XICHTEE

MANUAL

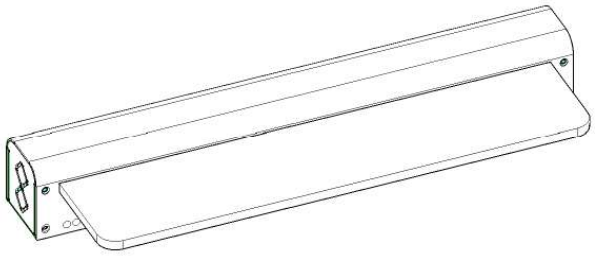
LMPSH-IP

Professional RGB Studio Signal Lamp

rev. 1.3

www.xichtee.com
office@xichtee.com

LMPSH-IP
Professional RGB Studio Signal Lamp



Contents

1. Introduction

The XICHTEE device is a network-controlled LED indicator system. It is designed to show clear visual states (for example: On-Air, Preview, Warning, or custom statuses) driven by rules and presets.
This manual explains how to access, configure, and operate the device. It focuses on the most common tasks: first start, basic configuration, enabling rules, and triggering rules via supported protocols.

Before you begin
For best results, connect the device to a trusted local network. The web interface uses HTTP (no HTTPS), so it is intended for LAN/VPN access, not direct Internet exposure.

2. First Start

2.1 Connect the hardware

1. Connect the device to your network using PoE Ethernet (IEEE802.3at class 4).
2. Wait about 5–10 seconds for the device to boot.

2.2 Find the device IP address

By default, the device uses DHCP.

If DHCP is not available (AutoIP)
If no DHCP server responds, the device automatically assigns itself a link-local address in the range 169.254.x.x. This allows direct access from a computer on the same Ethernet segment.

Common ways to find the IP address:

- Connect your PC and the device to the same network (same switch/router).
- Start XICHTEE Device Manager (the discovery tool. Download link: https://xichtee.com/downloads/deviceconfigapp.zip
- In Interface, select the network adapter you're using (Ethernet/Wi-Fi).
- Click SCAN BROADCAST and wait a moment for devices to appear.
- Read the device IP ADDRESS from the list (optional: select it and use DETAILS → OPEN WEB UI to open the web interface).

Change IP settings: Select the device in the list, open Network / IP Settings, choose DHCP or Static, enter the new IP / Subnet / Gateway (and DNS if requested), then click Apply/Save. The device may briefly reconnect while the new settings take effect.

DISCOVERY TOOL – IMPORTANT NOTE!

Works only inside the same local network (same "LAN"). Most routers do not forward broadcast packets between different networks.

Examples:

☐ **It will work**

- Your PC and the device are on the **same switch** (same office LAN).
- Your PC is on the **same Wi-Fi** as the device (same subnet/VLAN).

☐ **It will NOT work**

- Your PC is on **192.168.1.x** but the device is on **192.168.6.x** and there is a **router** between them.
- You are connected via **VPN** to another site/network and try to discover devices there.
- The device is in a **different VLAN** and your network routes between VLANs (L3 routing).

The tool has function called Poke Device. When you enter the device IP and start Poke, the tool sends UDP messages unicast (targeted packets) to that exact address. Because these packets are not broadcast, they can be routed through L3 networks (routers) the same way as normal IP traffic.

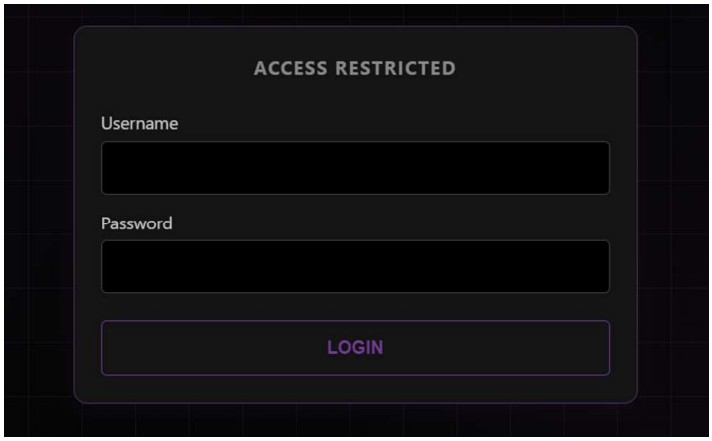
2.3 Open the web interface

Open a web browser on a computer in the same network and enter the device IP address:
http://<device-ip>
Example: http://192.168.1.20

2.4 Log in and secure the device

On the first login, use the default administrator credentials:

Field	Value
Username	admin
Password	admin



Security best practices

- Create separate user accounts for daily operation and keep the admin account for maintenance.
- Keep the device on a trusted network segment. Avoid exposing it directly to the Internet.
- Document your network settings and keep a backup of the configuration.

