same identity and revision values	202 accepted or 200 unchanged. Stop writes immediately.
7	Wait for reboot, then poll GET /api/cluster_settings	Expected identity/topology; reboot_pending=false; settings_durable=true; revision equals durable_revision; durable_settings exactly match.
8	GET /api/status and /api/health	Expected non-zero hash; cluster_ready=true; cluster_transfer=false; correct leader; expected build and healthy save state.
9	Resume application writes	Send only to the current ready leader.



Pending-save decisions

OBSERVATION	SAFE ACTION
reboot_pending=false and topology equal	Normal exact apply may return 200 unchanged.
Cluster-owned pending, exact same topology	Send matching expected_revision and supersede_pending=true to resume the save; expect 202 result=pending.
Cluster-owned pending, replacement topology	Send supersede_pending=true with the current identity and revision; expect 202 superseded or 409 supersede_busy.
pending_owner=other	Do not supersede it. A 409 non_cluster_reboot_pending means another operation must finish or be recovered first.
503 with Retry-After during the save	Do not replay the apply. Wait, reconnect and read /api/cluster_settings; use its pending and saved-record fields to decide the next action.
Capability marker absent	Update the firmware before using supersede_pending.

IMPORTANT A 202 response only means accepted. Completion requires the exact saved-record checks above, followed by the expected non-zero hash, cluster_ready=true, cluster_transfer=false and correct leader.

Synchronisation save time

Each Cluster synchronisation phase that waits for verified saving has a 180-second limit. Repeated pending acknowledgements do not restart or extend that phase. A complete update can include several phases; 180 seconds is not a total update time or a failover delay.

The 1.5-second authority expiry described in section 04 remains in effect during saving. Read cluster_ready, cluster_transfer and cluster_hash to follow completion. Upgrade both communicating devices to this firmware baseline to use the full save allowance; an older peer can retain a shorter limit.

Configuration updates are sent to one peer at a time. If a peer cannot be reached, the master retries it while continuing to offer updates to other eligible peers. Completion time depends on reachability, retries and saving. Verify every intended peer's readiness and matching configuration before maintenance or failover testing.

CONTROLLED DEPLOYMENT WAVES

A staged rollout keeps a known recovery path while roles and addresses change



Stop the rollout on the first identity, persistence, reboot, hash, readiness or leadership mismatch.



12 · Backup and restore

TWO PROTECTED RECOVERY ARTEFACTS

Application backup and device-local Cluster topology are deliberately separate

/API/BACKUP

APPLICATION

Application, segments, presets, Custom Effects, Rules, Logic and approved settings.

/API/CLUSTER_SETTINGS

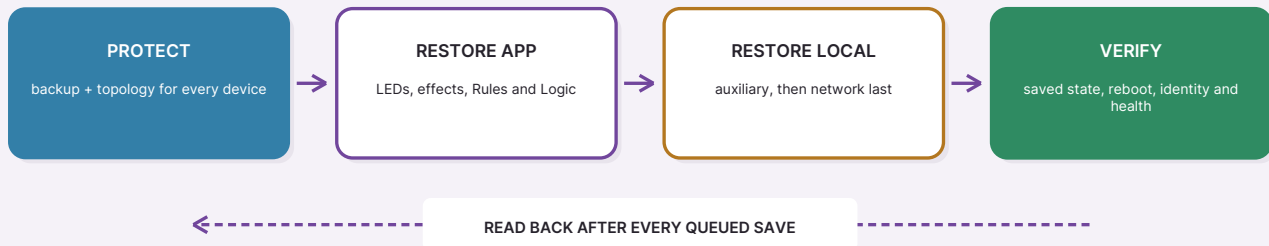
TOPOLOGY

Per-device role, peers, sensitive Group ID, revision and verified saved record.

Capture both from every device before a topology or restore operation; protect them from disclosure.

SAFE RESTORE JOURNEY

Restore independent sections in an order that preserves management access



Account records are outside this public restore contract.

Download application backup

GET`/api/backup`

Administrator · SAFE · SENSITIVE · STREAMED

Returns the application configuration as JSON, not a snapshot of live Rule Active states.

