



Remote Power Management

RPD-406

Operation Manual



FCC Information

This is a Class A product. When used domestically, this device may cause interference to communications equipment. Users are advised to take appropriate protective measures.

This product has been tested and shown to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy. If not installed and used in accordance with this manual, it may cause harmful interference to radio communications. Operation in a residential area may require the user to correct interference at their own expense.

RoHS Information

This product complies with RoHS requirements.

Safety Information

	Caution symbol. Refer to the cautions and instructions in this manual to avoid personal injury or equipment damage.
	Electric shock hazard symbol. High voltage may be present inside this product; do not touch. The equilateral triangle containing a lightning bolt and arrowhead warns users that uninsulated dangerous voltage is present inside the product enclosure and may be of sufficient magnitude to pose a risk of electric shock.
	Chassis ground symbol.

Warning: To reduce the risk of fire or electric shock, do not expose this equipment to rain or moisture. Dangerous high voltage is present inside the enclosure. Do not open the enclosure. Servicing must be performed by qualified personnel only.

Important Safety Instructions

1. Strictly follow all warnings and operating instructions in this manual and on the device. Keep this manual in a safe place. Do not operate this device until you have read all safety and operating instructions.
2. Set the maximum over-current protection for the power circuit according to the rated current information on the device label. Follow all applicable national regulations, safety codes, and breaker tolerance requirements.
3. Connect this device only to a properly grounded power outlet or grounded power system.
4. Ensure that the total output current of all connected equipment does not exceed the rated current shown on the device label.
5. Replacing the battery with an incorrect type may cause an explosion. Dispose of used batteries according to applicable regulations.
6. If the power supply is unstable, measurement results from this device may be inaccurate.
7. Do not use this device near water or in humid locations. To reduce the risk of fire or electric shock, do not expose this device to rain or moisture.
8. Clean only with a dry cloth.
9. Use only attachments and accessories specified by the manufacturer.
10. All servicing must be performed by qualified service personnel. Return the device for service if it is damaged in any way, for example:
 - The power cord or plug is damaged.
 - Liquid has been spilled or objects have fallen into the equipment.

- The equipment has been exposed to rain or moisture and does not operate properly, or has been dropped.

Do not attempt to service this equipment yourself. Opening the enclosure may expose you to dangerous voltage or other hazards. Contact your dealer for assistance.

11. Do not allow objects or liquids to enter the equipment. Contact with hazardous voltage points or short circuits may cause fire or electric shock.
12. Refer to the safety symbols on the equipment enclosure.
13. No one except qualified service personnel should adjust or repair this equipment.

User Information

The manufacturer reserves the right to modify the information, documentation, and specifications contained in this manual without prior notice. The manufacturer makes no warranty, express or implied, regarding merchantability or fitness for a particular purpose, including any manufacturer software described in this manual.

If a defect in the software is discovered after purchase, the purchaser (not the manufacturer, distributor, or reseller) shall bear all necessary service costs, repair liability, and any incidental or consequential damages caused by software defects.

The manufacturer is not responsible for radio or television interference caused by unauthorized modification of this device; the user must correct such interference.

If the operating voltage is not configured correctly before use, the manufacturer is not liable for resulting damage. Always verify the voltage setting before operation.

The manufacturer warrants this product to the original end user for one (1) year from the date of purchase against defects in materials and workmanship. During the warranty period, subject to proof of purchase, defective products or components will be repaired or replaced at no charge for parts or labor, at the manufacturer's discretion, to restore normal operation. Replacement may be new or refurbished with equivalent or greater value, as determined by the manufacturer. This warranty does not apply to products that have been modified, misused, altered, damaged by disaster, or operated outside normal conditions.

This warranty does not apply to defects caused by installation or use by any third party (including customers or end users), negligent or improper operation, unauthorized modification, repair not performed according to the manufacturer's written instructions, normal wear, disassembly, connection to incompatible equipment or software, integration into systems not intended for this product, connection of incompatible hardware or software, computer networks containing viruses, modified or interrupted carrier networks, or repair by unauthorized personnel.

If your device does not operate properly, contact the service provider listed on the support and warranty card included with the product packaging.

Contents

FCC Information	1
RoHS Information	2
Safety Information	3
Important Safety Instructions	3
User Information	5
Contents	6
Chapter 1 Product Introduction	9
1-1 Product Introduction	9
1-2 Applications	9
1-3 Features	9
1-4 Hardware Description	9
1-5 Package Contents	10
Chapter 2 Hardware Installation	11
2-1 Rack Mounting	11
2-2 Product Installation	11
Chapter 3 Initial Connection and Login	12
3-1 IP Search Utility	12
3-2 Network Connection	13
3-3 Login	13
3-4 Web Interface	15
3-5 Change IP Settings	16
Chapter 4 Device Monitoring and Parameters	18
4-1 Outlet	18
4-1-1 Monitoring Screen	18
4-1-2 Parameter Settings	19
4-2 Schedule	20
4-2-1 Add Schedule	20
4-2-2 Edit Schedule	22

4-3 Ping Monitor	24
4-3-1 Add Ping Monitor	25
4-3-2 Edit Ping Monitor	26
Chapter 5 Logs and Notifications	29
5-1 Event History	29
5-2 Notification List	30
5-2-1 Add Notification	31
5-2-2 Edit Notification	33
5-2-3 Delete Notification	34
Chapter 6 Accounts and Security	35
6-1 User Accounts	35
6-1-1 Add User	35
6-1-2 Edit User	36
6-2 Password Policy	38
Chapter 7 System Settings	40
7-1 System Parameters	40
Screen When Entering Device URL	40
7-2 Network	42
7-3 Network Service	43
7-4 Time Sync	46
7-5 Information	47
7-6 Firewall	48
7-6-1 Add Firewall Rule	49
7-6-2 Edit Firewall Rule	50
Chapter 8 Maintenance, Backup & Restore	
8-1 Backup and Restore	
8-2 System Maintenance	54
8-3 Firmware Update	55
Chapter 9 Engineering Mode	60
9-1 LDAP	60
9-1-1 LDAP Test	61

9-2 RADIUS / TACACS+	62
9-2-1 RADIUS / TACACS+ Test	63
9-3 SNMP Agent	64
9-4 Mail Server	66
9-4-1 Test Mail	67
9-5 Alert Service	67
9-6 Syslog	68
9-6-1 Add Syslog	69
9-6-2 Edit Syslog	71
Appendix	74
Factory Reset	74
Hardware reset (pinhole)	74
Web UI reset	74
Warranty	76

Chapter 1 Product Introduction

1-1 Product Introduction

RPD-406 integrates switched outlet control, web-based management, event logging, email and SNMP notifications, and scheduling. IT staff can monitor outlet status and resolve power-related issues remotely over the network, reducing downtime and on-site visits.

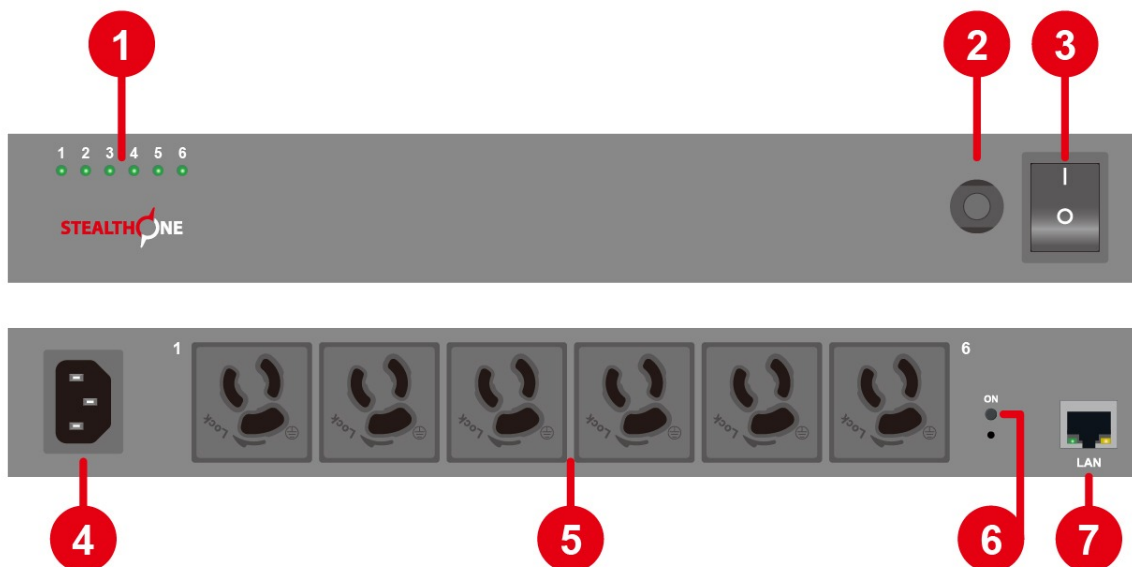
1-2 Applications

- Data center and server room equipment monitoring and management
- Computer center power management for government and enterprise sites
- Factory equipment power control
- Network equipment power monitoring
- Other power equipment monitoring and remote control applications

1-3 Features

- Front-panel LEDs show the on/off state of each outlet.
- Remote administrators can control outlets through a web browser, eliminating on-site visits.
- Supports email and Pushover alert delivery.
- Supports SNMP v1/v2c and v3 for network management integration.
- Supports Syslog for centralized log collection.
- Records user actions and alarm events for later review.
- Provides remote firmware update.
- Built-in overload circuit breaker protects connected equipment.
- 10/100 Mbps Ethernet management port.

1-4 Hardware Description



1	Outlet status LEDs — LEDs 1–6 on the front panel; green indicates the corresponding outlet is energized
2	Circuit breaker — Over-current protection (front panel, right side)
3	Power switch — Main rocker power switch (I/O)
4	Power inlet — IEC C14 AC inlet (rear panel)
5	Outlets 1–6 — Six switched NEMA 5-15R outlets with locking mechanism (rear panel)
6	RESET — Pinhole factory-reset button (rear panel; use a straightened paper clip)
7	LAN — RJ45 Ethernet port for management (rear panel)

1-5 Package Contents

	Remote power PDU × 1
	Power cord × 1
	Quick start / warranty card × 1

If any items are missing or defective, contact your dealer within seven (7) days of purchase for replacement.

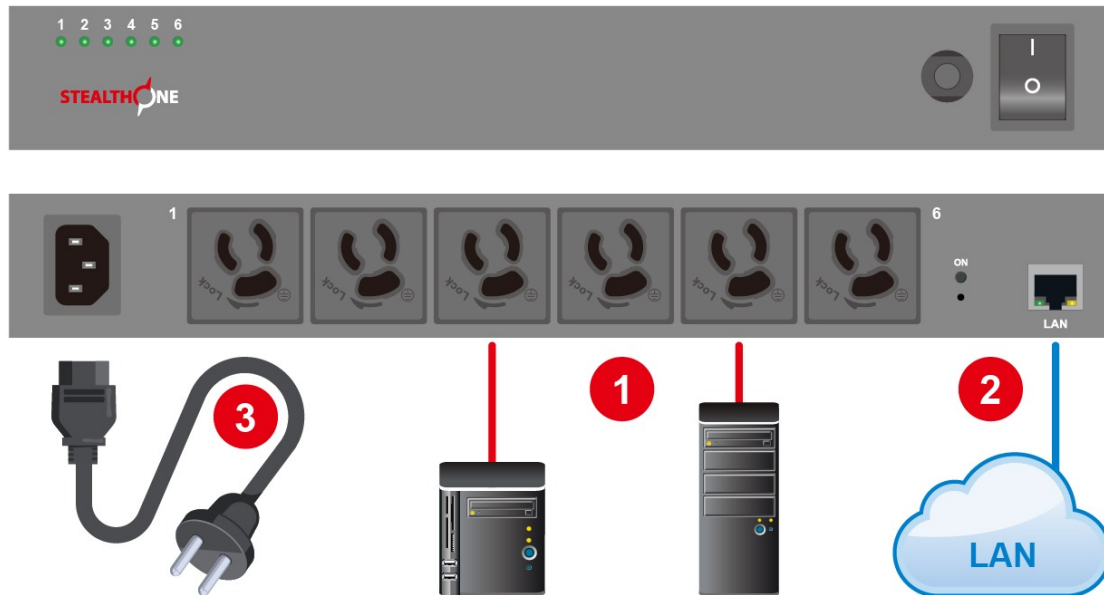
Chapter 2 Hardware Installation

2-1 Rack Mounting

RPD-406 fits standard 19-inch racks. Use the rack mounting accessories included in the package. Install the brackets on the unit first, then mount the assembly in the cabinet.

2-2 Product Installation

To ensure proper operation, follow these installation steps as shown in the diagram:



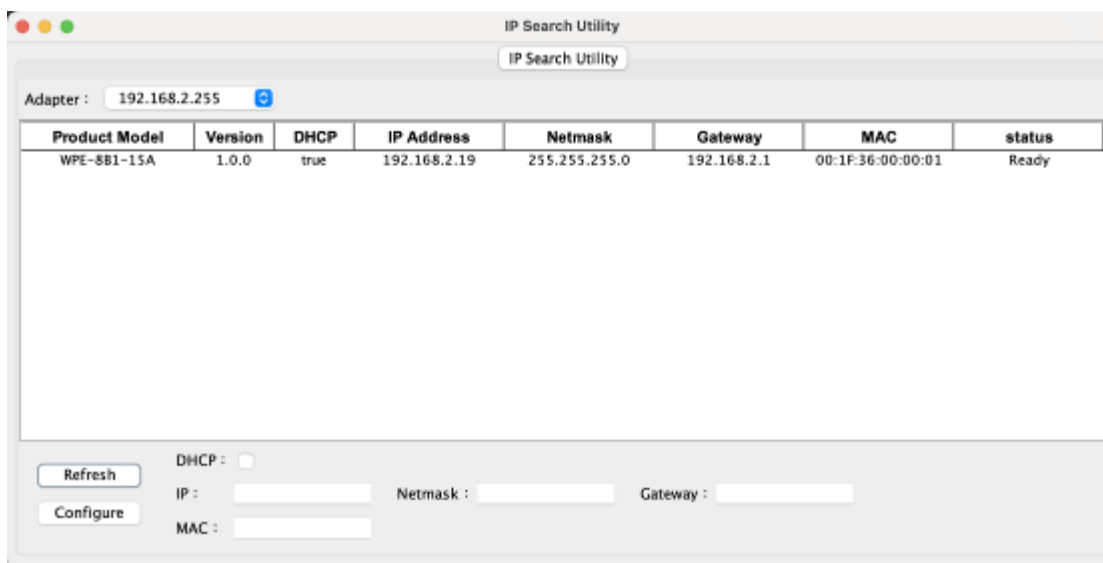
1. **Connect devices:** Plug your servers or equipment into the output outlets (1–6) on the rear panel.
2. **Network connection:** Connect a standard Ethernet cable to the LAN port for remote management.
3. **Power connection:** Plug the supplied power cord into the power inlet, then into a grounded AC outlet.

Chapter 3 Initial Connection and Login

This chapter covers the steps required for first-time connection and Web UI login. Follow the flow for IP search, network connection, login, screen layout, and changing IP settings.

3-1 IP Search Utility

This section explains how to use the Java IP Search Utility on Windows, macOS, Linux, and other platforms to discover devices on the local network and change IP settings or DHCP mode. Because the utility uses UDP broadcast packets, it cannot find devices across routers.



Adapter: Select the network interface used to send search packets. Choose a NIC on the same subnet as the device (some Windows versions allow only one NIC for broadcast).

Product List

Discovered devices appear in the list. Field descriptions:

Product Model	Device model name.
Version	Firmware version.
DHCP	`true` means the IP is assigned by a DHCP server; `false` means a static IP.
IP Address	Current IPv4 address of the device.
Netmask	Device subnet mask.
Gateway	Device default gateway.
MAC	Device MAC address.
Http Open	`true` means the HTTP management interface is enabled.

Http Port	HTTP port (default 80).
Https Open	`true` means HTTPS is enabled.
Https Port	HTTPS port (default 443).

Configuration

After selecting a device in the product list, change network parameters below and apply:

DHCP	When checked, the device obtains an IP via DHCP; uncheck to enter IP fields manually.
IP	Set the device IPv4 address (when DHCP is off).
NetMask	Set the device subnet mask.
Gateway	Set the device default gateway.
MAC	Shows the selected device MAC address (read-only) for verification.

Refresh

Search again for devices on the local network and refresh the product list.

Configure

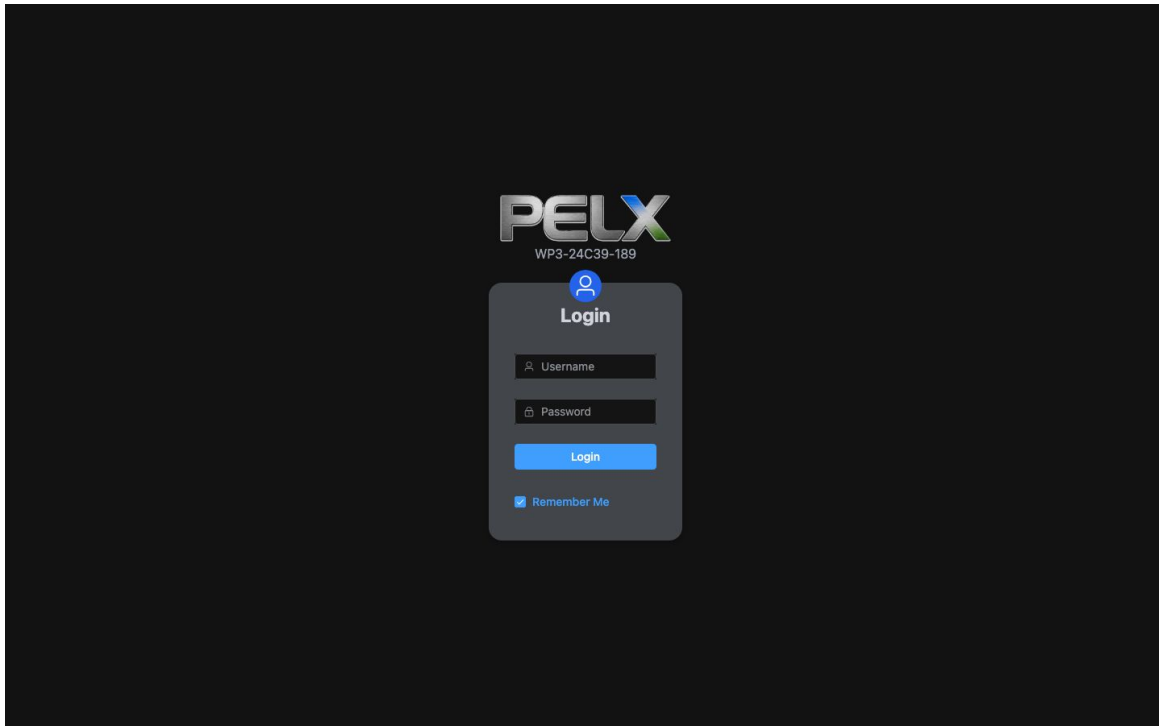
Write configuration to the selected device and reboot it. After reboot, click **Refresh** to read updated network information.

3-2 Network Connection

After connecting the network cable, the device obtains an IP address via DHCP (default **192.168.1.100** if no DHCP server is available). Discover the assigned IP with IP Search Utility (see 3-1 IP Search Utility).

3-3 Login

Navigation: Enter the device IP in a browser (when **Show Device List** is off), or select a device from the device list to open the login page. Factory default credentials are **admin** / **admin**. On a new device or after factory reset, sign in with **admin** / **admin** and click **Login**.



Field Descriptions

Username	Enter an account with access permission; it must match a user defined under Permissions .
Password	Enter the password for the account. Repeated failures may lock the account or trigger password policy restrictions.
Remember Me	When checked, the browser keeps login information on the next visit; do not use on shared computers.

Button Descriptions

Login	Sign in when credentials are valid; first login may require a password change.
--------------	--

On a new device or after factory reset, the system **requires a password change** after successful login (subject to password policy). Set a new password and click **OK** to continue. Use the new password thereafter; the default **admin** password is no longer valid.

