EDGELOR

MT7628

OpenWrt System and Management Basics

First login, configuration, backup, authorized extensions and application recovery

English | V1.3 | 2026-11-06

Models: YZW300X, YZW350L, YZW400, YZWK001 and YZW1010

Contents

Page numbers refer to this PDF. Select a chapter to open it; use Contents in the footer to return.

01 | Understand the delivered capabilities 4

1.1 What OpenWrt means on this product 4

1.2 Resources and model differences 4

1.3 Capabilities and standard delivery 5

02 | First login and secure access 5

2.1 Before connecting 5

2.2 Log in locally and change the administrator password 5

2.3 Web, CLI, SSH and physical serial access 6

03 | Save settings, check state and set time 6

3.1 Entered values, saved configuration and working service 6

3.2 Example: change LAN and log in again 7

3.3 Set time and establish a baseline 8

04 | Persistent storage and extensions 8

4.1 What survives a restart 8

4.2 Five checks before extending software 8

4.3 Planning scripts on MT7628 9

05 | Back up, restore and update 9

5.1 Define the backup scope 9

5.2 Make a traceable backup 10

5.3 Reboot, restore and reset are different 10

5.4 Safely update through the Web UI 10

06 | Remote maintenance and permissions 11

6.1 Verify the entire remote path 11

6.2 Maintain each access system separately 12

07 | Routine maintenance and diagnosis 12

7.1 Collect evidence before restarting 12

7.2 MT7628 example: MQTT stops reporting after a restart 13

7.3 Optional read-only checks in an authorized Linux Shell 13

08 | Acceptance and support records 13
8.1 Basic delivery acceptance 13
8.2 Send a complete support record 14
8.3 Scope and related material 15

01 | Understand the delivered capabilities

1.1 What OpenWrt means on this product

> **Read before purchase | Product-specific OpenWrt build**
>
> These products use a customized OpenWrt-based system containing the components required for the device and delivered functions. It is not a complete stock OpenWrt installation; other original components have been removed.
>
> **Before purchase, confirm that the required functions are retained and supported on the exact model, firmware and delivered configuration.**
>
> The words OpenWrt-based do not establish the presence of any particular package, function or development permission.

This product uses OpenWrt-based Linux with YZW Web management for delivered network, system and application functions. The UI is not generic LuCI. Community menus, package feeds, file paths and flashing procedures may not apply.

This guide covers **MT7628**, specifically YZW300X, YZW350L, YZW400, YZWK001 and YZW1010, for initial setup, routine maintenance and support. A shared platform does not imply identical interfaces, software or permissions. The exact model, order and delivered firmware take precedence.

1.2 Resources and model differences

Model	Memory/storage in current specifications	Practical meaning
YZW350L, YZW400, YZWK001, YZW1010	128 MB DDR2; 16 MB SPI NOR	Use the delivered networking, acquisition and maintenance functions. Do not plan installations as though all 16 MB were free.
YZW300X	128 MB DDR2; 32 MB SPI NOR	The storage layout differs from the 16 MB models; firmware is not interchangeable. LoRa functions require the corresponding model hardware and software.

K001, 350L, 400 and 1010 have different Ethernet, serial and cellular configurations. K001 has a LAN port, not the separate wired WAN arrangement of 350L. Match the ordered cellular module on 400; do not extend one model interface inventory to the entire platform.

1.3 Capabilities and standard delivery

Item	Current capability/boundary	Customer action
Web management	YZW custom Web UI	Follow this unit menus and manual, not generic LuCI tutorials.
Shell and Python	Current specifications list Shell and Python 3 environments	This does not authorize login or script upload. Agree deployment access, dependencies and startup behavior separately.
Node.js, Node-RED, Docker	Not standard delivered capabilities of the listed MT7628 products	Do not promise installation through generic plugins; assess customization or another product for these requirements.
Third-party packages	Arbitrary installation, upgrades and compatibility are not promised	Match MIPS architecture, kernel, dependencies and writable storage. MT7981 ARM packages are not interchangeable.
Web user accounts	The current account page changes the existing admin password	It does not add users, enable guest accounts or assign roles.
SSH/root	Subject to delivered authorization	Standard K001 samples do not expose SSH. Web admin credentials are not Linux root credentials.