IMPORTANT Treat the complete backup file as a secret: it can contain network-service credentials and protected device-account material. It does not include Cluster topology, so capture `/api/cluster_settings` separately. Discard an incomplete or truncated JSON download.



Responses

STATUS	BODY / MEANING	CALLER ACTION
200	Chunked JSON attachment	Require a complete valid JSON document, then store the whole file securely.
503	Backup temporarily unavailable; the body may be empty	Honour Retry-After when present. Finish or cancel another active web download, then retry the complete GET.
closed	No response or incomplete JSON	Discard partial data and request a fresh complete backup after the connection is available.

Request one download at a time. Another web download can temporarily prevent a backup from starting; a 503 busy response does not change the configuration. Health and status reads can continue while a download is active when another HTTP connection is available, subject to the existing save, update and restart restrictions.

An incomplete HTTP request can temporarily delay another request, subject to the 8 s header and 15 s ordinary-request limits in section 02. Completion or expiry ends that restriction; a complete request does not retain it while its download continues. Health and status access still follows the connection and save restrictions above.

During Backup synchronisation or recovery, this endpoint can return 503 with Retry-After: 1 before a download starts. It does not export a partially received configuration. Wait for recovery to settle, then request a fresh complete backup; never combine partial downloads.

Application backups contain configuration, not live Rule Active states. Keep Cluster topology separately. After restore, verify the configuration and re-establish the current controller state.

Restore section endpoints

GET /api/backup returns nested JSON that cannot be sent directly to the restore routes. Use a trusted backup from a compatible firmware version, convert each documented non-credential section into the flattened application/x-www-form-urlencoded form below, and preserve the documented types and encodings.

NOTE The protected backup can contain account records, but account restore is not part of this public API. Do not extract or submit those records through the endpoints below.

BACKUP JSON	RESTORE FORM NORMALISATION
network	dhcp boolean -> dhcp 1/0; ip/mask/gw/ntp/syslog unchanged; mqtt.en/ip/port/ka/topic/user/pass -> mq/mip/mp/mka/mt/mu/mps; ember_consumer.enabled/ip/port/path/stale_ms -> ece/ecip/ecp/ecpath/ecst; tz_idx -> tz; ports -> hp/ep/tp/pp/op/ap; sockets -> hs/es/ts/ps/os/as. Join a non-empty consumer path array with dots; an empty array becomes an empty ecpath awaiting selection. For mps, omission retains the stored password, an empty value clears it, and a non-empty value replaces it.
led_config	Top fields generally retain names; encode swap Boolean as swap=1 0. segments[N].c/n/r/g/b -> cN/nN/crN/cgN/cbN; preset members -> pN_* compact keys.
led_config.custom_effects[N]	POST separately with idx plus name->name, cfl->len, cfd->data, cfod->odata, cfs->style, cfc2->c2, cfc3->c3 and cfb->band.
led_config.rules[] + logic	Rule members -> rl_* keys. Logic v2 -> logic_v=2; lbnB, lbeB, liB_I, lbB_O and lrs forms.
special_settings	mode1/mode2 strings Sensor/GPI -> 1/0.

Restore network and service settings

POST /api/restore_net

Administrator · MUTATING · DEVICE-LOCAL · 202

Queues a complete device-local network/service section. Network changes can move or stop the management endpoint, so restore this section last.



DATASHEET

LMPSH-IP & HRNL-25W

REST API REFERENCE

Parameters

NAME / LOCATION	TYPE · REQUIRED	RULES / MEANING
body	URL-encoded · required	dhcp, ip, mask, gw, ntp, syslog; mq/mip/mt/mu; tz/mp/mka; hp/ep/tp/pp/op/ap; hs/es/ts/ps/os/as. Send the complete intended section.
tz · form	timezone index · optional	A non-empty value must decode to one or two ASCII decimal digits selecting index 0..23. Omitted or empty retains the current timezone. An invalid value rejects the entire network restore before any settings change or save is queued.
mps · form	string · optional, presence-sensitive	Omitted retains the stored MQTT password. Present with an empty value clears it. Present with a non-empty value replaces it. Treat this write-only value as a secret.
ece/ecip/ecp/ecpath/ecst · form	complete optional object	When ece is present, all five fields are required. ece is 0 1; ecip is provider IPv4; ecp is port 1..65535; ecpath is empty or 1..6 dot-separated components; ecst is 1,000..3,600,000 ms in 100 ms steps. An empty path is awaiting selection and does not monitor. Omitting ece leaves the existing consumer unchanged for backward compatibility.