3. Web Interface Basics

After logging in, you will see the Dashboard. The Dashboard provides quick access to the most important settings.

Typical areas you will use:

- Device Status: basic information, connected clients, and system health.
- Segment Settings: configure segment names/lengths and rule mappings.
- LED Presets: define reusable colors and (optionally) effects.
- Network & Services: IP settings, ports, socket allocation, time (NTP), syslog, and protocol configuration (Ember+, TSL, SW-08-P, OSC, MQTT & Rest API).
- User Management
- System: reboot, configuration backup/restore, and firmware update.

Saving changes

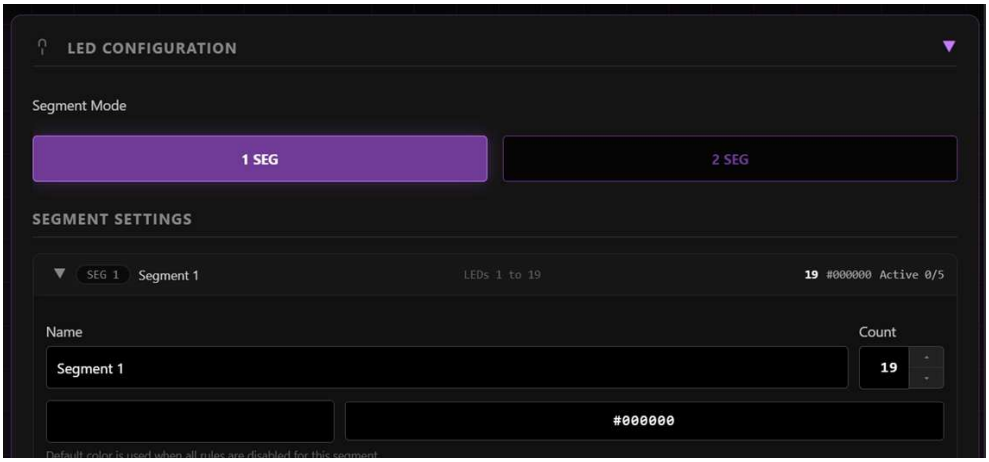
Changes take effect immediately. To reduce flash wear, the device saves web changes automatically after a short idle period (typically about 30 seconds after your last change).

4. Segments, Rules, and Presets

LED outputs are organized into Segments. Each Segment can be controlled manually or by Rules. Rules reference Presets so you can reuse the same look across multiple segments.

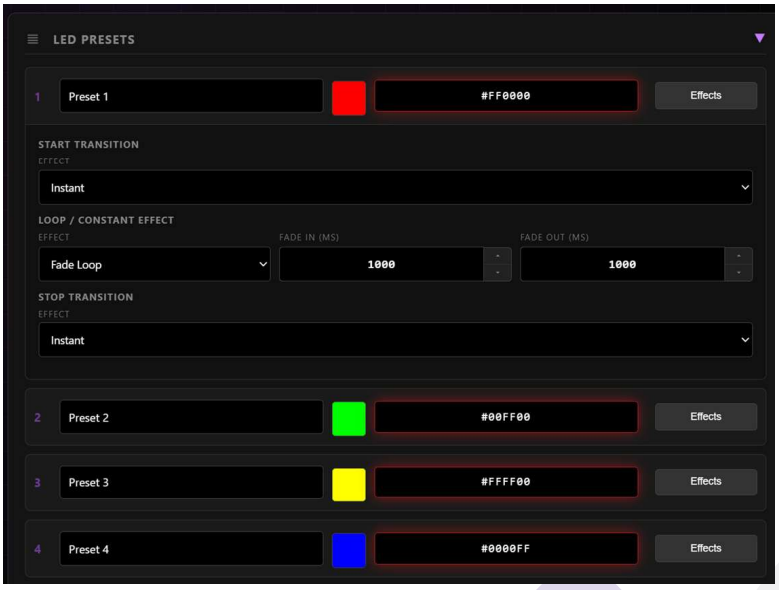
4.1 Segments

A Segment represents a physical LED section (one part of a strip). You can rename segments and set the number of LEDs per segment to match your installation.