Not standard means the function must not be promised as an already-delivered capability. It does not prove that the processor could never implement it. Agree scope, compatibility and support before customization or model selection.

02 | First login and secure access

2.1 Before connecting

Prepare the exact model manual, product label/delivery information, stable power and management PC. Prefer local wired LAN access. Use only a port identified as LAN or already configured as LAN; do not assume a WAN port allows management.

Record the current management address, HTTP/HTTPS scheme and port. Use delivered settings on a new unit and current settings on an installed unit. Example IPs are not factory defaults. Keep the PC in the management subnet and avoid duplicate addresses.

2.2 Log in locally and change the administrator password

1. Connect as specified for the model. For DHCP, check the obtained address; for static addressing, check address, mask and conflicts.

2. Enter the real management address in the browser address bar. Include a non-default port when applicable. Use delivered credentials, not assumed community OpenWrt defaults.
3. On Home verify model, interfaces and uplink. Open **System Management > User Management**, change the existing admin password and follow the actual validation rules.
4. Keep the original session open. Test the new password in a private browser window, then close the old session and update the controlled credential record.

Pass condition: a new login succeeds, the password is effective and the management address/subnet are recorded. If the page is inaccessible, check cabling, PC address, port role and scheme/port before considering a reset.

2.3 Web, CLI, SSH and physical serial access

Entry/account	Purpose	Important distinction
Web management	Configure delivered functions in a browser	An HTTPS switch does not prove HTTPS is active; reconnect with the actual port and verify server identity.
Product CLI	Authorized product commands	Not necessarily a Linux Shell; commands and permissions may differ.
SSH/Linux Shell	Authorized service or customization	Requires explicit access, account and connection arrangements. This guide does not enable restricted access or root.
RS232/RS485	Connect field business devices	A business serial port is not a Linux debug console; do not attach a generic console cable.

HTTP and Telnet do not provide transport encryption. On untrusted networks use delivered HTTPS or an authorized secure tunnel. Keep a recoverable local access path before changing management settings.

03 | Save settings, check state and set time

3.1 Entered values, saved configuration and working service

These are three different results. Save the entry, save the parent/global settings and enable the function where required. Reopen the page to confirm; one success notification is insufficient.

Stage	Action	Observable result
Entry/global settings	Complete Save/Apply instead of closing an unsaved page	Values and enable state remain correct after reopening.

Stage	Action	Observable result
Runtime	Check the actual interface/service/tunnel	It runs without repeated errors.
Application	Make a new request or publish fresh data	The peer receives this operation with a matching time.
After reboot	Reboot only in a maintenance window and repeat checks	Settings and required service recover as agreed.

Low-level network files may be regenerated by product management. Use Web settings for routine changes. Obtain the supported firmware-specific automation method before scripting configuration; do not copy generic UCI commands blindly.

3.2 Example: change LAN and log in again

This is an **isolated example, not a factory default**. Back up first, ensure the subnet is unused locally and remotely, and retain local cabling.

Item	Example	Meaning
Menu	Network Settings > LAN	Confirm the management LAN is being changed.
IP/mask	192.168.50.1 / 255.255.255.0	Plan the matching DHCP pool.
Static management PC	192.168.50.100 / 255.255.255.0	Must not duplicate another device.
PC gateway, if Internet access is needed	192.168.50.1	External access is not needed merely to open a same-subnet page.

1. Save the LAN change. A lost browser session is expected while settings apply; do not repeatedly reset.
2. Change a static PC address or renew DHCP. Confirm the new subnet and pool; use Windows `ipconfig` to check the actual address.
3. Reopen the new address with the valid scheme and port. `ping 192.168.50.1` is a supporting check, not a requirement if ICMP is disabled and Web access works.
4. Update static PLC/camera addressing, VPN local subnets, NAT targets and saved client addresses where necessary. Export the new working configuration.

If access fails: check PC address/lease, management-port role, scheme/port and conflicts. Check the old address if the change did not save. Do not perform this change over the only remote management path without local assistance.

3.3 Set time and establish a baseline

Open **System Management > System Time**, select the site time zone and reachable administrator-provided NTP servers, save and check the device time/synchronization result. Logs, certificates and schedules depend on device time, not the PC clock.

Record uplink, uptime and the CPU/memory state actually provided on Home. Use delivered storage-status access or support assistance when needed. Nominal Flash is not writable free space, and cache usage alone does not establish a leak.