Change Password

* New

* Confirm

Confirm

Field Descriptions

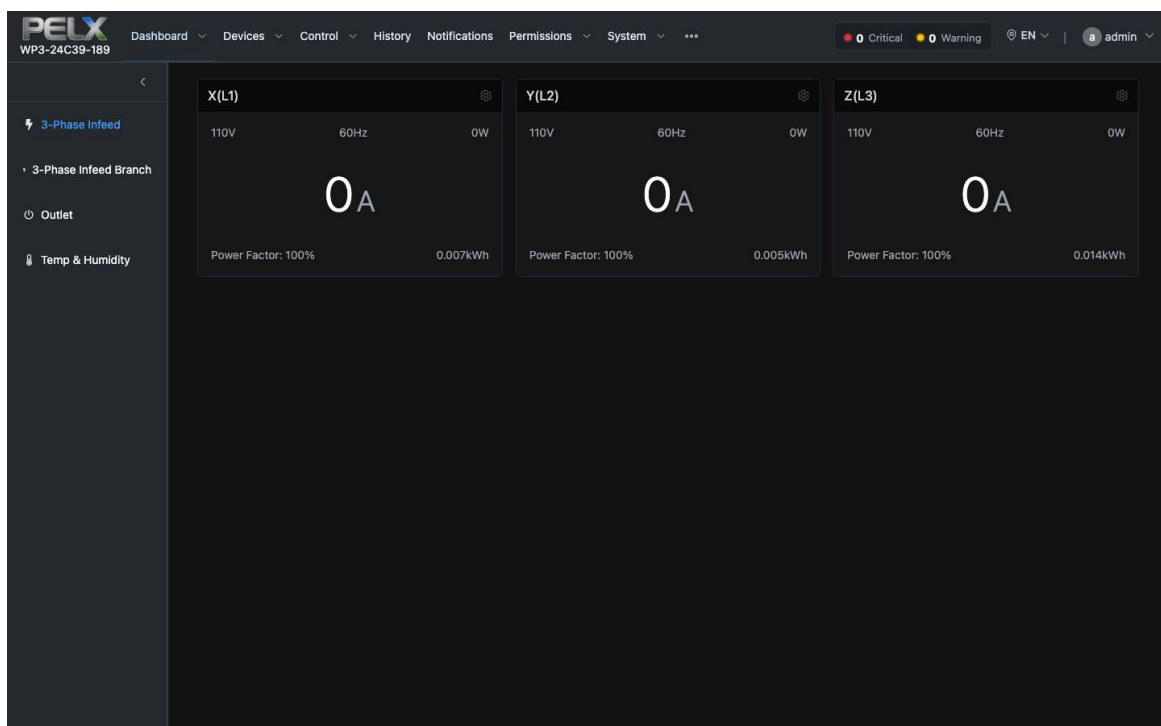
- New Password** Enter the new login password; it must meet the password policy if enabled.
- Confirm New Password** Re-enter the new password for confirmation; both entries must match.

Button Descriptions

- OK** Submit the new password and complete first-login setup.

3-4 Web Interface

After login, select a menu item to open the working screen. The layout is described below:



Field Descriptions

User Bar	Shows the current locale and signed-in account.
Menus	The top bar is the main menu; the left sidebar lists sub-items for the selected menu; the right panel shows the selected page.
Main Panel	Shows monitoring values, forms, or lists for the selected menu—the main work area.

The following sections describe each menu in detail.

3-5 Change IP Settings

Navigation: System > Network. If the device IP is assigned via DHCP and you need a different address, open **System**, then **Network** from the dropdown.

The screenshot shows a dark-themed network configuration window with two main panels: IPv4 on the left and IPv6 on the right. The IPv4 panel includes a DHCP toggle switch (currently off), a MAC address field, and fields for IP Address, Netmask, Gateway, DNS 1, and DNS 2, each preceded by a red asterisk indicating they are required. The IPv6 panel includes fields for IPv6 Address, Prefix Length (set to 64 with up/down arrows), IPv6 Gateway, IPv6 DNS 1, and IPv6 DNS 2. At the bottom right of the window are 'Cancel' and 'Save' buttons.

Field Descriptions

IPv4	
DHCP	When enabled, IPv4 is assigned by the LAN DHCP server; disable to enter fields manually below.
MAC	Shows this device's Ethernet MAC address (read-only) for network management or ARP lookup.
IP Address	Sets the device IPv4 address; must match subnet and gateway; you may need to sign in again after changing it.

Subnet Mask	Sets the IPv4 subnet mask defining the LAN range (commonly 255.255.255.0).
Default Gateway	Sets the default IPv4 gateway, usually the router IP.
DNS Server 1	Primary DNS server for name resolution; use a reachable DNS server.
DNS Server 2	Secondary DNS server as backup when primary fails; may be blank.

IPv6

IPv6 Address	Sets the device IPv6 address; must match prefix length and gateway.
Prefix Length	Sets the IPv6 prefix length (commonly 64) defining the LAN range.
IPv6 Gateway	Sets the IPv6 default gateway for outbound traffic.
IPv6 DNS Server 1	Primary IPv6 DNS server address.
IPv6 DNS Server 2	Secondary IPv6 DNS server address; may be blank.

Button Descriptions

Cancel	Discards changes and restores values from when the page was opened.
Save	Saves and applies network settings; reconnect with the new address if the IP changed.

Chapter 4 Device Monitoring and Parameters

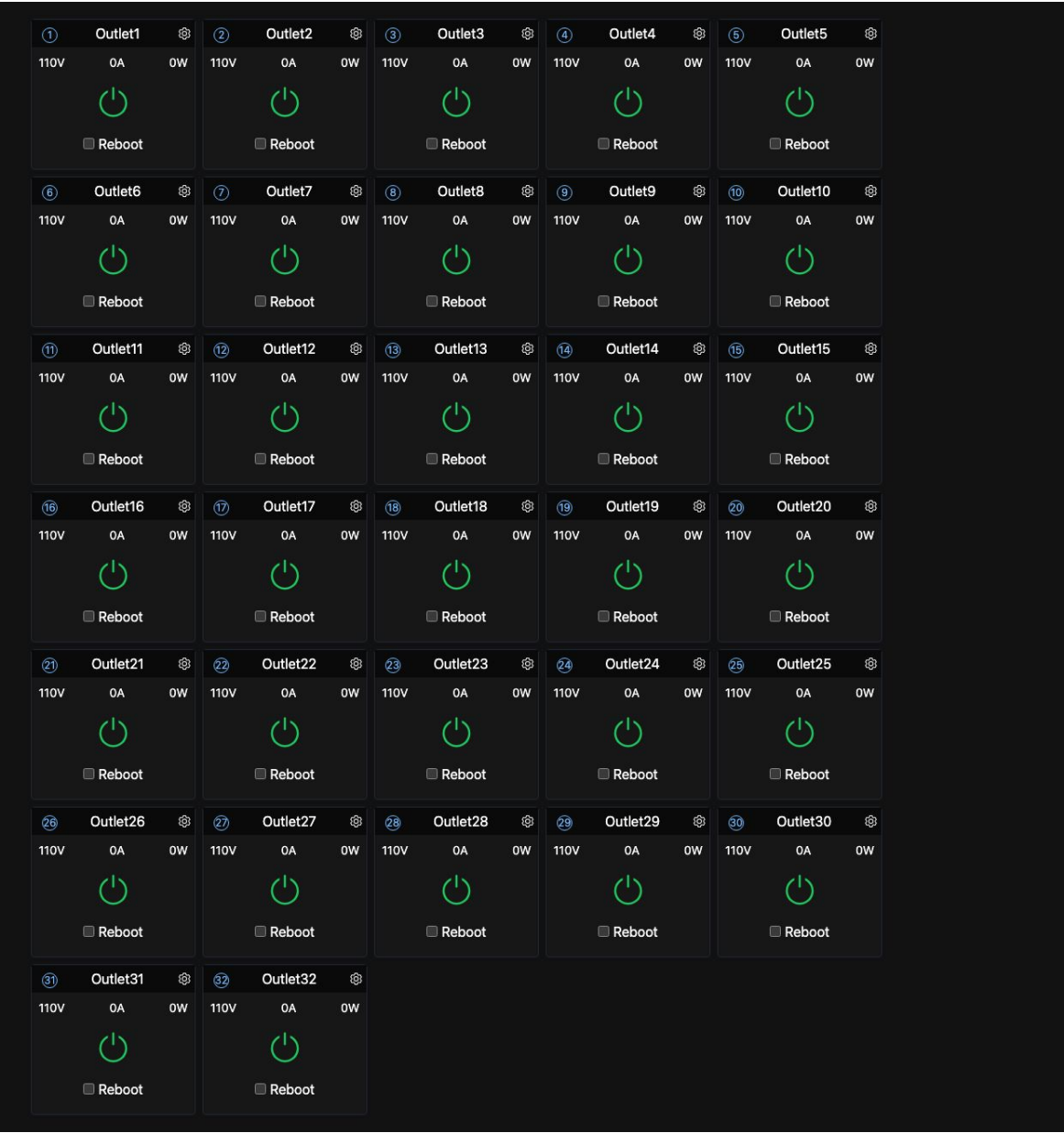
This chapter describes monitoring and configuration for outlets, schedules, ping monitors, and related settings.

4-1 Outlet

Shows outlet on/off state and allows direct switching from the web UI.

4-1-1 Monitoring Screen

Shows the power state of each outlet and allows direct switching from the web UI.



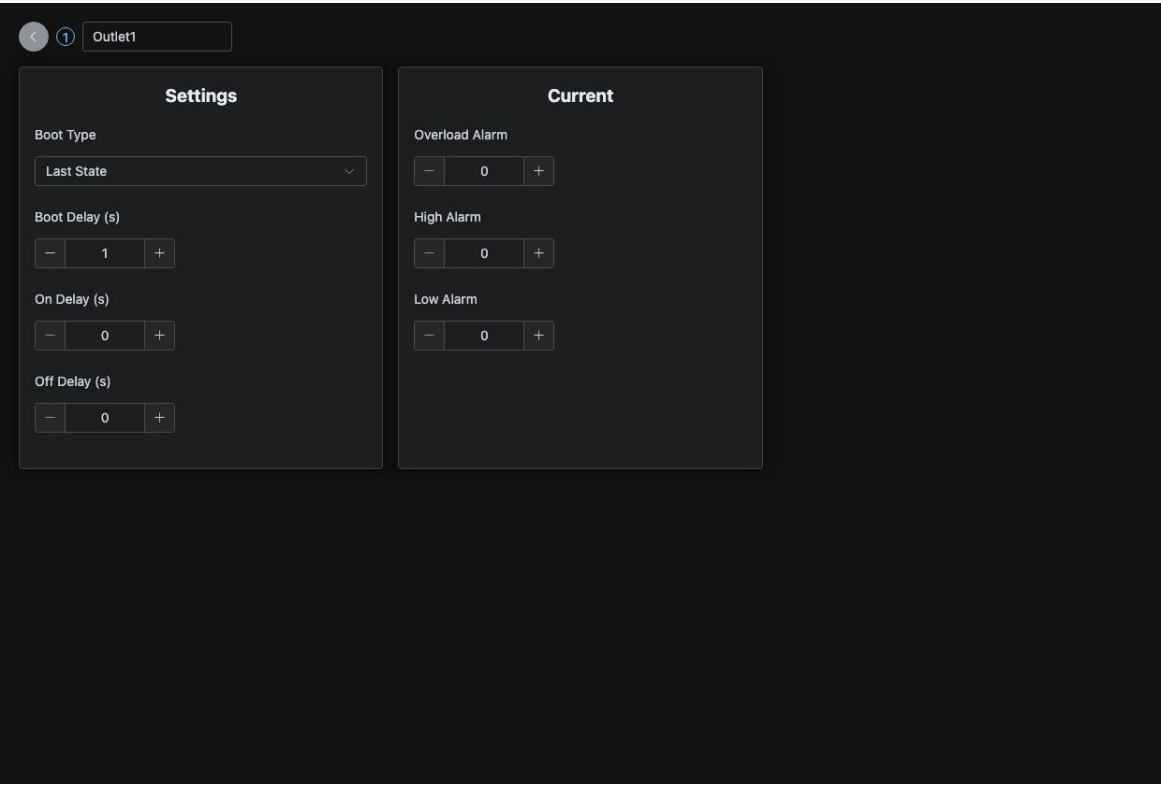
Field Descriptions

Outlets 1-6 Shows outlet name and index matching chassis and panel labels.

Power Icon	Shows outlet power state; green means energized. Click the icon to toggle the outlet.
Reboot	When checked, performs a power cycle (off then on) for remote device recovery.

4-1-2 Parameter Settings

The example below uses outlet 1 (Outlet1). Click the  icon in the upper-right corner of the outlet tile to open parameter settings. All outlets use the same layout.

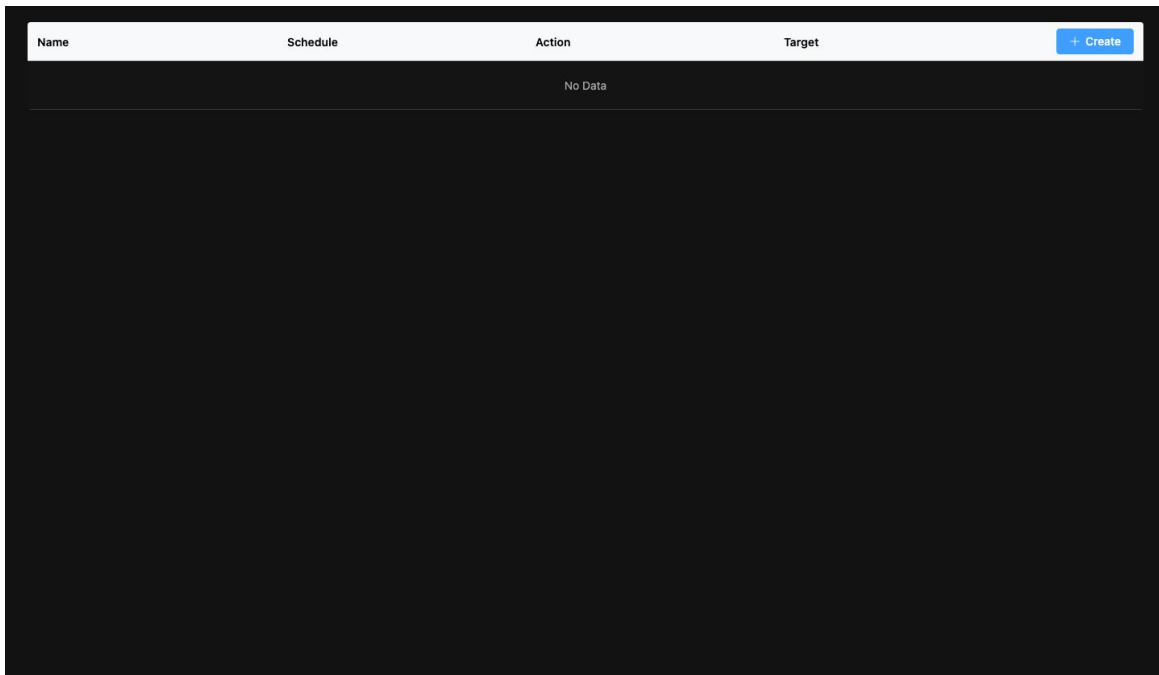


Field Descriptions

Boot Type	Default outlet power state after device reboot or power restoration; choose Off, On, Reboot, or Last State from the dropdown. • Off: Outlet stays off after power returns. • On: Outlet turns on automatically after power returns. • Reboot: Outlet power-cycles after restore—useful for rebooting downstream equipment remotely. • Last State: Restores the state before power loss.
Boot Delay	Delay in seconds before energizing the outlet after device power-on. Set different values per outlet for sequential power-on to avoid simultaneous inrush overload. For example: outlet 1 = 0 s, outlet 2 = 30 s, outlet 3 = 60 s.
On Delay	Delay in seconds before energizing when turning the outlet on remotely.
Off Delay	Delay in seconds before de-energizing when turning the outlet off remotely.

4-2 Schedule

Navigation: Control > Schedule. This page creates scheduled tasks to run preset actions on devices or outlets at specified times. If **Skip Holidays** is checked, the schedule does not run on configured holidays.



Field Descriptions

Name	Schedule name for identification.
Schedule	Summary of run time or recurrence.
Action	Operation when the schedule fires (e.g., turn outlets on or off).
Target	Device, group, or outlets the schedule applies to.

Button Descriptions

Add	Opens the form to create a schedule.
Running	Toggles whether the schedule runs. When Running , it fires at configured times; click to switch to Stopped and click again to resume.
Delete	Deletes this schedule.

4-2-1 Add Schedule

Click **Add** to open the form below.

Name	Schedule	Action	Target	+ Create
No Data				

Field Descriptions

General

Name	Schedule name.
Action	Operation when the schedule fires (e.g., turn outlets on, off, or reboot).
Skip Holidays	When enabled, this schedule does not run on holidays.
Run Missed on Boot	Whether to run missed schedules after device reboot.

Schedule

Recurrence: How often the schedule repeats; choose from the dropdown. After selecting recurrence, matching time fields appear (hour, minute, weekday, day, month, etc.).

- **Specific Date:** Run yearly on the specified month, day, hour, and minute; list summary shows Yearly M/D HH:MM.
- **Monthly:** Run monthly on the specified day, hour, and minute.
- **Weekly:** Run weekly on the specified weekday, hour, and minute.
- **Daily:** Run daily at the specified hour and minute.
- **Hourly:** Run hourly at the specified minute.

Hour	Hour to run (0–23); hidden for Hourly recurrence.
Minute	Minute to run (0–59).
Weekday	Weekday for weekly runs; shown only for Weekly recurrence.

Day	Day of month for monthly or specific-date runs; shown for Monthly and Specific Date recurrence.
Month	Month for specific-date runs; shown only for Specific Date recurrence.

Targets

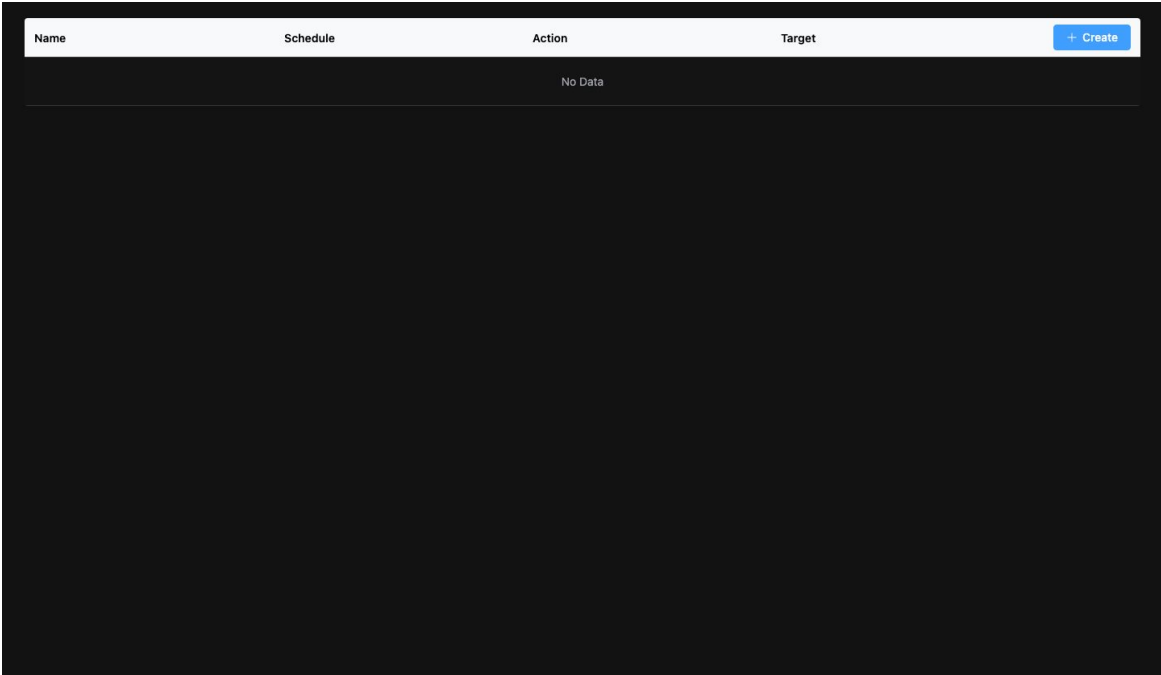
Select outlets this schedule applies to (Outlet1–Outlet6).