Responses

STATUS	BODY / MEANING	CALLER ACTION
202	{"status":"queued","verification":"pending"}	Stop writes; use serialized health save evidence, then reconnect if the address or service changed.
400	bad_timezone	Use a timezone index 0..23. The request applies no network changes and queues no save.
400	bad_ember_consumer	Correct the complete optional consumer object; the network restore is rejected before mutation.
413	Payload too large	Reduce headers/encoding without omitting required section values.
503	save_queue_rejected; Retry-After: 1	Running values may already differ. Preserve access, read current state and recover deliberately.

Restore LEDs, segments and presets

POST /api/restore_leds

Administrator · MUTATING · CLUSTER-GATED · 202

Queues a complete shared LED/preset section. Custom Effects from the backup still require separate slot requests.

Parameters

NAME / LOCATION	TYPE · REQUIRED	RULES / MEANING
body	URL-encoded · required	dev_name/mode/swap/hrnl_view; cN/nN/crN/cgN/cbN; pN_n/r/g/b, phase fields, Audio Monitor fields and legacy per-preset timeline fields. Send the complete intended section.

Responses

STATUS	BODY / MEANING	CALLER ACTION
202	{"status":"queued","verification":"pending"}	Read current application state, then require later save evidence before continuing.
403	license_required	Restore only supported licensed content.
409	cluster_remote_managed	Send the shared restore to the ready leader.
413	Payload too large	Use a compatible complete section that fits the request limit.
503	save_queue_rejected; Retry-After: 1	Running values may already differ. Read current state before recovery or retry.



Restore Rules, schedules and Logic

POST /api/restore_rules

Administrator · MUTATING · CLUSTER-GATED · 202

Patches supplied Rule/NTP configuration fields; it does not import live Active states. Logic is unchanged when logic_v is absent; with logic_v=2 the complete Logic configuration is required.

Parameters

NAME / LOCATION	TYPE · REQUIRED	RULES / MEANING
body	URL-encoded · required	rl_p/ti/tb/gi/ip/im/op/om/on/ox/os; NTP rl_nSm/a/w/t/d. Optional Logic: logic_v=2 plus complete lbnB/lbeB/liB_J/lbB_K/lrS.

Responses

STATUS	BODY / MEANING	CALLER ACTION
202	{"status":"queued","verification":"pending"}	Verify every size-limited Rule/NTP batch; submit complete Logic separately.
400	bad_logic_restore	A supplied Logic form must be complete and valid.
403	license_required	Restore only licensed segments.
409	cluster_remote_managed	Send the shared restore to the ready leader.
413	Payload too large	Split only patch-safe Rule/NTP fields; keep complete Logic in one request.
503	save_queue_rejected; Retry-After: 1	Read current state before recovery or retry.

Restore auxiliary port modes

POST /api/restore_special

Administrator · MUTATING · DEVICE-LOCAL · 202/REBOOT

Updates supplied device-local mode1/mode2 values and queues a save. The accepted response requires a later reboot; this endpoint does not itself reboot.

Parameters

NAME / LOCATION	TYPE · REQUIRED	RULES / MEANING
mode1 / mode2	0 GPI or 1 sensor · at least one	Omitted fields retain their current values.

Responses

STATUS	BODY / MEANING	CALLER ACTION
202	queued; verification=pending; reboot_required=true	Wait for later save evidence, then restart through the supported administrator interface.
400	bad_value	Correct the supplied port mode.
413	Payload too large	Send only the supported small form.
503	save_queue_rejected; Retry-After: 1	Do not reboot; read current state and recover the save first.



IMPORTANT Send complete data to `restore_net` and `restore_leds`. Missing fields may be disabled, cleared, or mixed with existing values. For `restore_net`, omitted or empty `tz` retains the timezone; a non-empty `tz` must select index 0..23. The MQTT password is another exception: omitted `mps` retains the stored password, while present-empty `mps` clears it. The Ember+ consumer is another compatibility exception: omitting `ece` retains it, but when `ece` is present its complete five-field object is required; `ecpath` may be empty to retain an awaiting-selection Consumer. `restore_special` updates only supplied fields but requires at least one supported field. For `restore_rules`, ordinary Rule/NTP fields update only when present and omitting `logic_v` leaves Logic unchanged; if `logic_v=2` is present, the complete Logic v2 form is required.