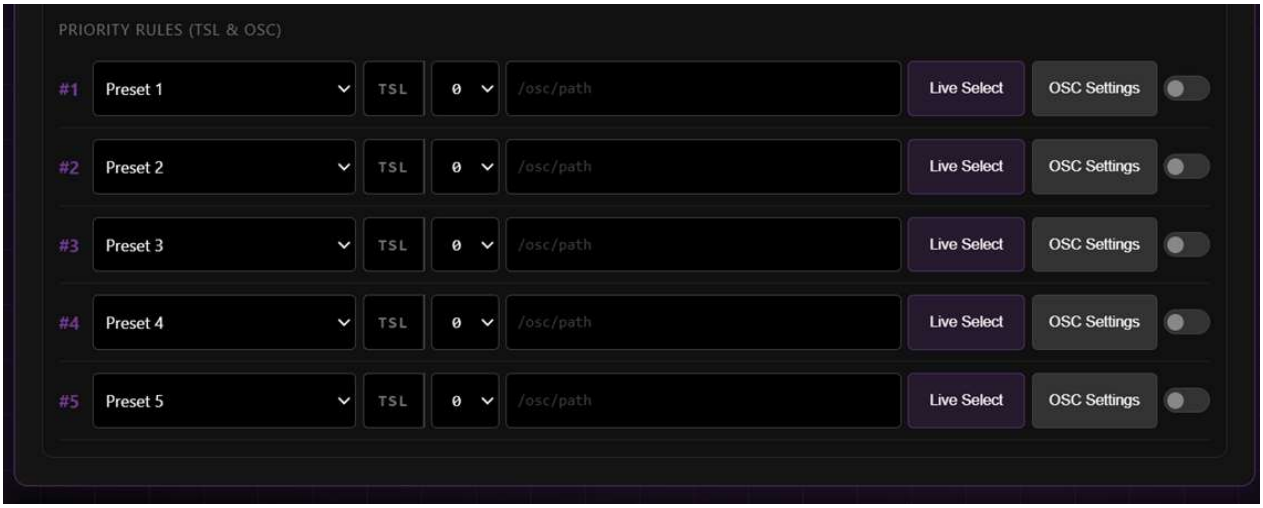
4.2 Presets

A Preset is a reusable visual definition. At minimum, a preset contains an RGB color. Presets can also include transitions and looping effects.
When you edit a preset, every rule that uses that preset will immediately use the updated preset.



4.3 Rules

Each segment contains up to 5 rules. A rule links an external trigger (such as a tally state or message) to a preset.
Priority: Rules are evaluated in order (Rule 1 to Rule 5). The first rule that is active determines what the segment displays.



4.4 Default configuration

Your device ships with a default configuration to help you start quickly.

Item	Default
Network mode	DHCP enabled (AutoIP link-local fallback if DHCP fails)
Web interface	HTTP on port 80
Default admin user	admin / admin
Segments	Segment 1 enabled by default (typical default length: 18 LEDs). Additional segments depend on hardware/ license.
Rules per segment	5 rules per segment, mapped to Presets 1–5, inactive by default
Presets	10 presets (Preset 1–4 pre-colored: red, green, yellow, blue)

Default service ports

Service	Transport	Default port	Notes
Web interface	TCP	80	Browser access (login required)
Ember+ provider	TCP	9000	Requires Ember+ license
TSL tally	TCP	8900	Tally input
Pro-Bel (SW-P-08)	TCP	2000	One socket per client
OSC	UDP	8000	UDP listener
MQTT	TCP	1883	Requires MQTT license; broker address required
Syslog	UDP	514	Sends logs to your syslog server
NTP	UDP	123	Time sync with your NTP server
Discovery	UDP	33333	Device discovery/announce on LAN
Management console	TCP	2323	Advanced diagnostics

5. Enabling Rules in the Web Interface

This section shows the simplest workflow for enabling rules. You will choose what the rule should display (Preset) and how it should be triggered.

5.1 Select a preset for the rule

1. Open Dashboard → Segment Settings.

2. Choose the segment you want to control.

3. Find the rule (Rule 1–Rule 5) you want to use.

4. Select the Preset from the drop-down list.

5.2 Choose the trigger type (simple)

Most users start with either TSL or OSC (software control).