Button Descriptions

Cancel	Discards changes and returns to the schedule list.
Save	Saves the schedule and returns to the list.

4-2-2 Edit Schedule

Click an item in the list to open the edit screen.



Field Descriptions

General

Name	Schedule name.
Action	Operation when the schedule fires (e.g., turn outlets on, off, or reboot).
Skip Holidays	When enabled, this schedule does not run on holidays.
Run Missed on Boot	Whether to run missed schedules after device reboot.

Schedule

Recurrence: How often the schedule repeats; choose from the dropdown. After selecting recurrence, matching time fields appear (hour, minute, weekday, day, month, etc.).

- **Specific Date:** Run yearly on the specified month, day, hour, and minute; list summary shows Yearly M/D HH:MM.
- **Monthly:** Run monthly on the specified day, hour, and minute.
- **Weekly:** Run weekly on the specified weekday, hour, and minute.
- **Daily:** Run daily at the specified hour and minute.
- **Hourly:** Run hourly at the specified minute.

Hour	Hour to run (0–23); hidden for Hourly recurrence.
Minute	Minute to run (0–59).
Weekday	Weekday for weekly runs; shown only for Weekly recurrence.
Day	Day of month for monthly or specific-date runs; shown for Monthly and Specific Date recurrence.
Month	Month for specific-date runs; shown only for Specific Date recurrence.

Targets

Select outlets this schedule applies to (Outlet1–Outlet6).

Button Descriptions

Cancel

Discards changes and returns to the schedule list.

Save

Saves changes and returns to the list.

Delete

Click **Delete** on the right of a list item to open a confirmation dialog.

Name	Schedule	Action	Target	+ Create
No Data				

- Cancel

Closes the dialog without deleting.
-
- OK

Confirms deletion of this schedule.

4-3 Ping Monitor

Navigation: Control > Ping Monitor. This page configures network reachability targets. The device periodically checks whether hosts or services are reachable; on failure, a preset action may run (e.g., outlet reboot).

#	Name	Device IP	Protocol	Execute	Command	Target	+ Create
No Data							

Field Descriptions

Name	Monitor entry name.
------	---------------------

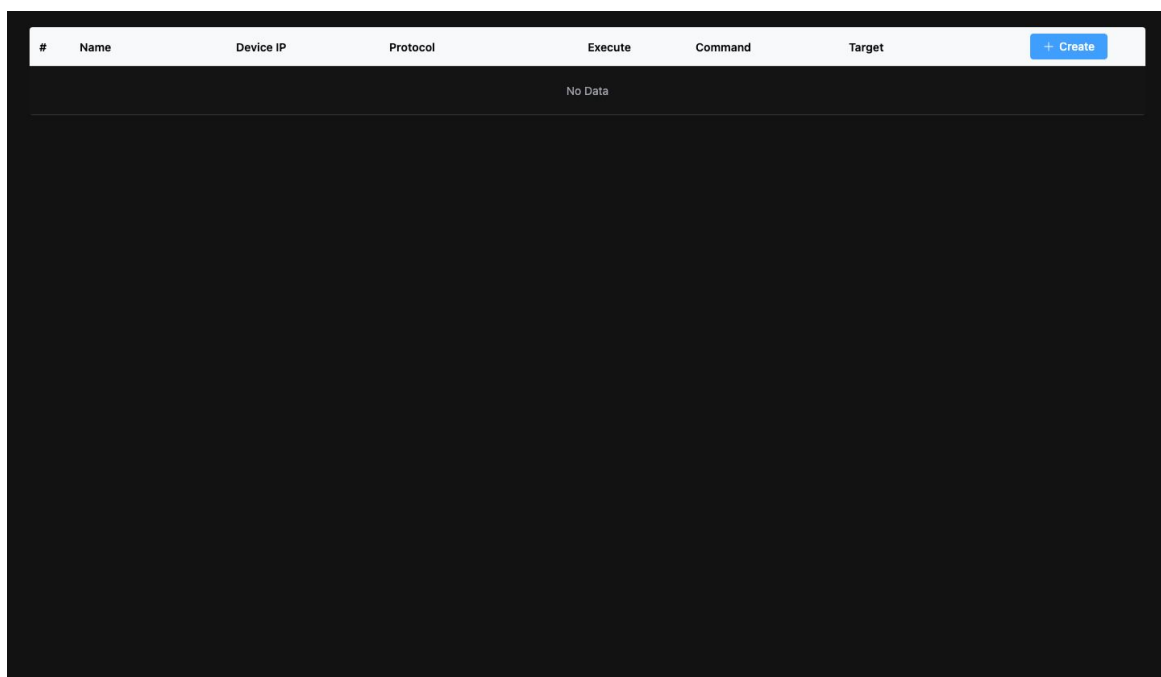
Target Host	IP address or hostname to monitor.
Protocol	Protocol for monitoring (ICMP or TCP).
Run Command on Failure	Whether to run the preset command on failure.
Command	Action on failure (e.g., reboot outlet).
Target	Outlets the command applies to.

Button Descriptions

Add	Opens the form to add a monitor entry.
Running	Toggles whether monitoring runs. When Running , checks run at the configured interval; click to switch to Stopped and click again to resume.
Delete	Deletes this ping monitor entry.

4-3-1 Add Ping Monitor

Click **Add** to open the form below.



Field Descriptions

General	
Name	Monitor entry name.
Protocol	Monitoring method; choose from the dropdown.

- **ICMP:** Ping the target host to verify reachability.

- **TCP:** Check reachability via TCP; enter **Port** when selected.

Target Host	IP address or hostname to monitor.
Port	TCP port; shown only for TCP protocol.
Check Interval (min)	Interval between checks.
Failure Count	Consecutive failures before triggering action.

Command

Run Command on Failure	When enabled, runs the command below on failure.
Recheck Delay (min)	Minutes after running the command before monitoring resumes.
Command	Action on failure (e.g., reboot outlet).

Targets

Select outlets this command applies to (Outlet1–Outlet6).

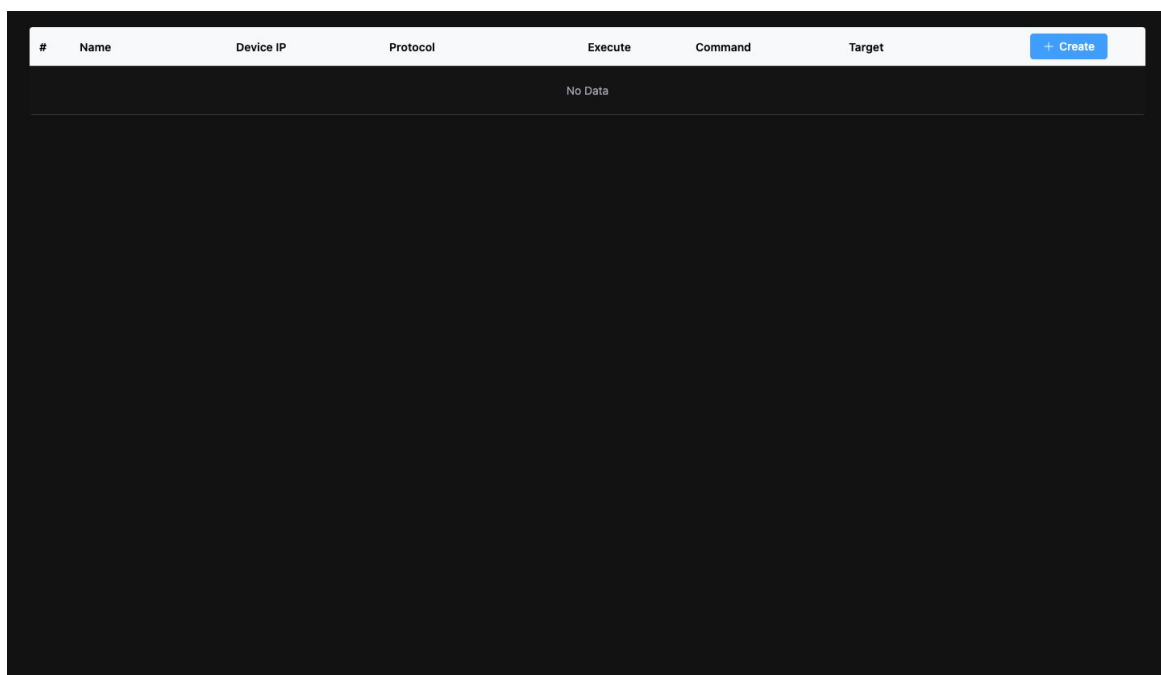
Button Descriptions

Cancel Discards changes and returns to the list.

Save Saves settings and returns to the list.

4-3-2 Edit Ping Monitor

Click an item in the list to open the edit screen.



Field Descriptions

General

Name	Monitor entry name.
Protocol	Monitoring method; choose from the dropdown. • ICMP: Ping the target host to verify reachability. • TCP: Check reachability via TCP; enter Port when selected.
Target Host	IP address or hostname to monitor.
Port	TCP port; shown only for TCP protocol.
Check Interval (min)	Interval between checks.
Failure Count	Consecutive failures before triggering action.

Command

Run Command on Failure	When enabled, runs the command below on failure.
Recheck Delay (min)	Minutes after running the command before monitoring resumes.
Command	Action on failure (e.g., reboot outlet).

Targets

Select outlets this command applies to (Outlet1–Outlet6).

Button Descriptions

Cancel Discards changes and returns to the list.

Save Saves changes and returns to the list.

Delete

Click **Delete** on the right of a list item to open a confirmation dialog.

#	Name	Device IP	Protocol	Execute	Command	Target	+ Create
No Data							

Cancel

Closes the dialog without deleting.

OK

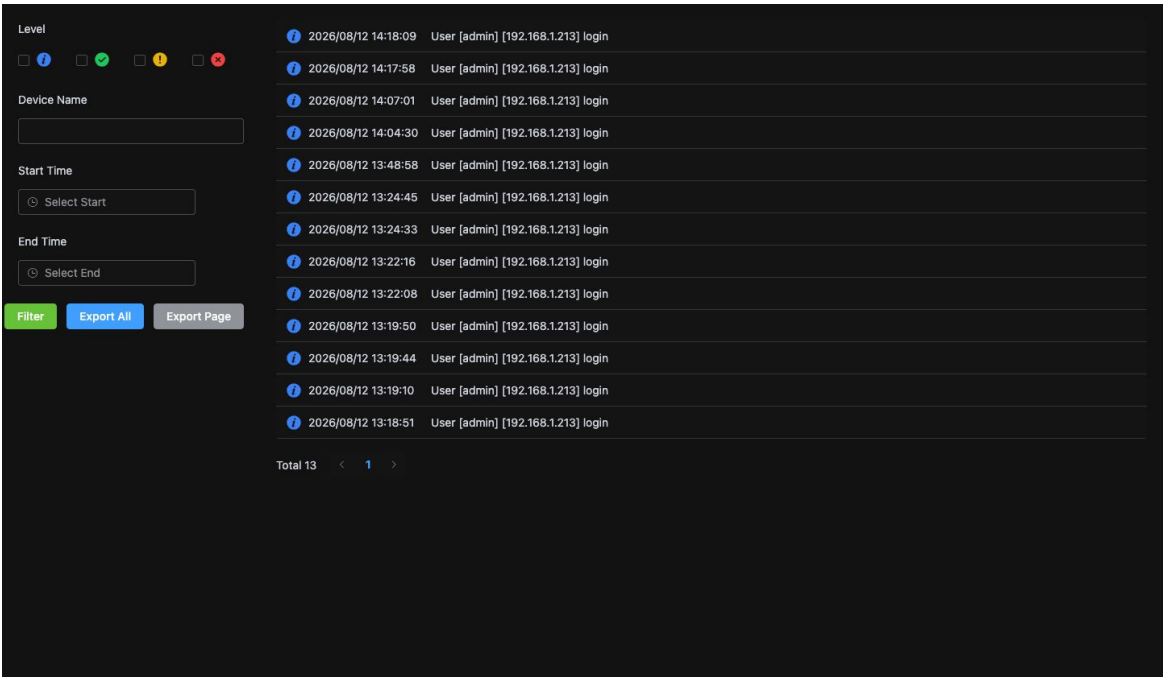
Confirms deletion of this ping monitor entry.

Chapter 5 Logs and Notifications

This chapter explains how to configure alarm and event notifications.

5-1 Event History

Navigation: History > Event History. This menu provides event history for system operations, device actions, and alerts.



Query Field Descriptions

Level	Select event levels to query (multiple selection). Info Success Warning Error
Peripheral Name	Enter keywords to filter peripherals or event content; partial match supported.
Start Time	Query start time; leave blank for no start limit.
End Time	Query end time; leave blank for no end limit.

Button Descriptions

Filter	Re-queries the event list by level, keyword, and time range.
Export All	Exports all matching events as a CSV download.
Export Page	Exports only events on the current page as CSV.

Level	Time	Account and Source IP	Description
Info	2026/08/12 14:18:09	User [admin] [192.168.1.213]	login
Info	2026/08/12 14:17:58	User [admin] [192.168.1.213]	login
Info	2026/08/12 14:07:01	User [admin] [192.168.1.213]	login
Info	2026/08/12 14:04:30	User [admin] [192.168.1.213]	login
Info	2026/08/12 13:48:58	User [admin] [192.168.1.213]	login
Info	2026/08/12 13:24:45	User [admin] [192.168.1.213]	login
Info	2026/08/12 13:24:33	User [admin] [192.168.1.213]	login
Info	2026/08/12 13:22:16	User [admin] [192.168.1.213]	login
Info	2026/08/12 13:22:08	User [admin] [192.168.1.213]	login
Info	2026/08/12 13:19:50	User [admin] [192.168.1.213]	login
Info	2026/08/12 13:19:44	User [admin] [192.168.1.213]	login
Info	2026/08/12 13:19:10	User [admin] [192.168.1.213]	login
Info	2026/08/12 13:18:51	User [admin] [192.168.1.213]	login

Event List Field Descriptions

After querying, matching events appear in the list on the right. Column descriptions:

Level Icon Event severity matching Info, Success, Warning, and Error in the query area.

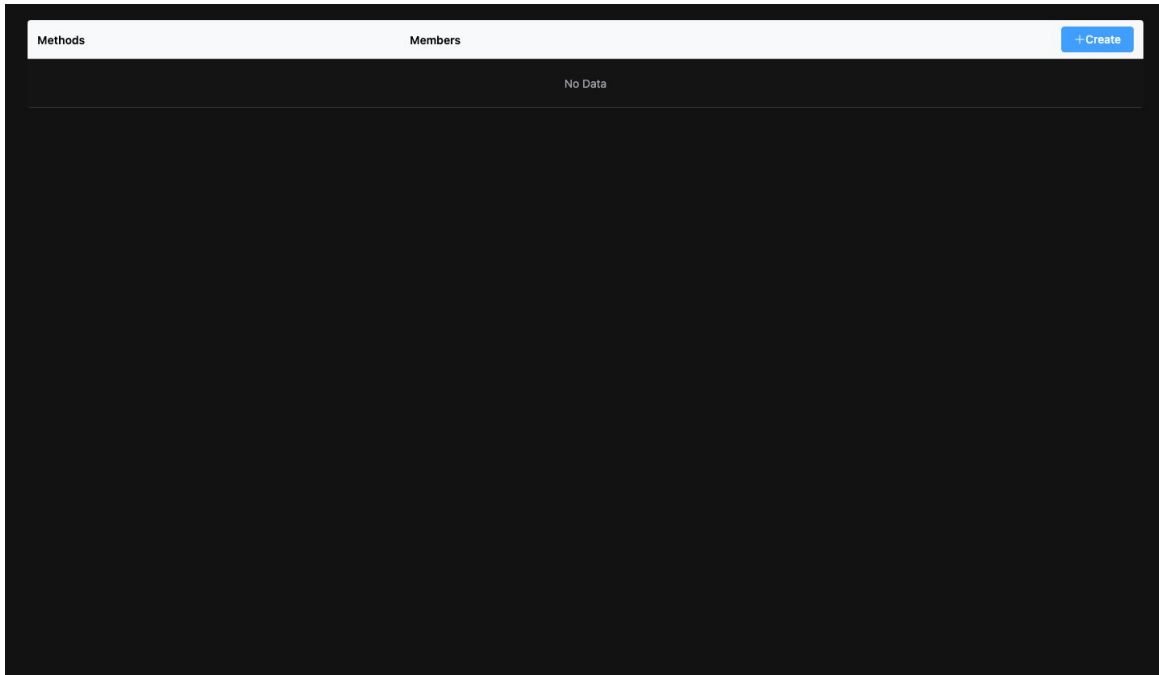
Time Event date and time (format per time format under System → System Parameters).

Account and Source IP Shows the user and source in `[account] [IP address]` format (e.g., `[admin] [192.168.1.213]`).

Description Brief event description (e.g., Login, alert text, or operation record).

5-2 Notification List

Navigation: Notifications > Notification List. This page lists notification methods and recipients.



Field Descriptions

Notify Method

Alert delivery channel (e.g., **All**, email) when conditions match.

Recipients

User accounts receiving notifications; each must have a valid email in user settings.

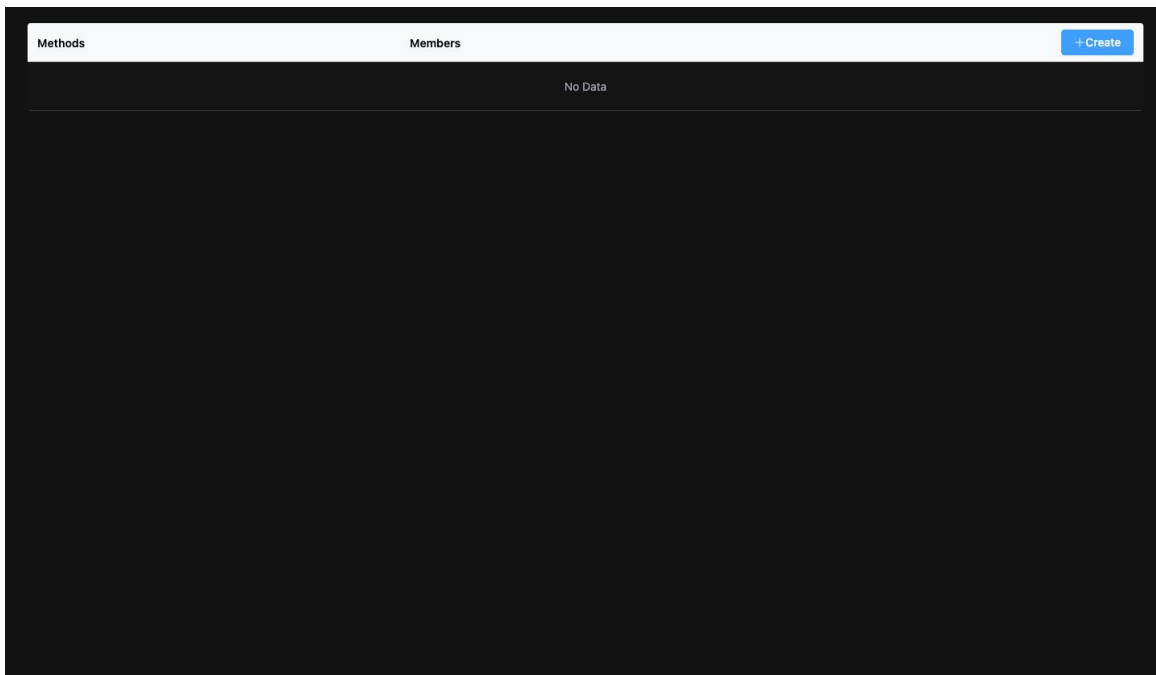
Button Descriptions

Add

Opens the form to add a notification rule.