IMPORTANT A complete non-OTA POST request, including headers and body, may be at most 16,381 bytes. A 45-segment Rule/NTP restore cannot fit in one request. Send size-limited Rule/NTP batches with `logic_v` omitted and verify each 202. Then send the complete Logic v2 form in a separate `restore_rules` request within the same size limit.

Safe restore order

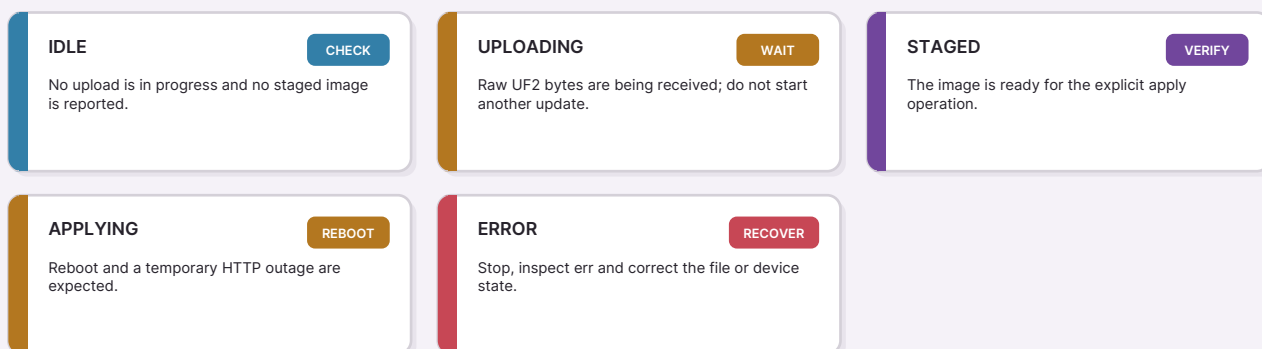
ORDER	ACTION	WHY / COMPLETION
1	POST <code>restore_leds</code>	Verify the queued save before continuing.
2	POST every Custom Effect separately	Wait until each slot reports <code>storagePending=false</code> and matches the backup.
3	POST size-limited <code>restore_rules</code> Rule/NTP batches	Omit <code>logic_v</code> ; keep each complete HTTP request at most 16,381 bytes and verify every 202.
4	POST the complete Logic v2 <code>restore_rules</code> form	Include <code>logic_v=2</code> and every Logic field in one request within the size limit; verify it.
5	POST <code>restore_special</code>	If <code>reboot_required</code> is true, wait until the settings are saved before restarting.
6	POST <code>restore_net</code> last	Network changes may change the device address or stop the management service.
7	Restart the device using the supported administrator interface	Restart only after the restored settings have been saved.
8	Reconnect and verify	Check identity, build, effective network/services, application configuration and Cluster topology separately. Re-establish current controller state and verify output.



13 · Firmware update

OBSERVABLE UPDATE STATES

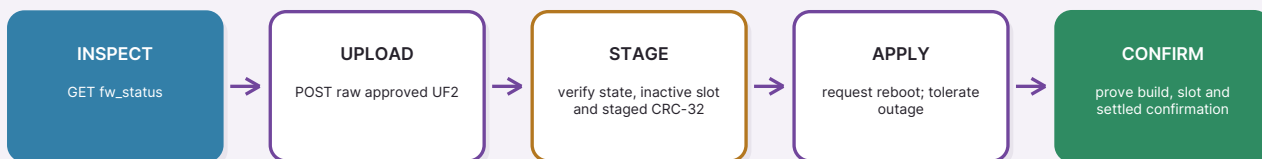
Read `/api/fw_status` before every decision and after every interrupted operation



A disconnect makes the result unknown: reconnect and read `fw_status` before upload or apply.