- To trigger the rule using TSL:
  - Set the TSL Address/Index to match your tally source.
  - Select which Tally Bit (1–4) should control this rule.
- To trigger the rule using OSC:
  - Enter the OSC Path (for example, /tally/cam1).
  - Leave the match mode at the default “Trigger” unless you have a specific need.

Keep it simple
Start with one segment and one rule. After you confirm the trigger works, copy the same approach to additional segments/rules.

5.3 Test the rule

Use the rule Active switch to quickly test how the preset looks on the segment. For normal operation, the Active state is typically controlled by your selected protocol (TSL, OSC, Pro-Bel, Ember+, or MQTT).

6. Presets and How They Affect Rules

Presets are designed to make your configuration scalable. Instead of changing colors/effects in many rules, you define a preset once and reuse it.

6.1 Configure a preset

1. Open Dashboard → LED Presets.
2. Select a preset (Preset 1–Preset 10).
3. Set the name and color.
4. Optionally configure transitions/effects.

6.2 Assign presets to rules

In Segment Settings, each rule has a Preset selector. When that rule becomes active, the segment displays the selected preset.

If multiple rules are active on the same segment, the rule with the highest priority (lowest rule number) is displayed.

6.3 Recommended naming convention

Clear names make maintenance easier. Examples:

- RED - On Air
- GREEN - Preview
- YELLOW - Warning
- BLUE - Info
- WHITE - Identify

7. Network and Services

This section explains the key network settings and how the device allocates network resources (sockets).

7.1 IP configuration (DHCP vs Static)

DHCP (default): the device obtains its IP address automatically from your DHCP server.
Static: you manually define IP address, subnet mask, and gateway. Use static addressing when you need a predictable device address.

Link-local fallback (AutoIP)
If DHCP is enabled but no DHCP server responds, the device assigns a link-local address (169.254.x.x). You can still access the web interface from a computer on the same link.

Best practices:

- Use DHCP reservations if you want the simplicity of DHCP with a stable IP address.
- Keep all control systems (TSL/Pro-Bel/OSC/Ember+/MQTT) on the same routed network, or ensure correct routing/firewall rules.
- Document the final IP address and ports used for your installation.

7.2 Socket allocation

The device can run multiple services, but the Ethernet controller has a limited number of hardware sockets. Socket allocation lets you choose how many simultaneous connections each service can use.

How it works (simple):

- One socket is reserved for system traffic (DHCP / NTP / Discovery).
- An additional socket may be reserved for the Management Console.
- The remaining sockets are shared by user services (Web, TSL, Pro-Bel, Ember+, OSC, MQTT, Syslog).

Default socket allocation

HTTP: 3 sockets
TSL: 1 socket
Ember+: 0 sockets
Pro-Bel: 0 sockets
OSC: 0 sockets

You can change this in the web interface under Network & Services → Socket Allocation.

7.3 Time (NTP) and timezone

NTP keeps the device time accurate. Correct time improves log readability and troubleshooting.

- Set the NTP server IP address.
- Set your timezone (or timezone offset).

7.4 Syslog

Syslog is recommended for professional environments. When configured, the device sends log messages to your syslog server (UDP port 514).

To enable syslog:

- Enter the syslog server IP address in the web interface.
- Ensure UDP 514 is allowed between the device and the syslog server.

8. Triggering Rules via Network Protocols

Rules can be triggered by several industry-standard protocols. Depending on your license and configuration, you may use one or combine multiple.

8.1 Protocol overview

Service	Transport	Default port	Notes
TSL (Tally)	TCP	8900	Broadcast tally control. Mapping is configured per rule.
Pro-Bel SW-P-08	TCP	2000	Router/tally protocol. One socket per client.
OSC	UDP	8000	Software control (automation/show control). Mapping is configured per rule.
Ember+	TCP	9000	Broadcast control/monitoring. Requires Ember+ license.
MQTT	TCP	1883	Automation integration. Requires MQTT license and a broker.

8.2 TSL (Tally)

TSL is commonly used to transport tally states. Each rule can listen to a specific TSL address and tally bit.

Setup summary:

- Allocate at least 1 TSL socket.
- Confirm the TSL port (default 8900).
- In the rule settings, set the TSL address/index and which tally bit (1–4) should drive the rule.

8.3 OSC

OSC (Open Sound Control) is a simple UDP protocol used by many applications for real-time control.

Setup summary:

- Allocate 1 OSC socket.
- Confirm the OSC listen port (default 8000).
- In the rule settings, set the OSC Path you will send (for example, /tally/cam1).