5-2-1 Add Notification

Click **Add** to open the form below.



Field Descriptions

Device

Level

Select alert levels that trigger this notification rule (multiple selection).

 **Info**

 **Success**

 **Warning**

 **Error**

Type

Select peripheral or device type; ****All**** means no type filter.

Notification

Email

When enabled, sends alert notifications by email.

Pushover

When enabled, sends notifications via Pushover (configure under Engineering first).

Users

Select users to notify; each must have a valid email address.

Button Descriptions

Cancel

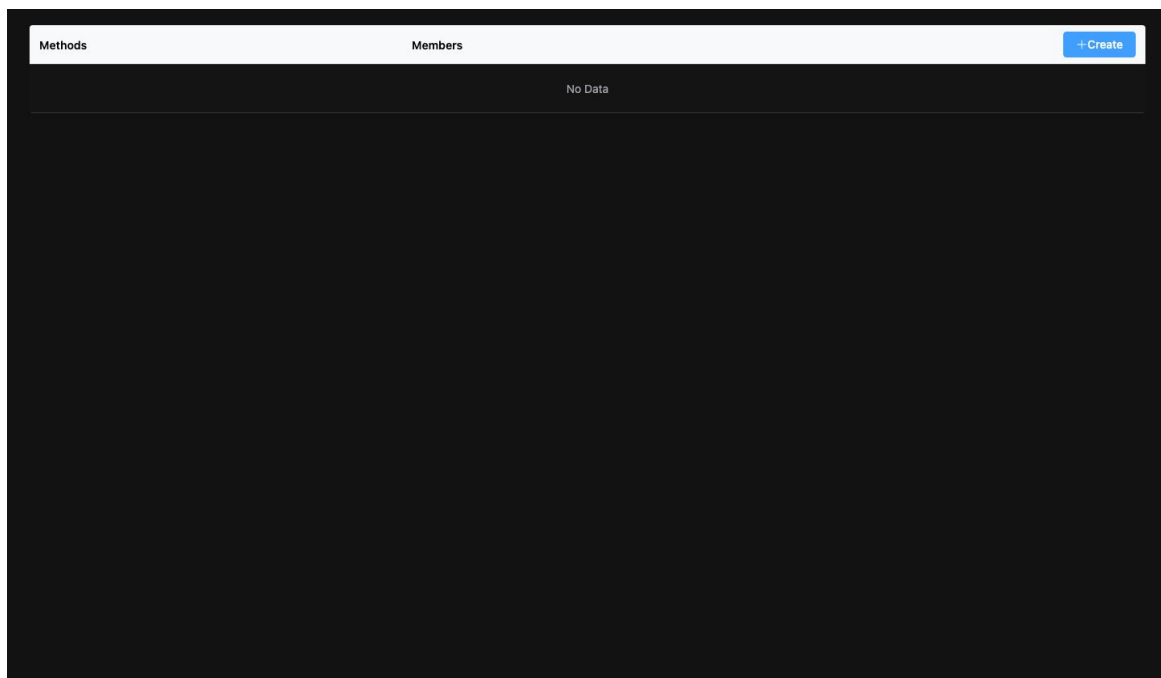
Discards changes and returns to the notification list.

Save

Saves the notification rule and returns to the list.

5-2-2 Edit Notification

Click an item in the list to open the edit screen.



Field Descriptions

Device	
Level	Select alert levels that trigger this notification rule (multiple selection).  Info  Success  Warning  Error
Type	Select peripheral or device type; **All** means no type filter.
Notification	
Email	When enabled, sends alert notifications by email.
Pushover	When enabled, sends notifications via Pushover (configure under Engineering first).
Users	

Select users to notify; each must have a valid email address.

Button Descriptions

Cancel

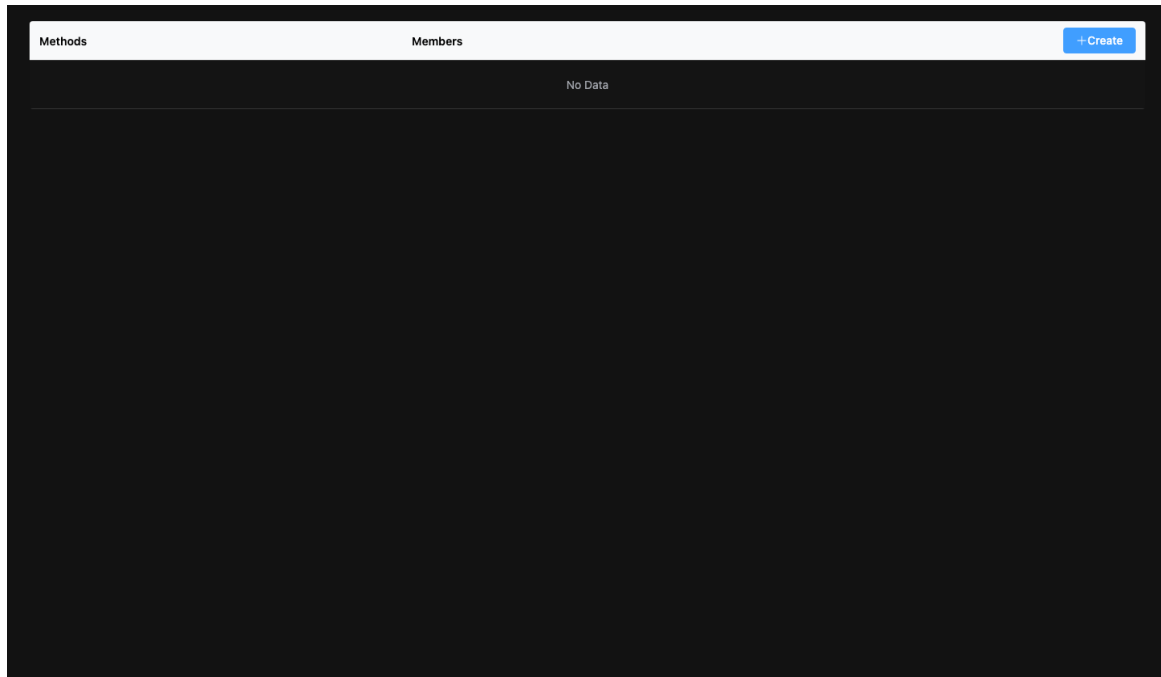
Discards changes and returns to the notification list.

Save

Saves the notification rule and returns to the list.

5-2-3 Delete Notification

Click **Delete** on the right of a list item to open a confirmation dialog.



Button Descriptions

Cancel

Cancels deletion and closes the dialog.

OK

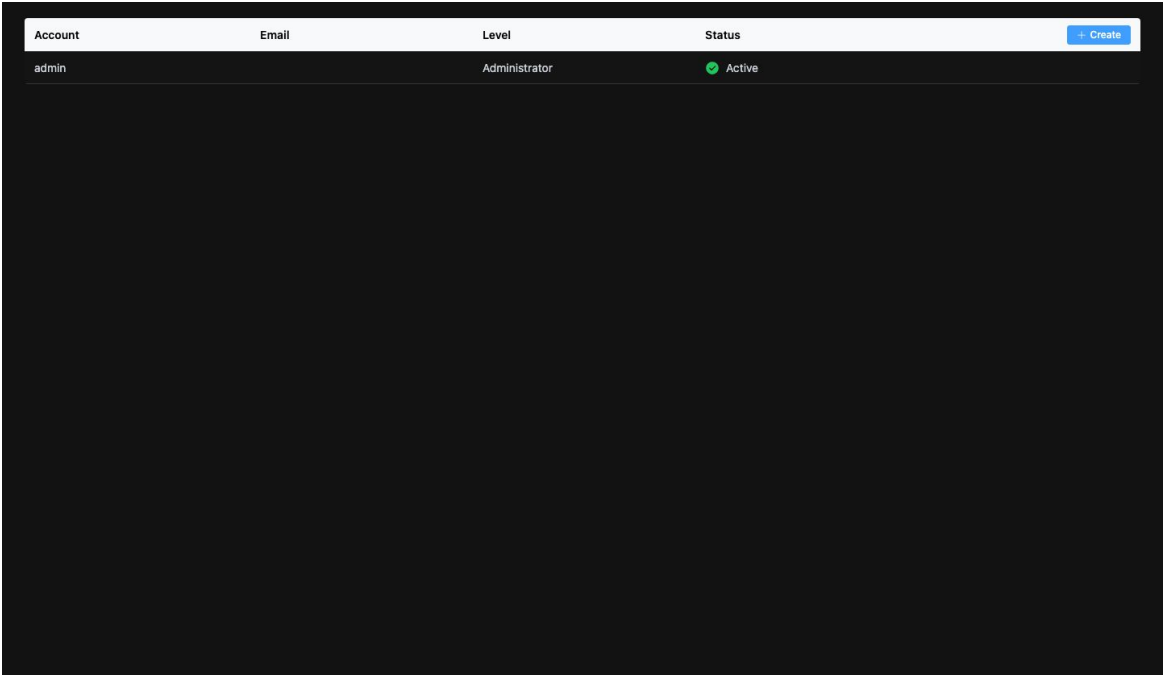
Confirms deletion of this notification rule.

Chapter 6 Accounts and Security

Manage user accounts, permissions, and security settings.

6-1 User Accounts

Navigation: **Permissions** > **Users** (submenu may show "Users"). This page lists all accounts with email, user level, and status.



Account	Email	Level	Status	
admin		Administrator	Active	

Field Descriptions

Account	Web UI login account name.
Email	User email for alerts and system messages.
Level	Permission level (e.g., System Administrator, Administrator, Viewer) determining accessible menus and actions.
Status	Account status (e.g., Normal, Locked); abnormal status may block login.

Button Descriptions

Add	Opens the form to create a user account.
-----	--

6-1-1 Add User

Click **Add** to open the form below.

Account	Email	Level	Status	
admin		Administrator	Active	+ Create

Field Descriptions

Level	User permission level (System Administrator, Administrator, Viewer); see permission level reference in this chapter.
Account	Web UI login account name.
Full Name	User display name (optional).
Password	Set or change login password.
Confirm Password	Re-enter password for confirmation.
Disabled	When enabled, the account cannot sign in.
Disable Notifications	When enabled, does not send notifications to this user.
Email	User email for alerts and notifications.
Pushover	Pushover user key or identifier (optional).

Button Descriptions

Cancel	Discards changes and returns to the user list.
Save	Saves the account and returns to the list.

6-1-2 Edit User

Click an item in the list to open the edit screen.

Account	Email	Level	Status	
admin		Administrator	Active	+ Create

Field Descriptions

Level	User permission level (System Administrator, Administrator, Viewer); see permission level reference in this chapter.
Account	Web UI login account name.
Full Name	User display name (optional).
Password	Set or change login password.
Confirm Password	Re-enter password for confirmation.
Disabled	When enabled, the account cannot sign in.
Disable Notifications	When enabled, does not send notifications to this user.
Email	User email for alerts and notifications.
Pushover	Pushover user key or identifier (optional).

Button Descriptions

Cancel

Discards changes and returns to the user list.

Save

Saves the account and returns to the list.

Delete

Click **Delete** on the right of a list item (system administrator account cannot be deleted) to open a confirmation dialog.

Account	Email	Level	Status	+ Create
admin		Administrator	Active	

Cancel

Discards changes and returns to the user list.

OK

Confirms deletion of this user account.

6-2 Password Policy

Navigation: Engineering > Password Policy (This section is numbered in chapter 8; the page is under the Engineering menu). This page sets login password rules for this device. Click [Save](#) when finished.

Password Policy

Min Length

-

6

+

Max Length

-

32

+

Require Uppercase

☐

Require Lowercase

☐

Require Numbers

☐

Require Special Chars

☐

Cancel

Save

Field Descriptions

Minimum Password Length	Minimum password length (factory default is often 6).
Maximum Password Length	Maximum password length (factory default is often 32).
Require Uppercase	When enabled, new passwords must include at least one uppercase letter.
Require Lowercase	When enabled, new passwords must include at least one lowercase letter.
Require Digit	When enabled, new passwords must include at least one digit.
Require Special Character	When enabled, new passwords must include at least one special character.

Button Descriptions

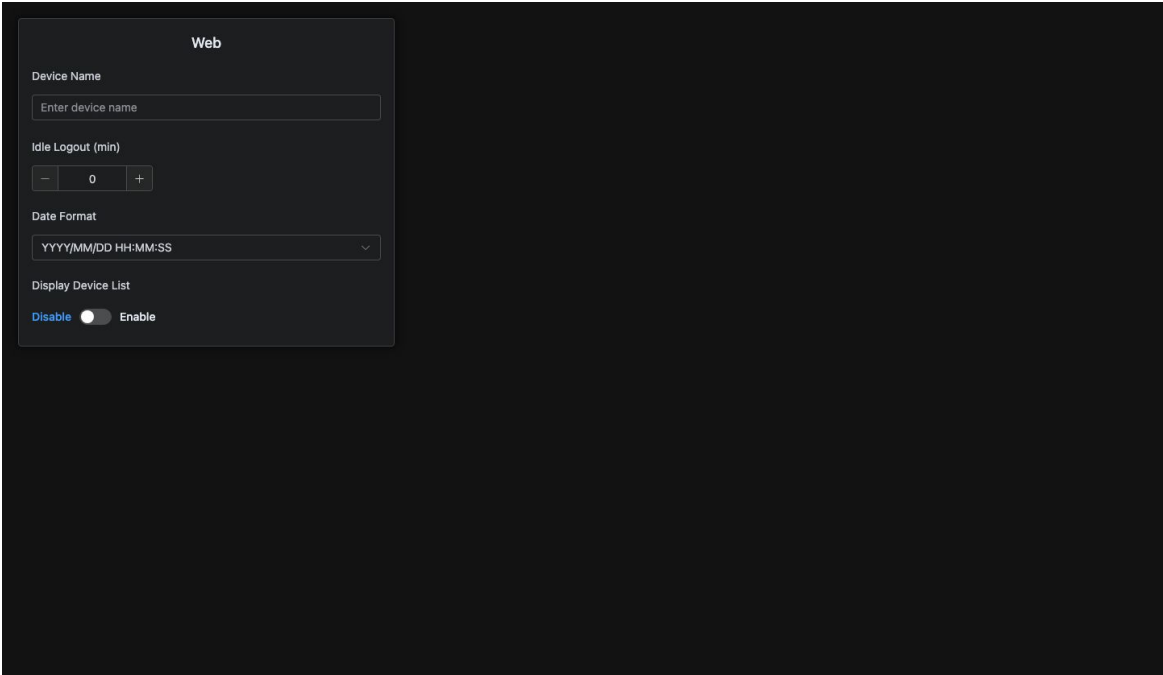
Cancel	Discards changes and restores password policy from when the page was opened.
Save	Saves password policy; future password changes must meet the new rules.

Chapter 7 System Settings

This chapter covers system settings such as network, network service, time sync, and firewall.

7-1 System Parameters

Navigation: System > System Parameters ("System Parameters" is a sub-page under System). This page configures Web UI behavior.

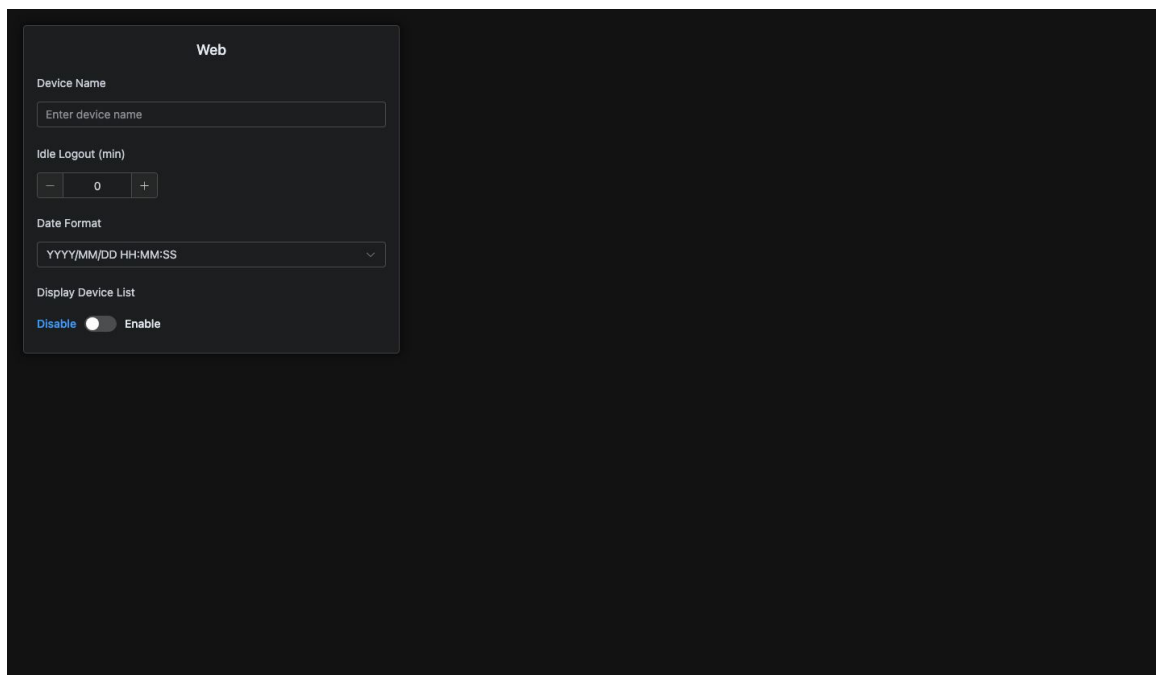


Field Descriptions

Device Name	Custom name in the Web UI and some reports to identify multiple devices.
Idle Logout (min)	Auto logout after idle minutes; 0 usually disables idle logout.
Time Format	Date/time format for events and UI (e.g., YYYY/MM/DD HH:MM:SS).
Show Device List	Default screen when entering the device URL in a browser. Yes (On) shows the device list first; No (Off) shows the login page directly.

Screen When Entering Device URL

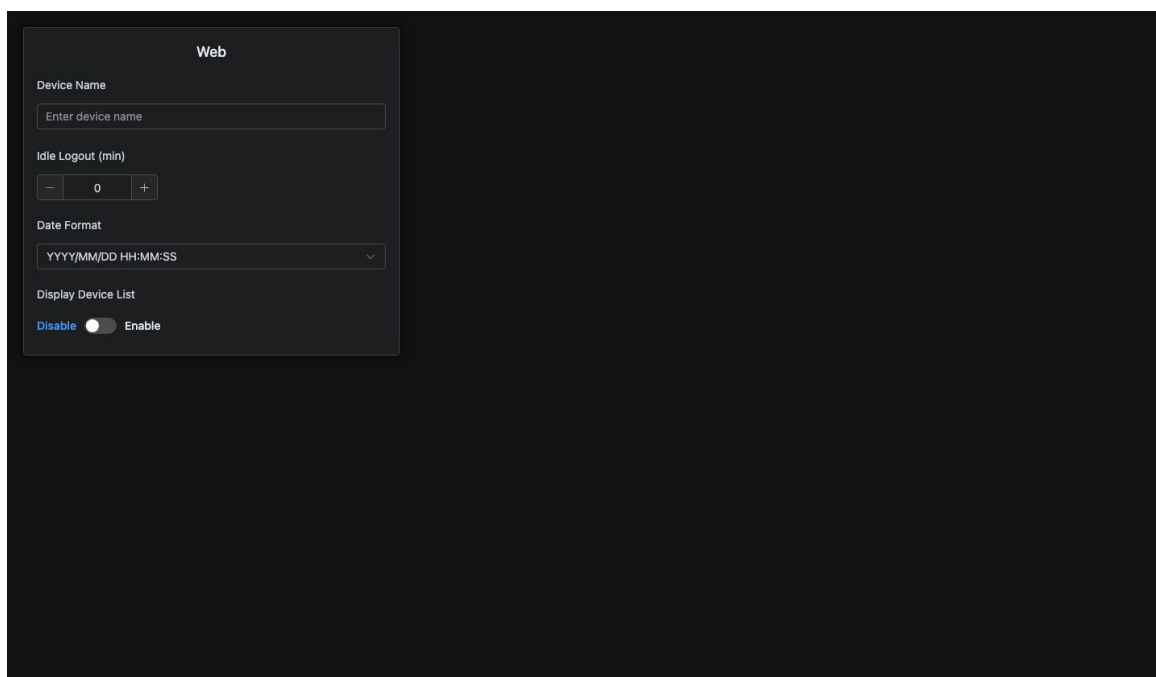
When **Show Device List** is **Yes**, entering the device IP shows the device list; click a device to open management.