FIRMWARE UPDATE SEQUENCE

Use the public state endpoints to prove each transition



Never apply unless `state=staged`, `ready_slot` is the expected inactive slot and `err=0`.

Integrity and authenticity

CHECK	PUBLIC CONTRACT
Device validation	The device validates UF2 framing, RP2040 family, complete block and page coverage, inactive-slot address limits and vector-table bounds. It checks written data against the received image and independently compares the complete stored-image CRC-32 with the received-image checksum before reporting staged.
Integrity scope	UF2 structural checks and CRC-32 detect malformed, incomplete or accidentally corrupted uploads. They are not cryptographic publisher authentication.
Authenticity	Firmware v1.3.0 does not verify a digital signature and has no provisioned firmware-signing trust root.
Client action	Obtain <code>ethernet_update.uf2</code> and its SHA-256 manifest through a trusted release channel, compare the digest before upload, and restrict Administrator access to the trusted management boundary.



IMPORTANT The CRC-32 returned by the device describes the staged image after comparison with the received image. It is a corruption check, not proof of who produced the firmware.

Read update state

GET /api/fw_status

Administrator · SAFE · NO-CACHE

Returns the current upload, validation and apply status.

FIELD	TYPE / MEANING
state	String: idle, uploading, staged, applying or error.
fw	String containing the running firmware identity.
content_len / rx	uint32 declared upload bytes / bytes received.
expected / blocks	uint32 expected UF2 block count / unique inactive-slot pages programmed.
image_size	uint32 validated image bytes.
crc32	Eight-character hexadecimal checksum, emitted lowercase; compare case-insensitively.
cur_slot / ready_slot / pending_slot	uint8: 0 Slot A, 1 Slot B, 255 none or unknown; never JSON null.
forensics_degraded / boot_confirmation_degraded	Boolean degraded post-boot evidence states.
err	int32; 0 means no reported error, a negative value means the update failed.

Responses

STATUS	BODY / MEANING	CALLER ACTION
200	application/json; no-cache	Use state, progress fields and err together.

Upload firmware image

POST /api/fw_upload

Administrator · FLASH WRITE · SIZE/TIME LIMITS

Upload the release's universal ethernet_update.uf2 as a raw UF2 body. Verify its SHA-256 against a manifest obtained through a trusted channel before upload.

Parameters

NAME / LOCATION	TYPE · REQUIRED	RULES / MEANING
Content-Type	application/octet-stream · expected	Recommended media type.
Content-Length	positive decimal bytes · required	Send the exact raw UF2 byte count in one header, following section 02. Missing, zero or invalid framing returns 411.
body	binary UF2 · required	Send the UF2 file as the raw request body, not multipart data. After authenticated headers are accepted, the upload has a 10 s no-progress timeout and a 300 s total time limit. Continued traffic does not extend the total limit.

The 8 s header limit applies before upload admission, including headers received in several TCP fragments. After admission, the streamed UF2 body uses the upload limits above. The device services control and monitoring between upload steps. When another HTTP connection is available, read /api/fw_status there to follow state, rx and err. The upload POST stays open until its final response; it does not return 202 or a separate job identifier.



```
# curl prompts for the password
curl --user "${USERNAME}" -X POST --data-binary @ethernet_update.uf2 \
-H "Content-Type: application/octet-stream" \
http://${DEVICE}/api/fw_upload
```

Responses

STATUS	BODY / MEANING	CALLER ACTION
200	{"ok":true,"image_size":123456,"crc32":"a1b2c3d4"}	GET /api/fw_status; require state=staged and the expected ready slot before apply.
400	UF2 parse / flash error. or Upload incomplete or invalid UF2.	Read fw_status; check the file and device health before restarting the complete upload.
408	Upload timed out.	Read fw_status, then restart the complete upload if no valid image is staged.
411	Length Required; empty body	Correct the framing and send one Content-Length header with the exact positive raw UF2 byte count.
413	Payload Too Large; empty body	The upload could not begin. Check fw_status and correct the image or device state before retrying.
503	Cluster recovery active. or Storage operation active.; Retry-After: 1	The upload did not start. Wait, read current status and retry only after the conflicting operation finishes.
closed	Upload ended without an HTTP status	The result is unknown. Reconnect and check fw_status before uploading or applying.