04 | Persistent storage and extensions

4.1 What survives a restart

Current NOR models use a read-only system image and a separate writable area. The source includes SquashFS and JFFS2 configuration/data partitions; sizes vary with Flash capacity. Neither 16 MB nor 32 MB is entirely available for programs and logs, and community configuration paths must not be assumed.

Content	Expected after an ordinary reboot	Maintenance rule
Factory system/built-in programs	A normal reboot does not select another firmware	Use an approved model-specific update, not direct system-file replacement.
Saved product configuration	Must persist as delivered	Save, reopen and verify after an approved reboot.
`/tmp` and other RAM-backed data	Not persistent; normally lost on restart	Never keep the only copy of a script, certificate, backup or data there.
Flows, databases, certificates and custom files	Depends on the application and actual path	Confirm persistent location, backup method and update/reset behavior separately.

Example: a small Python script may pull in dependencies and produce logs that fill the writable area and prevent settings from being saved. First collect storage usage and the exact error; ask the supplier which application files may be removed. Do not delete unfamiliar system directories. Send long-term records to the customer server.

4.2 Five checks before extending software

1. **Authorization and entry:** whether customer deployment is allowed and the approved Web/application/service path.
2. **Compatibility:** architecture, bitness, kernel, system libraries, runtime and native dependencies.
3. **Resource headroom:** installed size, working memory, log/cache growth; nominal capacity is not free space.

4. **Conflicts:** serial ports, listening ports, network rules and startup resources already in use.
5. **Maintenance:** restart behavior, upgrade migration, failure rollback and the responsible maintainer.

Do not bulk-upgrade packages, replace feeds or execute generic `opkg`/`apk` install instructions from tutorials. Package-manager availability, feed compatibility and support scope depend on delivered firmware. Prefer supplier-approved compatible system fixes.

4.3 Planning scripts on MT7628

A Python environment does not mean a PC project can run unchanged. Provide the purpose, third-party dependencies, package sizes, expected log volume and execution interval, then check the delivered runtime. Some libraries require native build components that may not be present.

Prefer delivered acquisition, MQTT and VPN functions. For an authorized custom script, agree a persistent deployment location, startup and restart policy, and upgrade-retention behavior. Do not use `/tmp` as permanent storage or promise that arbitrary `pip install` commands will succeed.

Assign one application to each physical serial port at a time. DTU, Modbus, remote COM and scripts must not open the same port concurrently. Confirm the number and electrical type from the model specification.

05 | Back up, restore and update

5.1 Define the backup scope

Export through **System Management > Configuration Management**. A configuration file is **not a full disk image or an automatic backup of all applications**.

Content	Backup method	Restore checks
Gateway network/system settings	Export the original format from configuration management	Match model, hardware/storage layout and supported version; verify LAN, uplink, roles and access rules.
VPN/platform/Broker credentials and certificates	Confirm export coverage; retain missing items securely	Web admin is not the authentication for every application.
Point maps and application settings	Use the relevant export/delivery method separately	Check device addresses, serial parameters, maps, topics, credentials and enable state.
Authorized scripts and dependency inventory	Retain separately as agreed; do not assume the gateway export includes them	Test startup, reporting and log limits on the same compatible model.

5.2 Make a traceable backup

1. Record exact model, hardware/storage, management address, actual firmware and date; click Backup in configuration management.
2. Verify the downloaded file is present and nonempty. Retain the actual extension; a model_site_date filename is suitable. Do not edit its contents.
3. Collect separate application exports, certificates and point maps. Backups may contain secrets; store them in a controlled project folder and use redacted copies for public support.
4. On Windows, record the checksum using the actual filename. A hash detects file changes; it does not prove recoverability.

```
Get-FileHash -LiteralPath '.\backup.cfg' -Algorithm SHA256
```

5. Verify recovery on a compatible same-model spare or in an approved maintenance window. A successful download proves export; restored applications prove usefulness.

5.3 Reboot, restore and reset are different

Operation	Site impact	Next step
Reboot	Interrupts sessions, not intended to clear saved settings	Wait for startup and verify uplink, remote path and applications.
Import compatible configuration	May restore previous LAN, passwords, roles and application settings	Reconnect using the backup address/credentials and verify every relevant function.
Factory reset	Restores management/application settings under model rules; data may follow separate rules	Back up and prepare cabling, login and application recovery.
Firmware update	Changes system software; retention depends on the approved release	Confirm compatibility and revalidate applications.