Field Descriptions

Device Name	Custom name in the Web UI and some reports to identify multiple devices.
IP	Device network address.
Model	Product model.
Version	Firmware version.

When **Show Device List** is **No**, entering the device IP opens the login page directly.



7-2 Network

Navigation: System > Network. This page configures network settings.

The screenshot shows a dark-themed network configuration interface. On the left, the 'IPv4' section has a 'DHCP' toggle (currently off), a 'MAC' address field, and fields for 'IP Address', 'Netmask', 'Gateway', 'DNS 1', and 'DNS 2'. On the right, the 'IPv6' section has fields for 'IPv6 Address', 'Prefix Length' (set to 64), 'IPv6 Gateway', 'IPv6 DNS 1', and 'IPv6 DNS 2'. At the bottom right are 'Cancel' and 'Save' buttons.

Field Descriptions

IPv4	
DHCP	When enabled, IPv4 is assigned by DHCP; disable to enter IP, mask, and gateway manually.
MAC	Shows this device's MAC address (read-only) for network management.
IP Address	Sets the device IPv4 address; reconnect to the Web UI with the new IP after changing it.
Subnet Mask	Sets the IPv4 subnet mask defining the LAN range.
Default Gateway	Sets the default gateway for outbound traffic.
DNS Server 1	Primary DNS server for name resolution.
DNS Server 2	Secondary DNS server as backup; may be blank.
IPv6	
IPv6 Address	Sets the device IPv6 address.
Prefix Length	Sets the IPv6 prefix length (commonly 64).
IPv6 Gateway	Sets the IPv6 default gateway.

IPv6 DNS Server 1	Primary IPv6 DNS server.
IPv6 DNS Server 2	Secondary IPv6 DNS server; may be blank.

Button Descriptions

Cancel	Discards changes and restores values from when the page was opened.
Save	Saves and applies network settings; reconnect with the new address if the IP changed.

7-3 Network Service

Navigation: System > Network Service. Open **System > Network Service** from the top menu to configure ICMP, SSH, Let's Encrypt, HTTPS manual certificates, and DDNS. Set DNS server addresses on the **Network** page (DNS Server 1 and DNS Server 2).

The screenshot displays the 'Network Service' configuration interface. It is divided into four main sections:

- Network Service:** Contains two toggle switches. 'Disable ICMP Echo' is currently turned off. 'Enable SSH' is also turned off.
- Let's Encrypt (UACME):** Features a toggle for 'Enable automatic certificate' which is turned on. Below this are input fields for 'Domain' (containing 'rpd406.sotokara.com') and 'Contact email' (containing 'juilwen@bellwin.com.tw'). 'Save' and 'Test' buttons are at the bottom right.
- HTTPS Manual Certificate:** Shows certificate details including Status ('In use (https-server)'), Subject ('CN = rpd406.sotokara.com'), Issuer ('C = US, O = Let's Encrypt, CN = YR1'), and Validity ('2026-08-14T05:14:00Z ~ 2026-11-12T05:13:59Z'). It includes an 'Upload certificate' section with a 'Select files' button and an 'Upload and apply' button at the bottom right. A note states: 'Select certificate.crt (optionally ca_bundle.crt). Do not upload private.key.'
- DDNS:** Contains a toggle for 'Enable DDNS' which is turned on. It includes a 'Provider' dropdown menu set to 'stealthone (sotokara.com)', a 'Domain name (subdomain)' field with 'rpd406', and a 'Check interval (minutes)' field set to '10'. 'Save' and 'Update now' buttons are at the bottom right.

Field Descriptions

Network Service	
Disable ICMP Echo	When enabled, the device does not respond to ping (ICMP), reducing scan exposure without affecting Web or SNMP.
Enable SSH	Enables SSH remote shell access; use only on trusted networks with strong passwords.

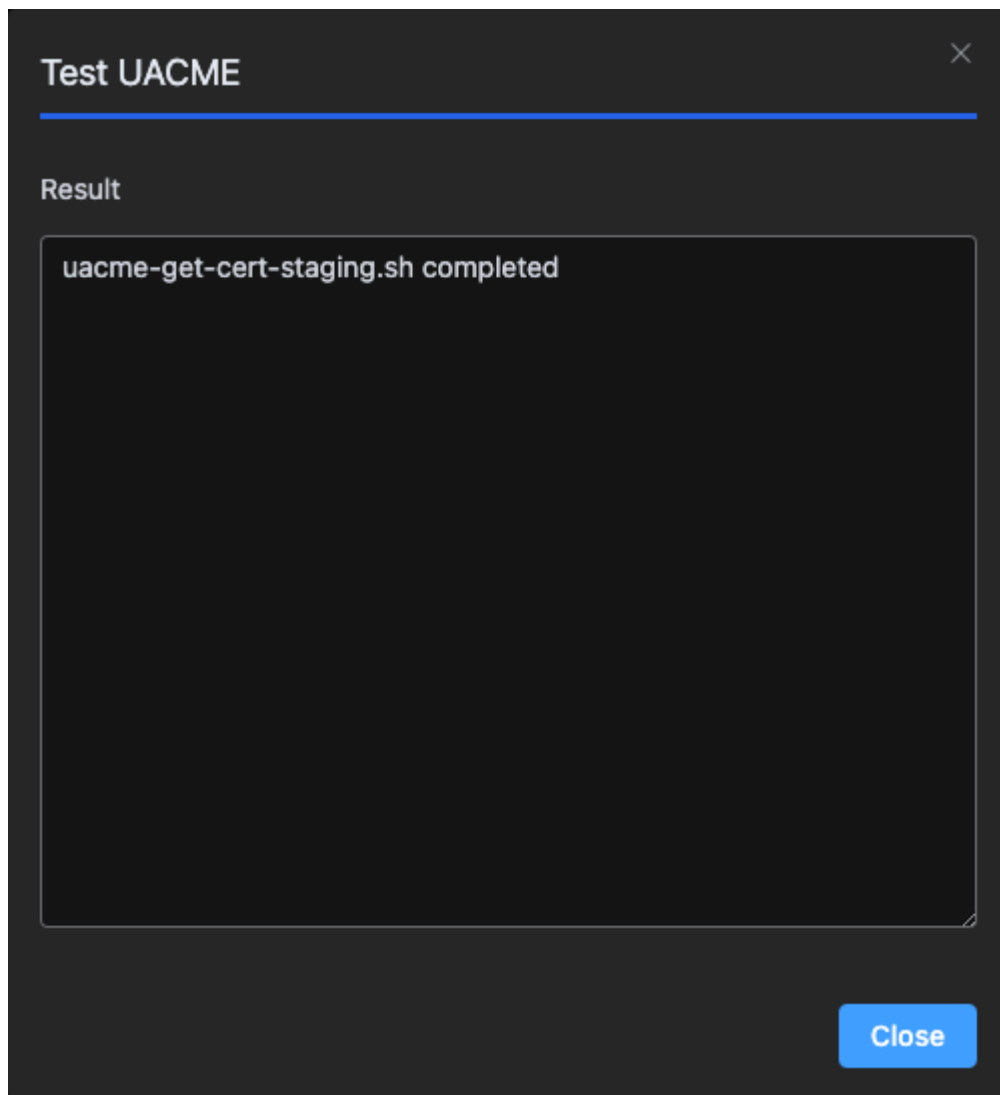
Let's Encrypt (UACME)

Enable automatic certificate	Enables automatic Let's Encrypt HTTPS certificate request and renewal; requires a resolvable domain and contact email.
Domain	Domain name for Let's Encrypt validation; must resolve to this device's public IP.
Contact email	Email address for Let's Encrypt registration and expiry notices.
Save	Saves and applies Let's Encrypt settings.
Test	Tests whether Let's Encrypt certificate prerequisites are met.

Before You Begin

Before requesting a Let's Encrypt certificate, confirm:

- **Domain** resolves to an IP address reachable from the Internet
- **DNS servers** are configured correctly (set DNS Server 1 and DNS Server 2 under System → Network)
- The device can reach the Internet for ACME validation
- **Firewall** (see 7-6 Firewall) does not block Let's Encrypt validation
- Click **Test** to verify prerequisites before enabling **Enable automatic certificate**



HTTPS Manual Certificate

Shows the current HTTPS certificate and lets you upload your own certificate files. This card appears on the same page as Let's Encrypt automatic certificates. After applying a manual certificate, confirm the browser is using the updated certificate.

Status	Current HTTPS certificate status (for example, in use and the related service name).
Subject	Subject of the current certificate, typically including CN (Common Name).
Issuer	Issuer of the current certificate.
Validity	Validity period of the current certificate.
Upload certificate	Select certificate.crt (optionally add ca_bundle.crt). Do not upload private.key.
Select files	Selects the certificate files to upload.
Upload and apply	Uploads the selected certificate files and applies them to HTTPS.

Advanced settings: Opens advanced certificate options. To use an internal CA or your own certificate, upload certificate.crt (optionally add ca_bundle.crt) under **HTTPS Manual Certificate**. Do not upload private.key.

DDNS

Enable DDNS

When enabled, the device updates the dynamic DNS record so the domain points to the current public IP.

Provider

This screen uses **stealthone (sotokara.com)**.

Domain name (subdomain)

The subdomain registered with the provider (for example `rpd406`); combined with `sotokara.com` it forms the full hostname.

Check interval (minutes)

How often, in minutes, the device checks and updates the DDNS record.

Save

Saves DDNS settings.

Update now

Immediately updates the current public IP with the provider.

7-4 Time Sync

Navigation: System > Time Sync. This page configures device time, time zone, and NTP servers.

Device Time

Time

2026/08/12 14:19

Timezone

(UTC+08:00) Asia/Taipei

Time Sync

Enable Time Sync

☒

Custom Time Server

☐

Server URL

pool.ntp.org

Test

Manual Sync

Date

2026-08-12

Time

14:19:19

Read

Sync

Field Descriptions

Device Time

Time

Current device system time (read-only) to verify NTP or manual sync.

Time Zone	Device time zone; set correctly so event timestamps match local time.
Time Sync	
Enable Time Sync Service	When enabled, syncs time with NTP periodically; mutually exclusive with manual sync.
Use Custom Time Server	When enabled, syncs using the server in Server URL .
Server URL	Custom NTP server hostname or IP (default is often pool.ntp.org).

Test Tests connectivity to the configured NTP server.

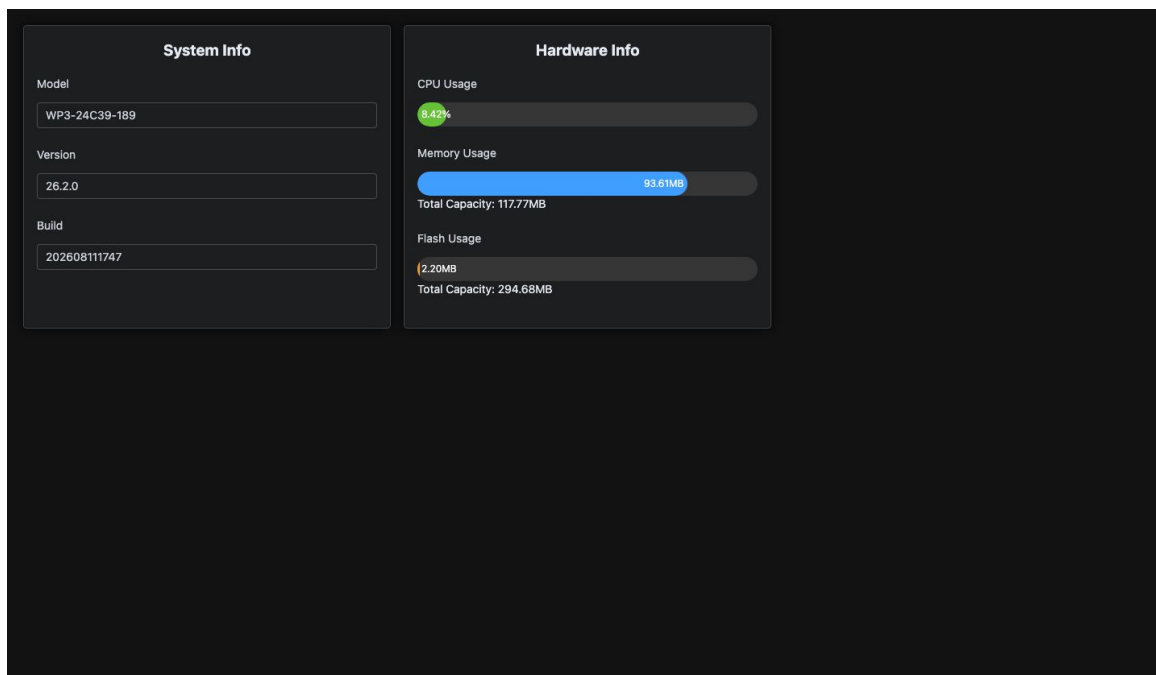
The screenshot displays a configuration interface for time synchronization, divided into three main panels: Device Time, Time Sync, and Manual Sync.

- Device Time:** Contains a 'Time' field with the value '2026/08/12 14:19' and a 'Timezone' dropdown menu currently set to '(UTC+08:00) Asia/Taipei'.
- Time Sync:** Features a toggle for 'Enable Time Sync' which is turned on. Below it is a 'Custom Time Server' toggle which is turned off. The 'Server URL' field contains 'pool.ntp.org', and a 'Test' button is located to its right.
- Manual Sync:** Includes a 'Date' field with '2026-08-12' and a 'Time' field with '14:19:19'. At the bottom right of this panel are two buttons: 'Read' (green) and 'Sync' (blue).

Manual Sync	
Date	Date for manual sync; disable Enable Time Sync Service first.
Time (Manual Sync)	Time for manual sync; use Read to copy the computer's current time.
Read	Fills Manual Sync fields with the computer's current date and time.
Sync	Writes manually set date and time to the device; disable automatic time sync first.

7-5 Information

Navigation: System > Information. This page displays device information.



Field Descriptions

System Information

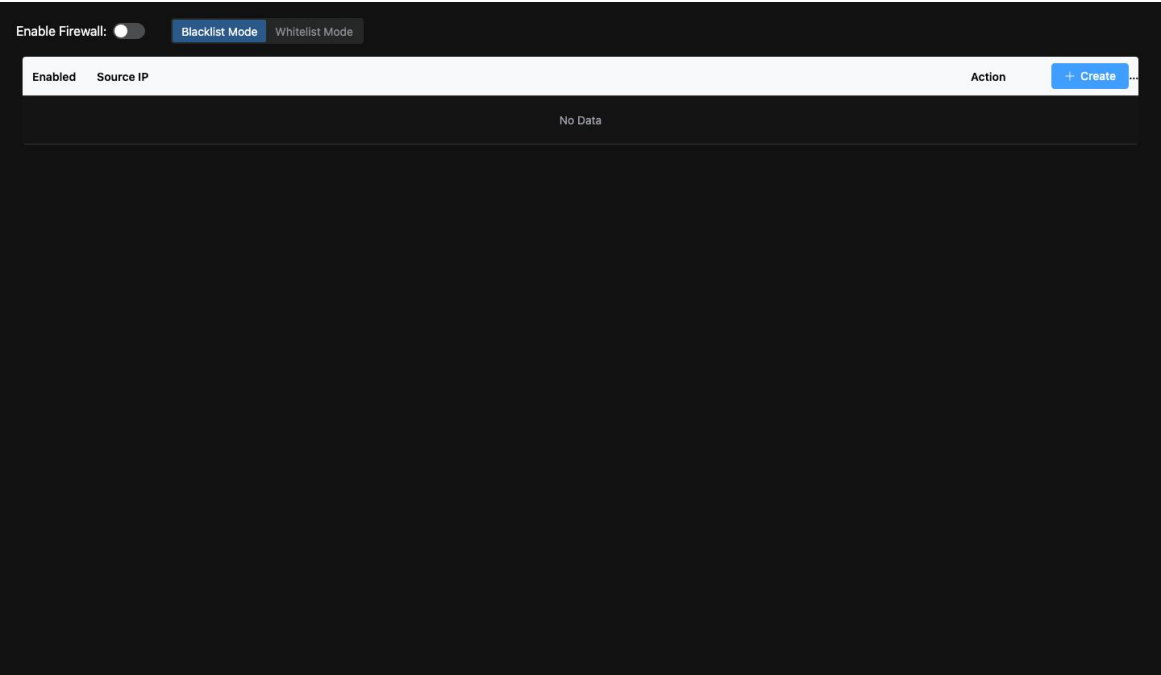
Product Model	Product model (read-only) for support and maintenance.
Firmware Version	Firmware version (read-only) for comparison before and after upgrade.
Build Number	Shows the firmware build number (read-only) for detailed version comparison.

Hardware Information

CPU Usage	CPU usage percentage (read-only); high values may slow response.
Memory Usage	Memory used and total capacity (read-only).
FLASH Usage	FLASH used and total capacity (read-only); run maintenance cleanup when space is low.

7-6 Firewall

Navigation: System > Firewall. This page enables the firewall and restricts which IP addresses may connect using blacklist or whitelist mode.



Field Descriptions

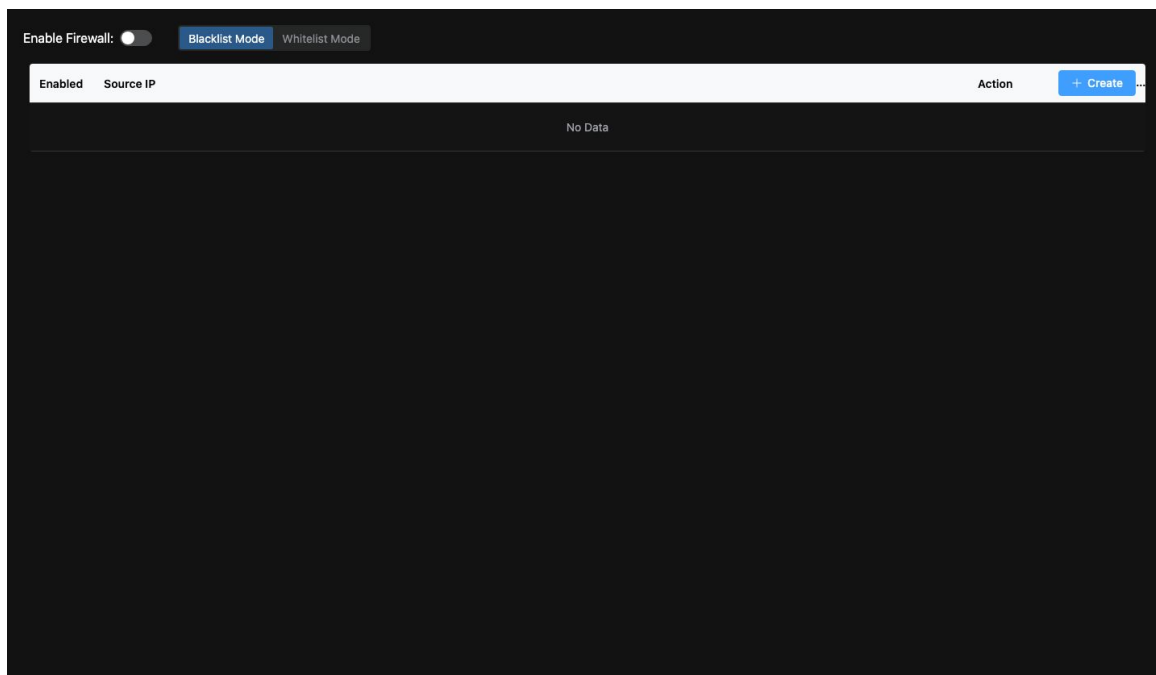
Enable Firewall	Enables or disables the firewall.
Blacklist Mode	Listed IPs are blocked; others are allowed.
Whitelist Mode	Only listed IPs may connect; all others are denied.
Enabled	Whether each rule is active.
IP	Source IP to allow or deny (may include a subnet).
Action	Allow or deny behavior for this rule.