IMPORTANT Upload errors can have a plain-text or empty body without a Content-Type header; do not assume JSON. A lost connection aborts an unfinished upload. There is no resume operation: if state is not staged with err=0 and the expected ready_slot, send the complete file again. Never apply a partial upload.

Apply uploaded image

GET /api/fw_apply

Administrator · LEGACY MUTATING GET · REBOOT

Rechecks the staged image size, vector table and CRC-32, then requests a controlled restart to install it. An accepted apply can wait for verified Rule Active saving before restart. This operation does not verify a digital signature.

Responses

STATUS	BODY / MEANING	CALLER ACTION
200	text/html waiting page	Accepted, not a completed restart. Stop writes and allow saving to finish; expect an HTTP outage. Reconnect with bounded retry and require the expected build/current slot, pending_slot=255 and no degraded confirmation state.
409	No staged firmware.	Upload and validate an image first.
503	Storage verification pending; retry firmware apply. · Retry-After: 1	A pending save or Cluster recovery prevents apply. Wait, re-read fw_status and health, then retry only if the image is still staged and the action is needed.



Invalidate uploaded image

GET /api/fw_invalidate

Administrator · LEGACY MUTATING GET

Prevents the staged image from being applied.

Responses

STATUS	BODY / MEANING	CALLER ACTION
200	text/plain OK	Returned even when no image was staged; read fw_status to verify effective state.

NOTE HTTP can be deliberately unavailable while update confirmation finishes. Reconnect with bounded retry, then verify /api/health and /api/fw_status: expected firmware/build and current slot, pending cleared, and forensics_degraded=false plus boot_confirmation_degraded=false.



14 • HTTP responses and errors

STATUS-TO-ACTION COMPASS

Use the status family first, then the endpoint-specific body and completion rule

2XX Success or acceptance. Follow the documented readback, save and reboot steps. FOLLOW	400 / 411 / 413 / 415 Correct the request, length, size or media type; do not repeat unchanged. CORRECT	401 / 403 Supply valid credentials or use an account/feature with the required access. ACCESS
409 The request conflicts with current identity, revision, authority or state. Re-read. RECONCILE	503 Temporarily unavailable. Honour Retry-After and confirm the operation is still needed. WAIT	CLOSED / PARTIAL Outcome unknown. Discard partial data and inspect the current endpoint state. RECOVER

Error bodies are not uniform across compatibility routes; validate status and Content-Type before parsing.

STATUS	MEANING IN THIS API	RECOVERY
200	The request succeeded. Some legacy writes return 200 before the 30-second save finishes.	Read the response body and follow the endpoint's save and verification steps.
202	The request was accepted or queued; saving, processing, or rebooting is still in progress.	Do not consider the operation complete until the endpoint-specific verification succeeds.
204	Readiness probe success with no body.	The HTTP API is responding.
400	The request contains an invalid, incomplete or unsupported field or body.	Correct the request; do not repeat it unchanged.
401	Recognised strict API routes use 401 for missing or invalid HTTP Basic credentials; some compatibility routes can return HTML or another response shape.	Require the expected status and Content-Type, then send valid credentials.
403	Strict routes use 403 for an insufficient role or missing licence; compatibility-route responses are not uniform.	Validate the body type; use the required account role or licensed feature.
404	Unknown route or operation unavailable for the current firmware or role.	Check firmware, path and authenticated role; validate the returned body type.
408	The firmware upload stopped making progress or exceeded its total time limit.	Restart the complete upload.
409	Current-state conflict, or a legacy save failure after the running values may already have changed.	Use the response code and body to follow the recovery steps for that endpoint.
411	Missing, zero, invalid, out-of-range or repeated Content-Length; unsupported Transfer-Encoding; or a folded header line in a POST request or OTA upload.	Follow section 02 and send one exact positive decimal Content-Length.
413	A non-OTA request exceeds its route limit (16,381 bytes generally; 768 bytes for the Ember+ browse POST), or a firmware upload cannot start because of its size or the current device state.	Correct the request size; split only restore data that supports partial updates. Otherwise check fw_status.err.
415	A JSON-only POST, including Cluster and Ember+ browse, has a different Content-Type.	Set Content-Type: application/json.
500	Save, identity, or verification failure.	Treat the operation as failed; inspect /api/health and the saved settings.