OSC matching
Most installations can use the default OSC match mode “Trigger” (value > 0). Advanced matching (Exact/Range/String) is available for special cases.

8.4 Pro-Bel (SW-P-08)

Pro-Bel SW-P-08 is often used in broadcast routing and tally environments. Device can accept Pro-Bel connections and update rule states based on received commands.

Setup summary:

- Allocate the required number of Pro-Bel sockets (one per client).
- Confirm the Pro-Bel port (default 2000).
- Set the Pro-Bel Matrix ID if your environment requires it (default 1).
- For advanced addressing details, see Appendix B.

8.5 Ember+

Ember+ is a control and monitoring protocol used in professional broadcast systems.
When Ember+ is licensed and enabled, controllers can read and set rule active states and edit configuration values.

Setup summary:

- Ensure your device has an Ember+ license enabled.
- Allocate Ember+ sockets for the number of concurrent Ember+ controllers.
- Connect your Ember+ controller to the device IP and Ember+ port (default 9000).
- Navigate to: <Device> → Rules → Segment X Rules → Rule Y → Active.

8.6 MQTT

MQTT is useful for automation and integration with control systems (dashboards, scripting, building management, etc.).
The device connects to your MQTT broker and receives commands via topics that end with /cmd.

Setup summary:

- Ensure your device has an MQTT license enabled.
- Allocate 1 socket for MQTT.
- Set the broker IP address and port (default 1883).
- Set a topic prefix (default: xichtee).
- Optionally set username and password.

MQTT best practice
Use a dedicated topic prefix per site and keep the broker on the same LAN/VPN. Use broker authentication where possible. For examples, see Appendix B.

9. Troubleshooting

If something does not work as expected, check the following items.

9.1 Cannot open the web interface

- Verify the device has power and the Ethernet link is up.
- Confirm the IP address (DHCP lease list, network scan, or link-local mode).
- Confirm you are using http:// (not https://).
- Check whether your network blocks access to TCP port 80.

9.2 Rules do not trigger

- Check socket allocation: the protocol service must have at least one allocated socket.
- Verify you configured the correct port numbers and that your sending device targets those ports.

- For TSL/OSC, verify the rule mapping fields (TSL address/bit, OSC path).
- Use the rule Active switch to confirm the preset looks correct on the segment.

9.3 Resetting configuration

If you are locked out or the network settings are unknown, a factory reset may be required. Factory reset restores default settings including the default admin credentials.

Important
Factory reset removes your saved configuration. If possible, create a backup before resetting.

Appendix A: Default Values (Reference)

These values are provided as a quick reference. Your device may differ if your system integrator has customized the configuration.

Parameter	Value
DHCP	Enabled by default
HTTP Port	80 (TCP)
Ember+ Port	9000 (TCP)
TSL Port	8900 (TCP)
Pro-Bel Port	2000 (TCP)
OSC Port	8000 (UDP)
MQTT Port	1883 (TCP)
Discovery Port	33333 (UDP)
Syslog Port	514 (UDP)
Management Console	2323 (TCP)

Appendix B: Protocol Mapping Quick Reference (Advanced)

This appendix is intended for system integrators. It summarizes how rules are mapped for Pro-Bel and MQTT.

B.1 Pro-Bel destination mapping

Each Pro-Bel destination number targets one Segment/Rule pair.

Mapping rules:

- If your device is configured for more than 5 segments: Destination = (SegmentIndex × 5) + RuleIndex.
- If your device is configured for 5 segments or fewer (legacy compatibility): Destination = (SegmentIndex × 20) + RuleIndex.
- SegmentIndex starts at 0 for Segment 1. RuleIndex starts at 0 for Rule 1.

Example (more than 5 segments):

Target	Pro-Bel destination
Segment 1 / Rule 1	Destination 0
Segment 1 / Rule 5	Destination 4
Segment 2 / Rule 1	Destination 5

B.2 MQTT topics and basic commands

The device subscribes to two command topics:
<prefix>/<device-uuid>/cmd
<prefix>/all/cmd

The device publishes status as JSON to:

- <prefix>/<device-uuid>/status

Command payloads can be JSON or key=value pairs. Examples:

Action	Example payload
Reboot device	{“cmd”:”reboot”}
Set Rule Active	{“cmd”:”set_rule”,”seg”:0,”rule”:0,”active”:1}
Clear Rule Active	{“cmd”:”set_rule”,”seg”:0,”rule”:0,”active”:0}