Button Descriptions

Add	Adds a firewall rule.
-----	-----------------------

7-6-1 Add Firewall Rule

Click **Add** to open the form below.



Field Descriptions

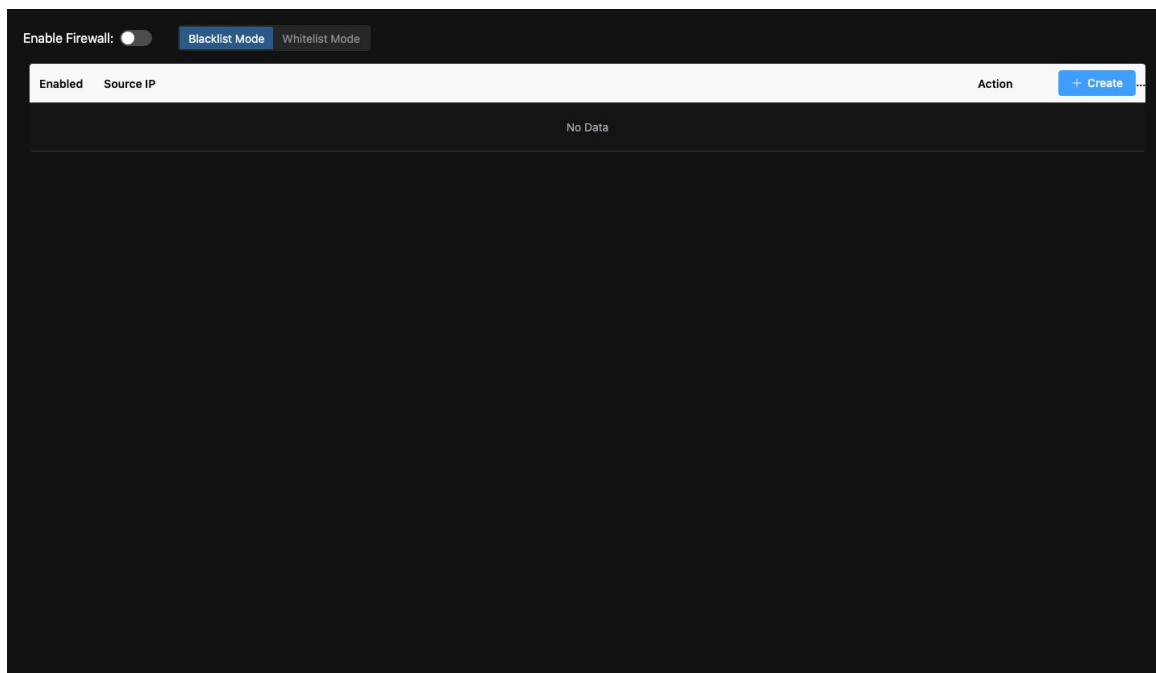
Enabled	Whether this rule is active.
Source IP	How to specify the source address; choose from the dropdown. • Single: A single IP address; enter IP when selected. • Range: An IP address range; enter Start IP and End IP.
IP	Single source IP; shown only for Single.
Start IP	Range start address; shown only for Range.
End IP	Range end address; shown only for Range.
Action	Choose Allow or Deny .

Button Descriptions

Cancel	Discards changes and returns to the list.
Save	Saves the rule and returns to the list.

7-6-2 Edit Firewall Rule

Click an item in the list to open the edit screen.



Field Descriptions

Enabled Whether this rule is active.

Source IP How to specify the source address; choose from the dropdown.

- **Single:** A single IP address; enter **IP** when selected.
- **Range:** An IP address range; enter **Start IP** and **End IP**.

IP Single source IP; shown only for Single.

Start IP Range start address; shown only for Range.

End IP Range end address; shown only for Range.

Action Choose **Allow** or **Deny**.

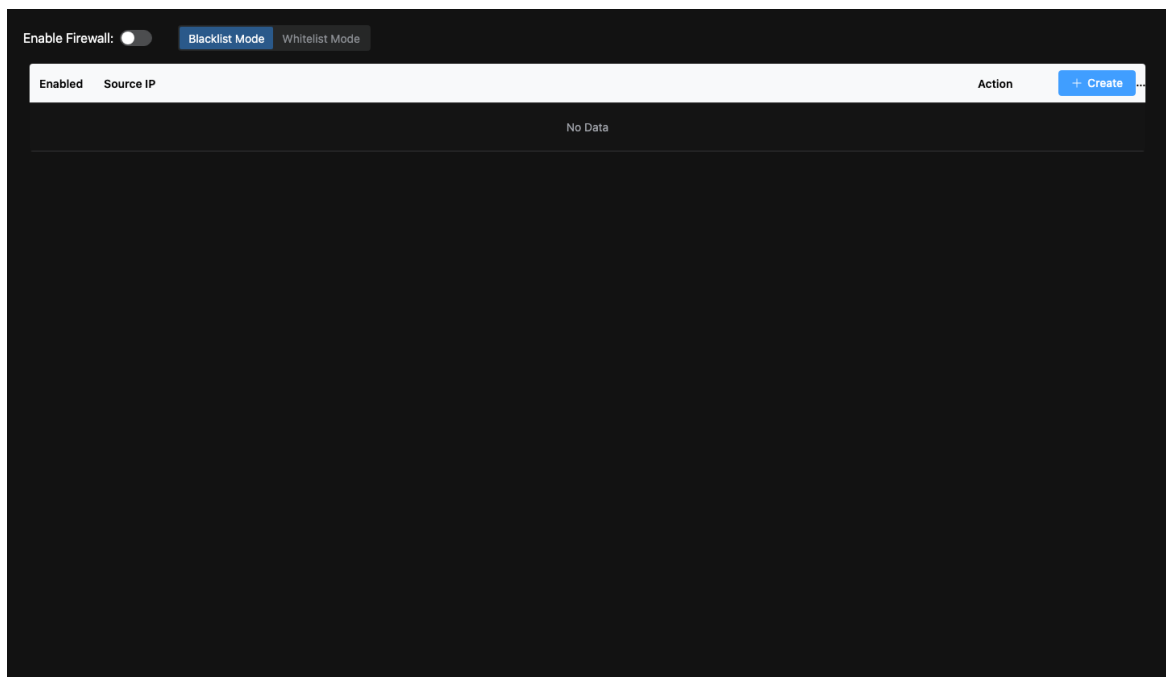
Button Descriptions

Cancel Discards changes and returns to the list.

Save Saves changes and returns to the list.

Delete

Click **Delete** on the right of a list item to open a confirmation dialog.



Cancel

Closes the dialog without deleting.

OK

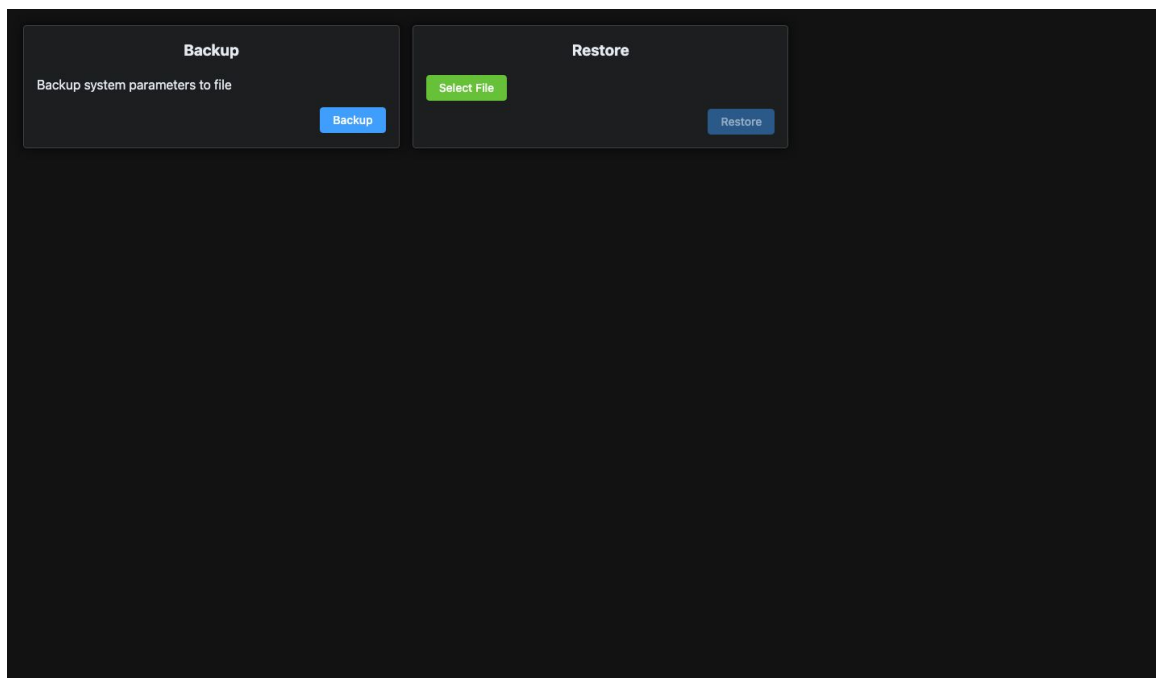
Confirms deletion of this firewall rule.

Chapter 8 Maintenance, Backup & Restore

This chapter covers backup, restore, maintenance, and firmware update operations.

8-1 Backup and Restore

Navigation: **System > Backup & Restore** (or backup under Maintenance, depending on firmware version). This page backs up and restores device parameters.



Parameter Backup

Back up system parameters and download the file to your computer.

Backup

Exports current device parameters to a file and downloads it.

Parameter Restore

Select File

Selects a previously backed-up parameter file to restore.

Restore

Uploads a parameter file and overwrites device settings; back up current settings first.

Backup Contents

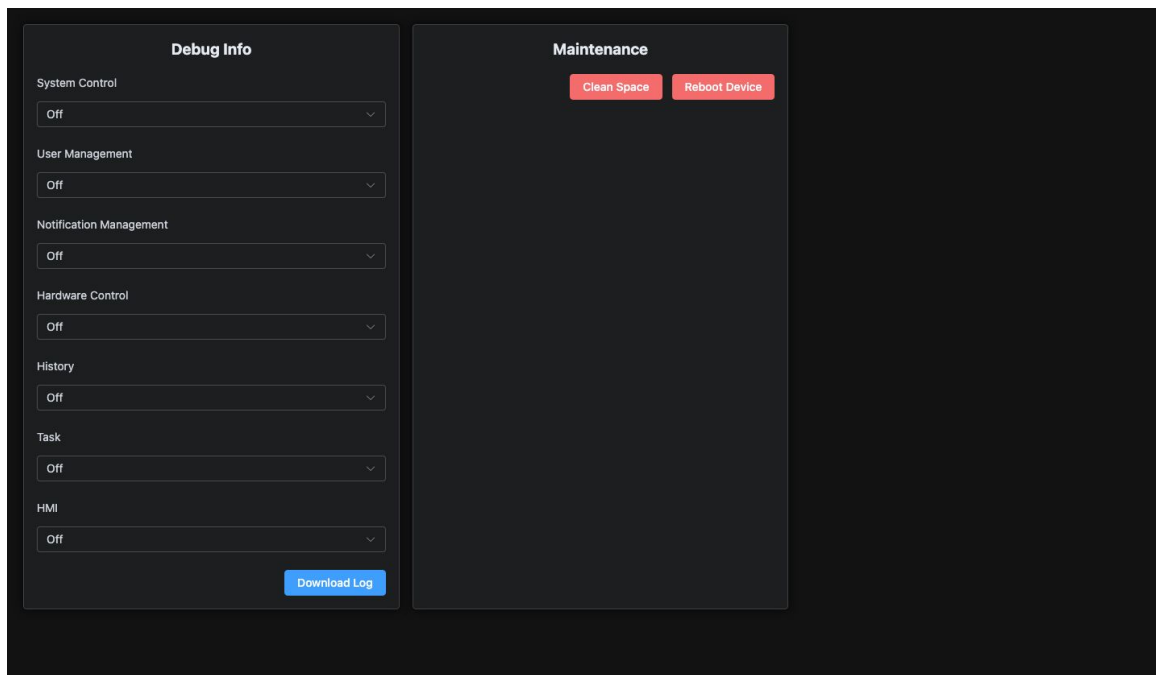
Backup files mainly contain **configuration settings** (alert thresholds, schedules, notification rules, SNMP, network services, engineering parameters, etc.). The following are usually **not included** and must be reconfigured or verified after restore:

- Historical events and statistics
- User account passwords (verify Users and login credentials after restore)
- Firmware version (restore does not upgrade or downgrade firmware)

- Network IP address (if the backup includes network settings, the IP may change after restore —reconnect using the new address)

8-2 System Maintenance

Navigation: System > Maintenance. This page sets debug levels, downloads debug logs, and provides system maintenance. Debug levels are for technical troubleshooting; normal operation needs no changes—the factory default is **Off** for all modules.



Field Descriptions

Debug Information

Each module can be configured **independently**. When a level is selected, the system logs **that level and more severe levels** (from most to least severe: Critical → Error → Alert → Info → Debug → Trace; see Debug Level Reference below).

System Control	Log threshold for system core and services (startup, config apply, internal state).
User Manager	Log threshold for login, accounts, and permissions.
Notification Manager	Log threshold for alerts, email, and Pushover delivery.
Hardware Control	Log threshold for sensors, outlet control, and hardware communication.
History	Log threshold for event and history data writes.
Tasks	Log threshold for background and periodic tasks.

Debug Level Reference

Off	Does not log debug messages for this module; recommended for normal operation .
Critical	Logs only severe events that may cause service interruption or data anomalies.
Error	Logs error and critical messages (e.g., operation failures, communication errors).
Alert	Logs alert, error, and critical messages (e.g., recoverable anomalies or unexpected states).
Info	Logs routine operational messages and more severe levels (e.g., main process execution records).
Debug	Logs debug details and more severe levels; commonly used for troubleshooting, but log volume increases significantly.
Trace	Logs the most detailed trace messages; enable briefly only when directed by technical support, then set back to Off .

Usage Recommendations

1. **Troubleshooting workflow:** As directed by support, raise only **relevant modules** (e.g., **System Control** for network issues, **Hardware Control** for sensor issues), reproduce the issue, click [Download Debug Log](#), send the file to support, then set levels back to **Off**.
2. **Performance and storage:** **Debug** or **Trace** increases log frequency and FLASH usage and may slightly affect response time. If FLASH usage on the **Information** page is high, click [Free Space](#).
3. **Difference from Event History:** **History** is for operators to query actions and alerts; debug logs on this page are for internal diagnostics and are technical—most users do not need them.

Download Debug Log

Downloads packaged debug logs from all modules (usually a compressed file) for support analysis; download immediately after reproducing the issue.

System Maintenance

Free Space

Clears accumulated debug logs to free FLASH space; does not affect alerts, accounts, or general configuration.

Reboot Device

Reboots the device; active connections will drop briefly.

8-3 Firmware Update

Navigation: Engineering > Firmware Update(Same page as Engineering → Firmware Update; this section provides the full procedure.) This page provides firmware update and factory reset.

The screenshot shows a dark-themed user interface with two main panels. The left panel, titled 'Firmware Update', contains three input fields: 'Model' with the value 'WP3-24C39-189', 'Version' with '26.2.0', and 'Build' with '202608111747'. Below these fields are two buttons: a green 'Select File' button and a blue 'Update' button. The right panel, titled 'Factory Reset', contains a text description 'Reset device to factory settings. All parameters will be cleared' and a prominent red 'Factory Reset' button.

Firmware Update

Product Model	Shows the product model (read-only). Verify the firmware file matches this model before upgrading.
Firmware Version	Shows the current firmware version (read-only). Updates after a successful upgrade.
Build Number	Shows the firmware build number (read-only) for detailed version comparison.

Procedure

Firmware update procedure:

1. Click **Select File**.
2. Browse to the firmware file and select it.

The screenshot shows a dark-themed web interface with two main panels. The left panel, titled 'Firmware Update', contains three input fields: 'Model' with the value 'WP3-24C39-189', 'Version' with '26.2.0', and 'Build' with '202608111747'. Below these fields is a green 'Select File' button and a blue 'Update' button at the bottom right. The right panel, titled 'Factory Reset', contains the text 'Reset device to factory settings. All parameters will be cleared' and a red 'Factory Reset' button.

3. The selected file name appears below the Select File button.

This screenshot is identical to the one above, showing the 'Firmware Update' and 'Factory Reset' panels. The 'Firmware Update' panel has the 'Model' field set to 'WP3-24C39-189', 'Version' to '26.2.0', and 'Build' to '202608111747'. It features a green 'Select File' button and a blue 'Update' button. The 'Factory Reset' panel displays the text 'Reset device to factory settings. All parameters will be cleared' and a red 'Factory Reset' button.

4. Click **Update** to upload, verify, and apply the firmware.

Warning: This device updates offline. The Web UI may be unavailable for about 3–7 minutes. Do not power off or disconnect the network during the upgrade.

The screenshot shows a dark-themed web interface with two main panels. The left panel, titled 'Firmware Update', contains three input fields: 'Model' with the value 'WP3-24C39-189', 'Version' with '26.2.0', and 'Build' with '202608111747'. Below these fields are two buttons: a green 'Select File' button and a blue 'Update' button. The right panel, titled 'Factory Reset', contains a text description 'Reset device to factory settings. All parameters will be cleared' and a prominent red 'Factory Reset' button.

This is a duplicate of the screenshot above, showing the same 'Firmware Update' and 'Factory Reset' interface with the same data and layout.

Select File

Select a firmware file from the local computer (extension per product specification).

Update

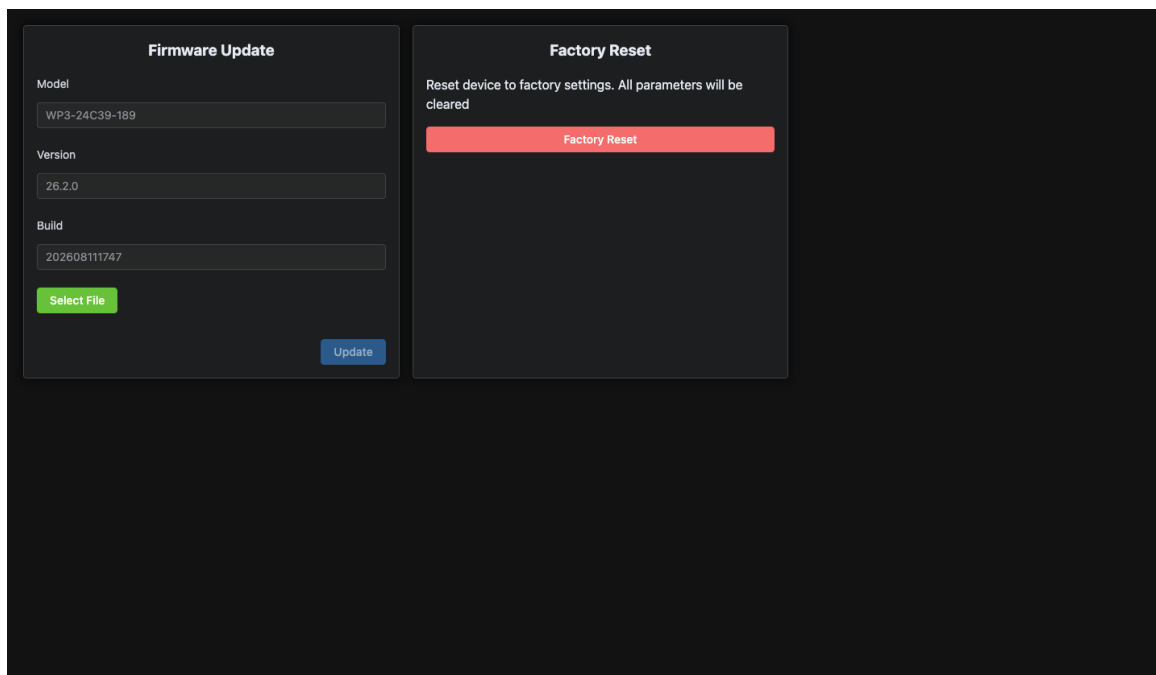
Upload and apply firmware; do not power off or disconnect the network during the process.