STATUS	MEANING IN THIS API	RECOVERY
503	The device is temporarily busy, often with Retry-After: 1.	Wait, read the current state, and retry only if the operation is still needed.

Machine-readable error codes

FAMILY	EXACT VALUES IN v1.3.0
Cluster parse/schema	malformed_json, invalid_type, invalid_ipv4, too_many_followers, invalid_group_id, invalid_revision, invalid_identity, unknown_field, duplicate_field, missing_field, unsupported_schema
Cluster topology	invalid_role, invalid_primary, invalid_backup, master_address_conflict, invalid_follower, follower_master_conflict, duplicate_follower, primary_required, backup_required, group_id_required, followers_not_allowed, followers_required, role_address_mismatch
Cluster state/save	identity_mismatch, revision_conflict, reboot_pending, non_cluster_reboot_pending, supersede_busy, save_failed, canonicalization_failed, identity_unavailable, cluster_settings_overflow, response_overflow, license_required, unsupported_media_type
Application/storage	cluster_remote_managed, cluster_persistence_pending, storage_writer_busy, storage_queue_rejected, overlay_verify_failed, buffer_too_small
Logic/Custom/restore payload	missing_body, bad_idx, bad_value, bad_timezone, bad_ember_consumer, no_keyframes, unsupported_version, invalid_payload, invalid_bank, invalid_name, invalid_bank_state, invalid_input, invalid_output, invalid_matrix, invalid_config, logic_cycle, scratch_exhausted
Status response	STATUS_SNAPSHOT_BUSY

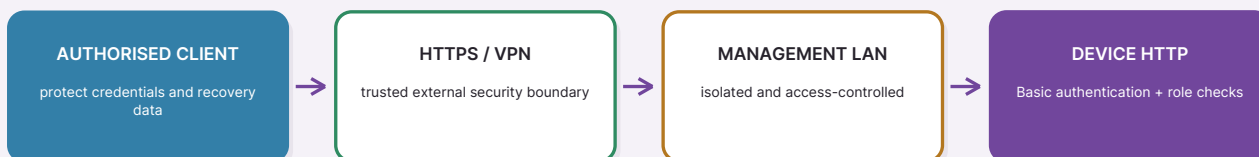
NOTE Error responses are not uniform across all endpoints. Cluster operations use the strictest schema; other endpoints may return JSON, text, HTML or an empty body as documented above.



15 • Limits and security

TRUSTED MANAGEMENT BOUNDARY

The device serves native HTTP; confidentiality must come from the surrounding network



Never expose native HTTP directly to an untrusted network or log credentials, backups or Group IDs.

RESOURCE	LIMIT / RULE
Segments	LMP SH-IP up to 2; HRNL-25W up to 45 where enabled, normally 5 without Extended Segments.
Firmware LED range	Each active segment 1..120; firmware ceiling 5,400 LEDs total. Product hardware limits still apply.
HRNL-25W hardware	25 W PoE power supply; maximum 120 LEDs total across all segments. Extended Segments does not increase this total.
Rules	5 per segment; maximum 225 rules in total.
Preset / Custom Effects	10 each; Custom Effect slots map to preset mode values 10..19.
Logic	10 banks, 12 inputs/bank, 5 branches/bank.
Remote Ember+	One device-local monitored Parameter; path depth 1..6; Boolean, Integer -2,147,483..2,147,483, or Real -2,147,483.648..2,147,483.647; stale timeout 1,000..3,600,000 ms.
Ember connections	Up to 4 inbound provider clients without the outbound consumer; up to 3 while the consumer is active.
Cluster	One Primary, one optional Backup, and 1..32 ordered Followers in each master record. The Group ID must be non-zero.

Security-sensitive values

VALUE	HANDLING
HTTP Basic credentials	Never log. Native HTTP exposes credentials on an untrusted network; use a trusted HTTPS boundary.
Network-service credentials	Restore payloads and backups can contain sensitive service configuration. Transmit and store them securely.
Cluster group_id	Treat as confidential; do not log or share it.
Backups/topology recovery	Encrypt backups or restrict access to authorised operators. Confirm the backup is complete before changing Cluster settings.