Factory Reset

Restore all device parameters to factory defaults. All configuration will be erased.

Procedure

1. Click **Factory Reset**.
2. Confirm the dialog with **OK**; the device reboots and clears all settings.



3. After reboot, sign in with factory default **admin / admin** (see 3-3 Login).
4. The system requires a password change; set a new password per policy and click **OK**.

Factory Reset	Restore factory defaults; this cannot be undone—back up configuration first.
OK	Confirms factory reset and device reboot.
Cancel	Close the dialog without resetting.

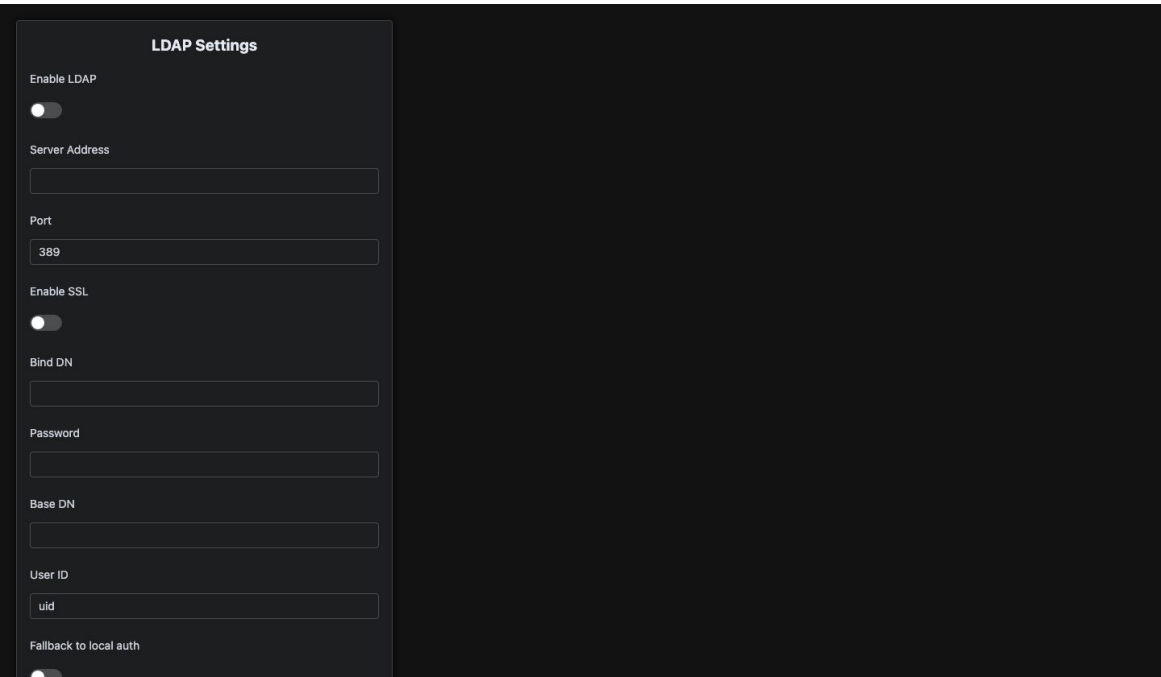
Chapter 9 Engineering Mode

Advanced settings for administrators. Open from the top menu **Engineering**. This chapter includes:

- **LDAP:** Directory-service login authentication
- **RADIUS / TACACS+:** External authentication servers
- **SNMP Agent:** SNMP monitoring and management
- **Mail Server:** SMTP and test mail
- **Alert Service:** External notifications such as Pushover
- **Syslog:** Syslog server and forwarding

9-1 LDAP

Navigation: Engineering > LDAP. This page configures and tests LDAP.



Field Descriptions

Enable LDAP	When enabled, login validates against LDAP; when disabled, local accounts only.
Server Address	LDAP server hostname or IP.
Port	LDAP port (commonly 389; 636 with SSL).
Enable SSL	When enabled, uses LDAPS encryption for credential transport.
Bind DN	Bind DN for LDAP connection and queries.

Password	Password for the Bind DN. When already set, the field shows eight asterisks (`*****`); submitting those eight asterisks on save means the existing password is not changed.
Base DN	Base DN for user search.
User ID Attribute	LDAP attribute matching login names (commonly uid or sAMAccountName).

Fall Back to Local Password When LDAP Unavailable: When enabled, uses local credentials if LDAP is unreachable, avoiding login lockout.

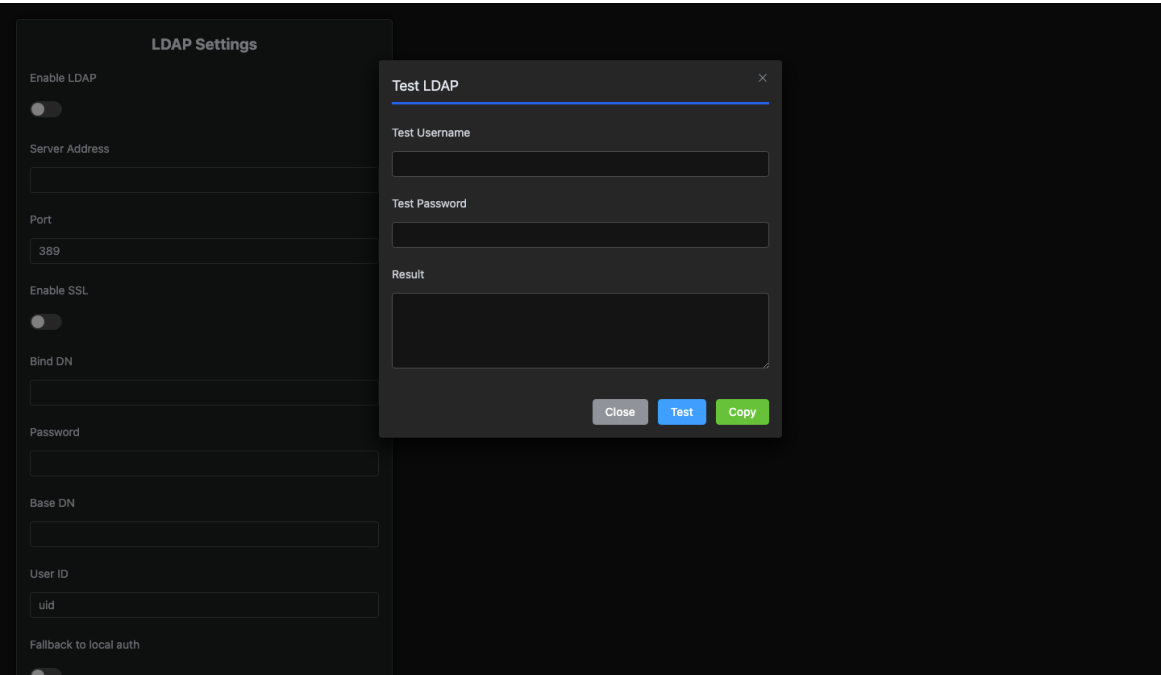
Permissions and Account Mapping

LDAP only validates credentials. After authentication, access is determined by the **Level** (System Administrator, Administrator, Viewer) of the **matching account name** in **Permissions > Users**. Create a local account matching the LDAP login name and assign a level first; without it, expected permissions may not apply.

9-1-1 LDAP Test

Procedure

Press **Test** to open the test window; fill in the account and password and press **Test**. The LDAP test results will be displayed in the result area.



Field Descriptions

Test Username	Enter the LDAP account to be verified to test whether the binding and search are successful.
---------------	--

Test Password	Enter the password for this LDAP account.
Result	Displays LDAP connection and authentication result messages for debugging settings.

Button Descriptions

Close	Close the LDAP test dialog box.
Test	Performs an LDAP authentication test using the entered password.
Copy	Copy the test result text to the clipboard.

9-2 RADIUS / TACACS+

Navigation: Engineering > RADIUS / TACACS+. This screen configures a RADIUS or TACACS+ server so that Web UI logins are authenticated by an external service.

Field Descriptions

Enable RADIUS / Enable TACACS+	When enabled, login authenticates against the corresponding server; when disabled, only local accounts are used.
Server Address	IP or FQDN of the authentication server.
Port	Authentication service port (commonly 1812 for RADIUS and 49 for TACACS+).
Key	The shared key agreed with the authentication server. When already set, the field shows eight asterisks (`****`); submitting those eight asterisks on save means the existing key is not changed.

Timeout

Seconds to wait for a server response.

Maximum retries

Number of retries when the connection fails.

Fall back to local password when unable to connect: When the server cannot be reached, whether local accounts may be used to log in.

Permissions and Account Mapping

RADIUS / TACACS+ authenticates accounts against an external server. After authentication, access is determined by the **Level** of the **matching account name** in **Permissions > Users**. Create a local account with the same remote login name and assign a level first. To map permissions from server groups, configure the correspondence between RADIUS/TACACS+ groups and local account levels.

Button Descriptions

Cancel

Discards this change.

Save

Saves RADIUS / TACACS+ settings.

Test

Tests connectivity with the authentication server.

9-2-1 RADIUS / TACACS+ Test

Procedure

Click **Test** on the RADIUS or TACACS+ card to open the test window (titled "Test RADIUS" or "Test TACACS+"). Enter the account and password, then click **Test**. Results appear in the result area.

The screenshot displays two side-by-side configuration panels for RADIUS and TACACS+ settings. The RADIUS Settings panel on the left includes fields for 'Enable RADIUS' (disabled), 'Server Address', 'Port' (1812), 'Secret', 'Timeout' (5), 'Max Retries' (3), and 'Fallback to local auth' (disabled). The TACACS+ Settings panel on the right includes fields for 'Enable TACACS+' (disabled), 'Server Address', 'Port' (49), 'Secret', 'Timeout' (5), and 'Fallback to local auth when TACACS+ unavailable' (enabled). Both panels have 'Cancel', 'Save', and 'Test' buttons at the bottom.

Field Descriptions

Test Username	Account used to test authentication against the RADIUS / TACACS+ server.
Test Password	Password for that account.
Result	Connection and authentication result messages for debugging.

Button Descriptions

Close	Closes the test window.
Test	Runs the authentication test with the entered credentials.
Copy	Copies the result text to the clipboard.

9-3 SNMP Agent

Navigation: Engineering > SNMP Agent.

The screenshot shows the 'SNMP Agent' configuration interface. It is organized into three vertical panels. The first panel, 'SNMP Agent', contains fields for 'Device Name' (WP3-24C39-189), 'Contact' (admin), and 'Location' (office), with a 'Download MIB' button. The second panel, 'SNMP v1/v2c', features toggle switches for 'Enable v1/v2c' and 'SNMP Write', and text boxes for 'Read Access' (public) and 'Write Access' (private). The third panel, 'SNMP v3', includes a toggle for 'Enable v3', and text boxes for 'Username', 'Type' (Read Only), 'Auth Type' (MD5), 'Auth Password', 'Privacy Type' (None), and 'Privacy Password'. 'Cancel' and 'Save' buttons are located at the bottom right.

This page configures SNMP v1/v2c and v3 Agent settings. SNMP lets NMS tools **actively poll** device status via MIBs; for proactive alerts, configure **Notifications**, Syslog, or email/Pushover. For trap OIDs, see the MIB file from [Download MIB](#).

Field Descriptions

SNMP Device Information

Device Name	Shown as sysName in SNMP tools; use a recognizable name.
Device Contact	Shown as SNMP sysContact; enter owner or department contact.
Device Location	Shown as SNMP sysLocation; enter rack or room location.

Download MIB Downloads this device's MIB for SNMP management tools.

SNMP v1/v2c

Enable SNMP v1/v2c	Enables SNMP v1/v2c Agent; management tools cannot access v1/v2c when disabled.
Read Community	SNMP v1/v2c read community string (default is often public); must match the manager.
SNMP Write	Enables SNMP Set; use only on trusted networks.
Write Community	SNMP v1/v2c write community string (default is often private).

SNMP v3

Enable SNMP v3	Enables SNMP v3 Agent with stronger authentication and encryption.
Username	SNMP v3 login name; must match the manager.
Type	Account permission type: read-only or read-write.
Auth Type	SNMP v3 authentication algorithm (MD5 or SHA).
Auth Password	SNMP v3 authentication password. When already set, the field shows eight asterisks (`****`); submitting those eight asterisks on save means the existing password is not changed.
Privacy Type	SNMP v3 packet encryption; None means no payload encryption.
Privacy Password	Privacy password when using DES or other encryption. When already set, the field shows eight asterisks (`****`); submitting those eight asterisks on save means the existing password is not changed.

Button Descriptions

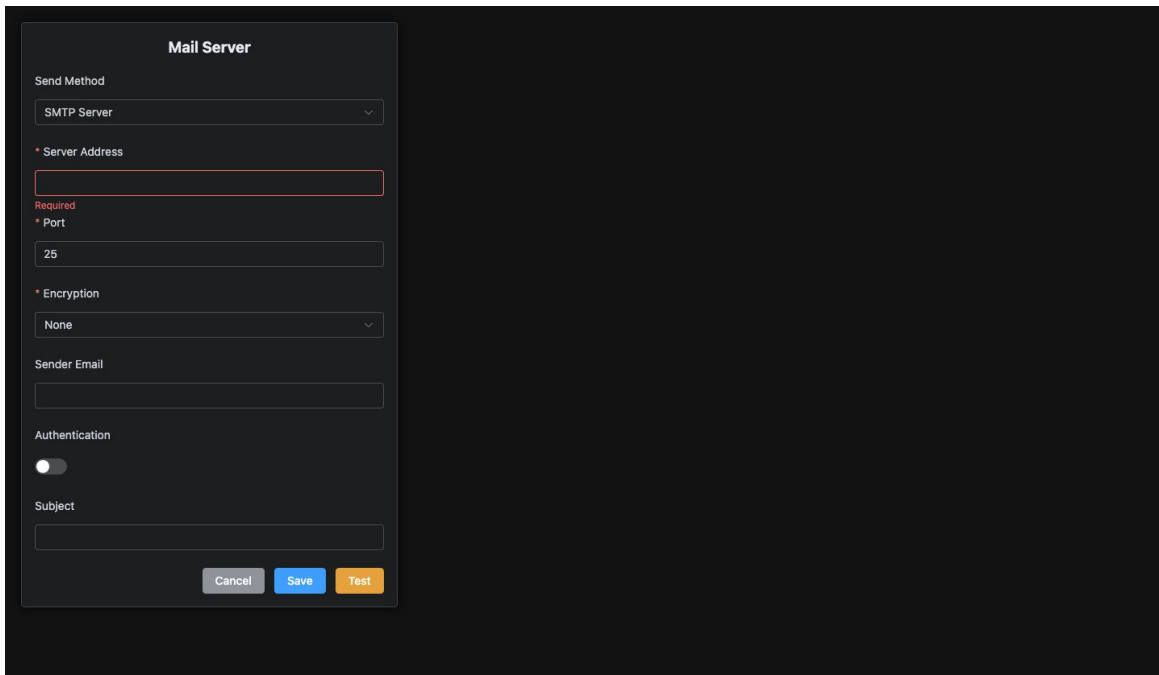
Cancel Discards changes and restores SNMP settings from when the page was opened.

Save

Saves and applies SNMP settings.

9-4 Mail Server

Navigation: Engineering > Mail Server. This page configures the mail server and related settings.



Mail Server

Send Method
SMTP Server

* Server Address
Required

* Port
25

* Encryption
None

Sender Email

Authentication
☐

Subject

Cancel Save Test

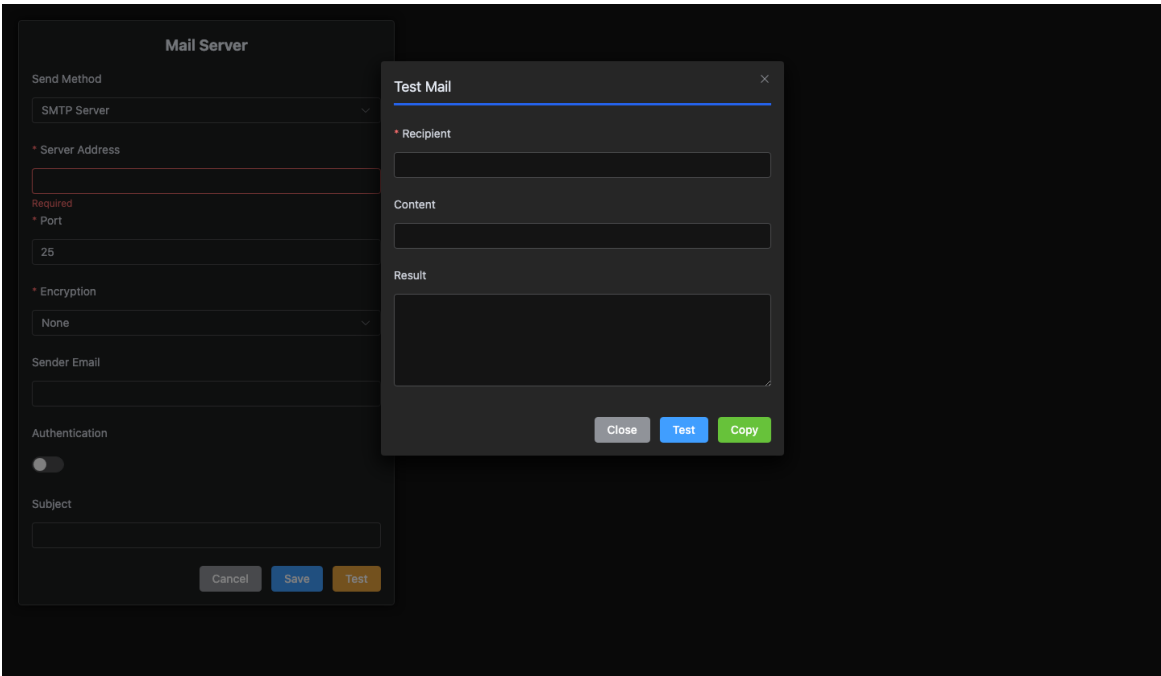
Field Descriptions

Mail Delivery Method	Send alerts and notifications via SMTP mail server.
Server Address	SMTP server hostname or IP.
Port	SMTP port (commonly 25, 465, or 587, depending on encryption).
Encryption	Transport encryption: None, SSL, or TLS; must match the mail server.
Sender	From address recipients see.
Authentication	When enabled, requires SMTP account and password.
Account	SMTP authentication account (usually full email address).
Password	SMTP authentication password. When already set, the field shows eight asterisks (`*****`); submitting those eight asterisks on save means the existing password is not changed.
Subject	Default subject prefix for alert emails.

9-4-1 Test Mail

Procedure

Press **Test** to open the test window; after filling in the email and content to be tested, press **Test** to send, and the results will be displayed in the result area.



Field Descriptions

Recipient Email	The recipient email of the test email. It is recommended to send it to yourself for confirmation first.
Content	Test email content, you can leave it blank or use the default test text.
Result	Displays the success or failure message for checking the SMTP settings.

Button Descriptions

Close	Close the test email dialog box.
Test	Send a test email based on the current SMTP settings.
Copy	Copy the test results to the clipboard.

9-5 Alert Service

Navigation: Engineering > Alert Service. This page configures the alert server and Pushover settings.

The image shows a configuration interface with two main sections: 'Alert Server' and 'Pushover'. The 'Alert Server' section contains a 'Language' dropdown menu with 'English' selected. The 'Pushover' section contains three input fields: 'API Token', 'Title', and 'User Key'. Below these fields are two buttons: 'Web' (blue) and 'Test' (orange).

Field Descriptions

Alert Server

Language: Display language for Pushover and other alert messages; choose from the dropdown (default **English**).

- **English**
- **Traditional Chinese**

Pushover

Pushover is a third-party push notification service. Before configuring, register at the Pushover website and create an application:

1. After signing in to Pushover, copy your **User Key** from **Your User Key**
2. Create an Application and copy its **API Token**

API Token	Pushover application API Token from the Pushover website.
Title	Title text shown in push messages.
User Key	Pushover User Key determining which device receives messages.
Website	Opens the Pushover website to look up or request API Token and User Key.
Test	Sends a test push to verify Pushover settings.

9-6 Syslog

Navigation: Engineering > Syslog. Lists configured Syslog server addresses and ports.

Address	Port	Tag	+ Create
No Data			

Field Descriptions

Address	Syslog server IP or FQDN; the device sends logs to this host.
Port	Syslog port (UDP default is often 514).
Tag	Custom tag to distinguish devices or purposes on the log server.

Button Descriptions

Add	Opens the form to add a Syslog server.
------------	--

9-6-1 Add Syslog

Click **Add** to open the form below.

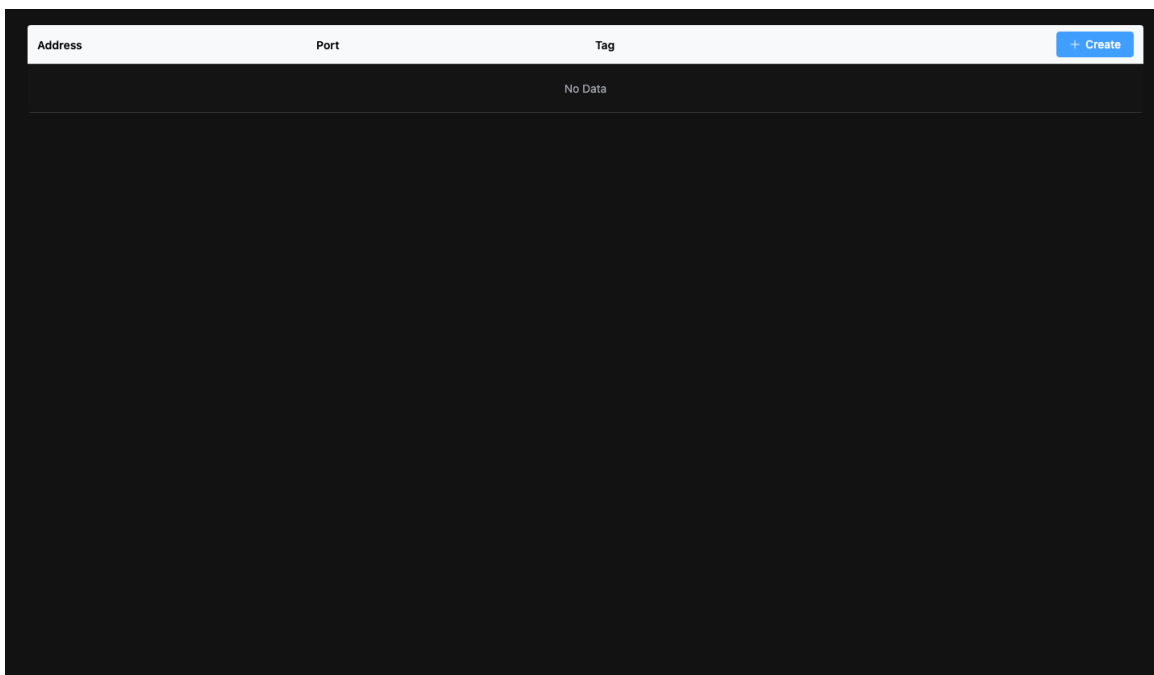
Address	Port	Tag	+ Create
No Data			

Field Descriptions

Address	Syslog server IP or FQDN; the device sends logs to this host.
Port	Syslog port (UDP default is often 514).
Tag	Custom tag to distinguish devices or purposes on the log server.

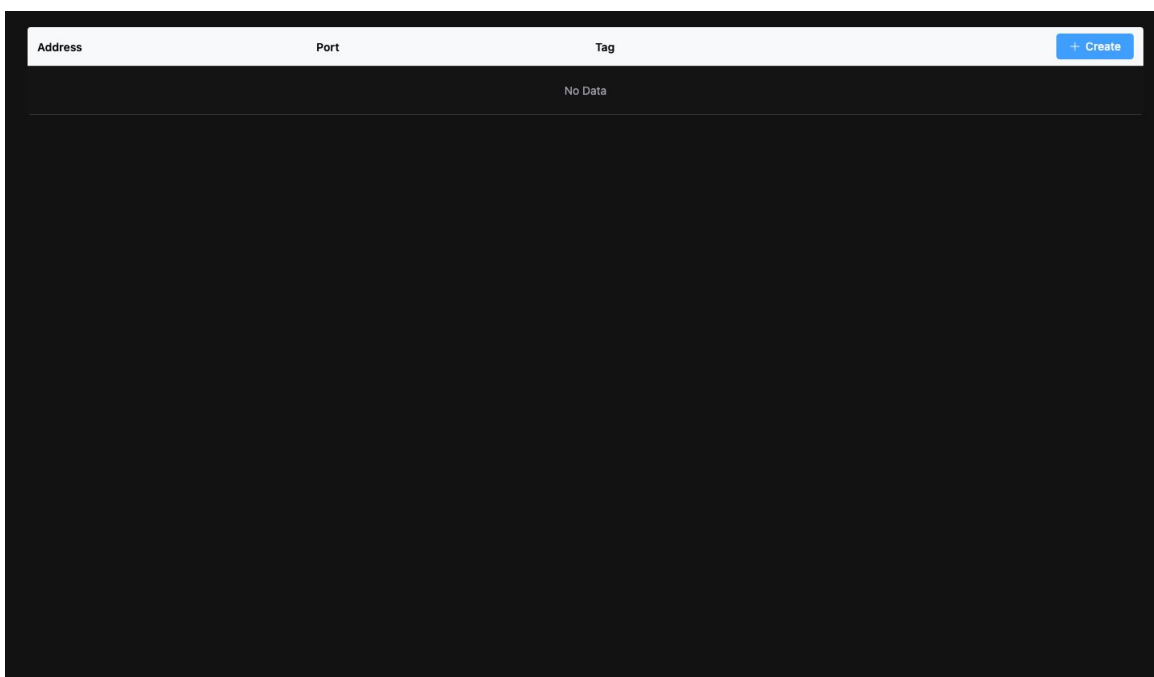
Button Descriptions

Cancel	Discards changes and returns to the Syslog list.
Save	Saves Syslog settings and returns to the list.
Test	Sends a Syslog test message.



9-6-2 Edit Syslog

Click an item in the list to open the edit screen.



Field Descriptions

Address	Syslog server IP or FQDN; the device sends logs to this host.
Port	Syslog port (UDP default is often 514).
Tag	Custom tag to distinguish devices or purposes on the log server.

Button Descriptions

Cancel

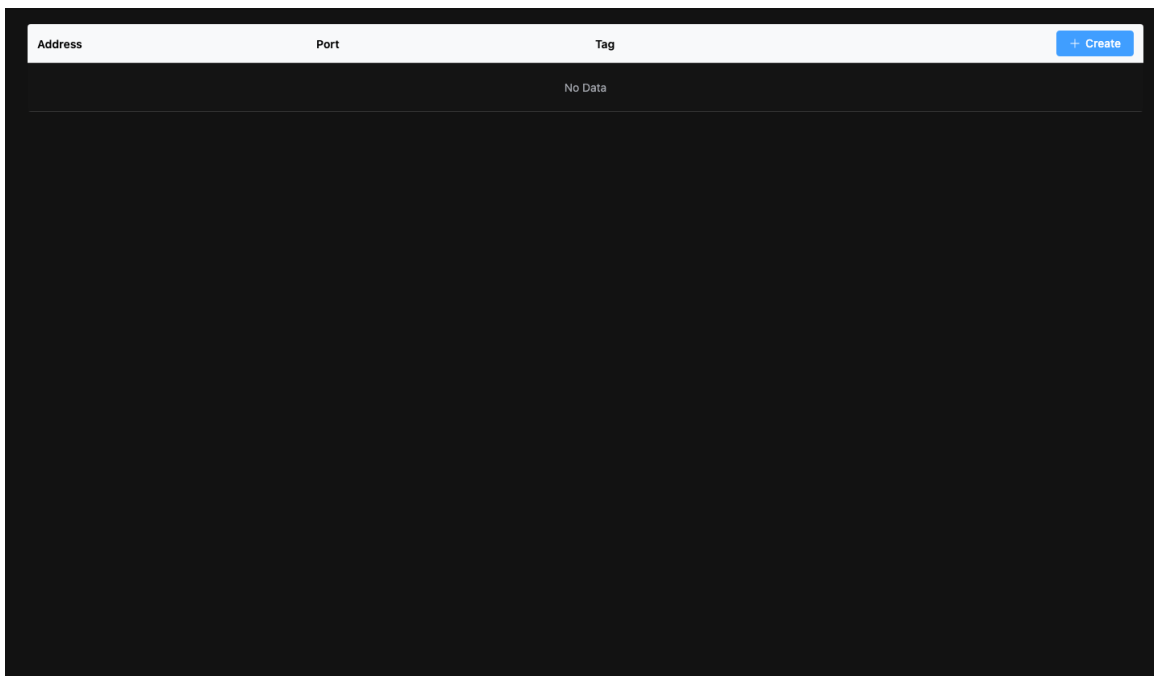
Discards changes and returns to the Syslog list.

Save

Saves Syslog settings and returns to the list.

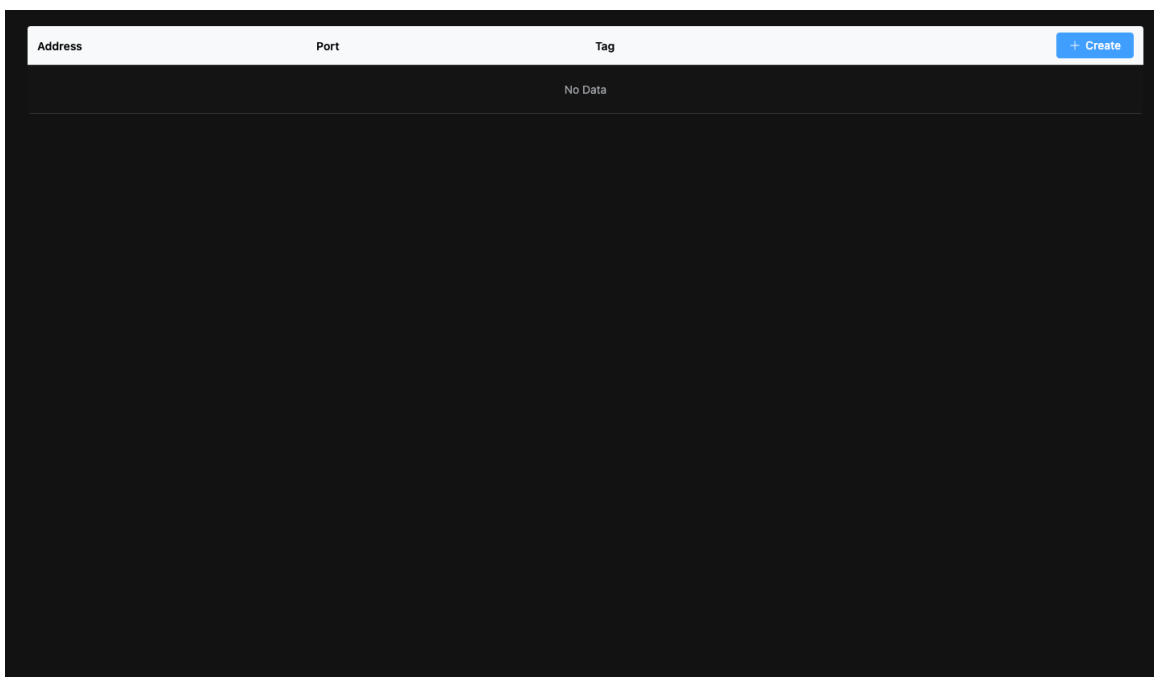
Test

Sends a Syslog test message.



Delete

Click **Delete** on the right of a list item to open a confirmation dialog.



Cancel

Discards changes and returns to the Syslog list.

OK

Confirms deletion of this Syslog server entry.

Appendix

Factory Reset

If you forget the network account password for this product, use the **RESET** button to restore the system to factory defaults. The device will also reboot.



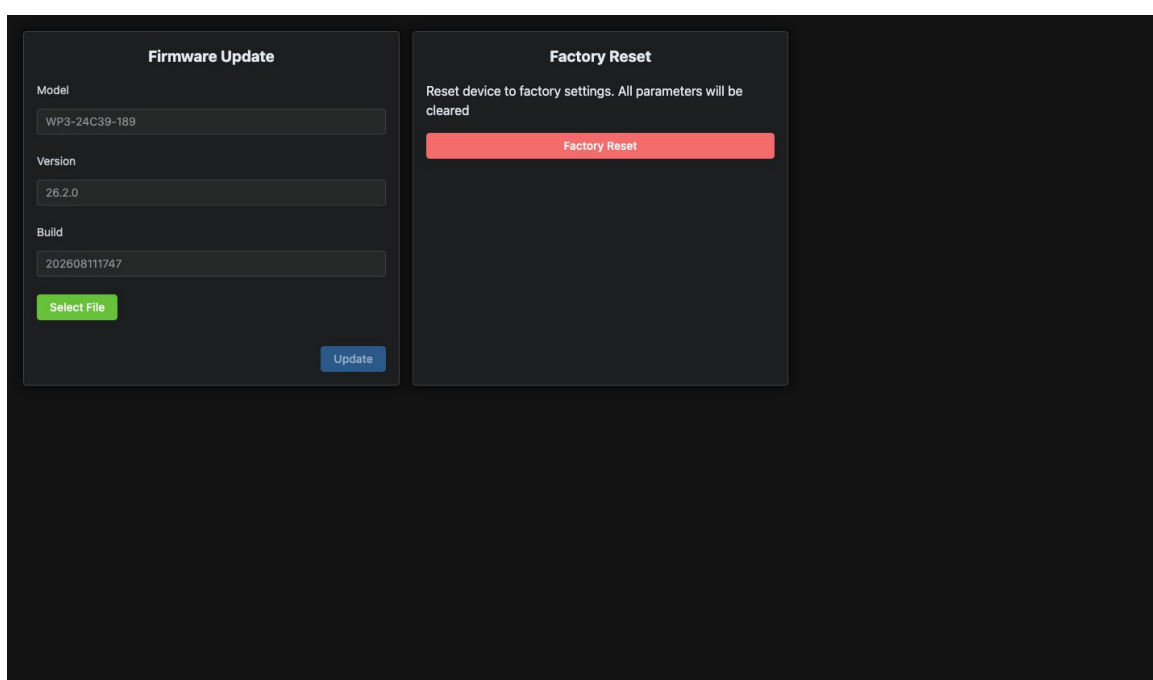
Hardware reset (pinhole)

Use a straightened paper clip to press the **RESET** pinhole on the rear panel (see the figure above; also labeled **6** in 1-4 Hardware Description).

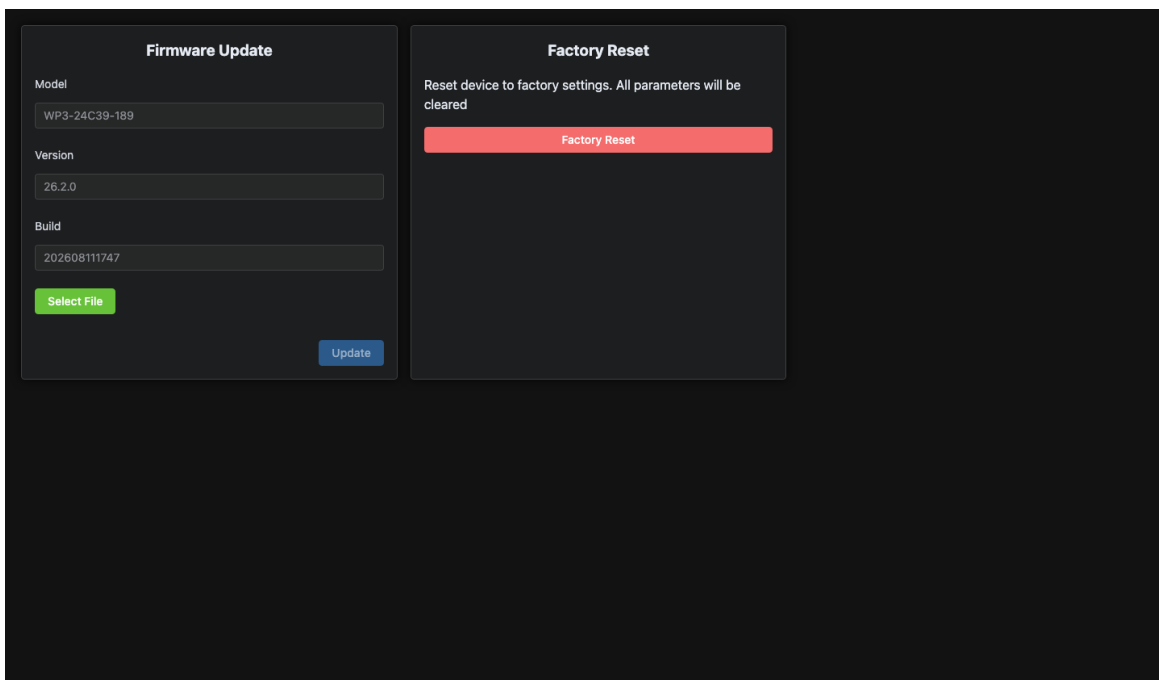
1. Press and hold **RESET** for more than 3 seconds until the red LED starts flashing. Release within 3–10 seconds to reset the **admin** password to the factory default **admin** and obtain an IP via DHCP (if no DHCP server is available, the default IP is **192.168.1.100**). After reboot, sign in with **admin** / **admin**; the system requires a password change (see 3-3 Login).
2. Press and hold **RESET** for more than 10 seconds until the LED stays solid. Release to clear all device data.

Web UI reset

Alternatively, an administrator can restore defaults from **Engineering > Firmware Update** in the web UI (see 8-3 Firmware Update). After reset, network settings return to factory defaults and the default administrator account is restored.



1. Click **Factory Reset**.
2. Confirm the dialog with **OK**; the device reboots and clears all settings.



3. After reboot, sign in with factory default **admin / admin** (see 3-3 Login).
4. The system requires a password change; set a new password per policy and click **OK**.

Warranty

This product is warranted for one year from the date of purchase against defects in materials and workmanship. If a problem occurs during the warranty period, contact your dealer for repair or replacement. Refunds are not provided. Requests for factory repair without original proof of purchase cannot be processed.

When returning this product for factory service, pack it in the original packaging, or packaging that provides equivalent protection. The package must include proof of purchase, and the RMA number must be clearly marked on the outside.

If the serial number label provided by the manufacturer has been removed or altered, this warranty is void.

This warranty does not cover cosmetic damage, or damage caused by acts of nature, accident, misuse, abuse, or unauthorized modification of any part of the product. It also does not cover damage caused by improper operation or maintenance, connection to unsuitable equipment, or repair attempts by non-authorized personnel. This warranty does not apply to products resold in "as is" or defective condition.

Under no circumstances shall the company's liability exceed the purchase price paid for this product. The company is not liable for any direct, indirect, special, incidental, or consequential damages arising from the use of this product, software, or documentation, including but not limited to loss of data, loss of profits, downtime, loss of goodwill, damage to equipment or property, or costs of replacement, recovery, or reconstruction of programs and data.

The company makes no warranties, express, implied, or statutory, regarding the product, documentation, intended use, or bundled software, and specifically disclaims warranties of quality, performance, merchantability, or fitness for a particular purpose.

The company reserves the right to modify or update this product, software, or documentation without prior notice to any individual or entity.

For more information about extended warranty options, contact your dealer.