A factory reset changes management and application settings. A reboot is not a factory reset, and a reset is not a universal repair for a failed update. Use the exact model reset instructions instead of a generic button-hold duration.

5.4 Safely update through the Web UI

1. Obtain the approved file for the exact model, hardware and Flash layout, together with checksum, compatibility notes and rollback method. A shared CPU is not permission to cross-flash.
2. Export configuration and separate application data. Confirm the maintenance window, stable power and local management path.

3. In **System Management > Firmware Upgrade**, use **Factory reset after upgrade**: **select it when the new firmware changes configuration; leave it unchecked for a program-only update with no configuration changes**. Checked means reset, not retain. After a reset reconfigure as required; old-backup compatibility is a separate decision.
4. Select the approved file and upload using stable local wired access where possible. Do not interrupt power or force a reset while writing. Wait as instructed, then check management address, scheme/port and renew the PC lease if needed.
5. Verify the actual version, configuration, uplink, VPN, acquisition, reporting and applications. An update-complete message does not prove service recovery.

If upload is rejected or the unit becomes inaccessible: retain filename/hash, full error and time. Check model/layout and management settings first. Contact support if boot state is unclear; do not try stock OpenWrt, another model image, forced flashing or an unapproved downgrade.

06 | Remote maintenance and permissions

6.1 Verify the entire remote path

Work in order: **local service baseline > authorized VPN/platform channel > routes/access rules > actual remote target**. An online gateway alone is insufficient.

Layer	Check	Pass result
Local equipment	Gateway LAN, PLC/camera IP, target service and return path	A site PC reaches the actual target address and required port.
Uplink	Real cellular/wired connection, DNS and approved outbound ports	Gateway reaches the agreed remote service.
Secure channel	VPN/m2mCloud authorization, tunnel and routes	Remote traffic reaches the site subnet, not only the control connection.
Application operation	Vendor tool/browser target and protocol	A new read/access succeeds; control follows site permission and safety rules.

With cellular CGNAT, direct inbound Internet access to the SIM address is generally unavailable. An outbound connection to a reachable authorized VPN/platform may provide the path. If neither peer accepts inbound connections, arrange a reachable server or appropriate relay. DDNS updates DNS; it does not itself create inbound CGNAT reachability.

An ordinary Layer-3 VPN routes IP traffic; it does not automatically forward Layer-2 vendor discovery broadcasts. Check the tool and delivered topology. Test an explicit IP first when supported. Agree platform/server, licensing, relay ownership and fees separately; OpenWrt does not make them automatically free.

6.2 Maintain each access system separately

Use the delivered management-access page to allow the intended LAN/WAN/VPN sources and protocols. Restrict WAN management when unnecessary. Test both an allowed and a denied source after changes, retaining local recovery access.

Web admin, VPN keys, platform accounts, Broker credentials and application accounts are separate. Changing the Web password does not rotate the others. A restored backup may also restore old credentials; verify again after import.

Development requests: OpenWrt-based does not mean standard SSH/root, an SDK or arbitrary production flashing is provided. Agree exact model, compatibility, authorization and maintenance responsibilities before implementation.

07 | Routine maintenance and diagnosis

7.1 Collect evidence before restarting

Open **System Management > Local Log**, match the failure time/module and export or save logs before deciding on a restart. Persistence depends on configuration; complete previous logs may not survive power loss.

Symptom	Check first	Evidence for support
Web page inaccessible	Cabling, PC IP, LAN role, actual URL, scheme/port and access rules	PC addressing, connection sketch, URL and full error.
Save fails or settings revert	Field validation, entry/global saves, writable storage and actual version	Save message/time, redacted configuration and storage diagnostics.
Gateway online but no data	Fresh acquisition, application enable, endpoint/authentication/topic	Same-period input values, connection logs and receiver records.
Wrong time/certificate error	Time zone, device clock, NTP, then certificate identity/validity	Device time, full error and redacted certificate information.
Sustained CPU/memory anomaly	New tasks, repeated reconnects, error logs or duplicate processes	Normal/abnormal state, duration and recent changes.
Remote gateway reachable, field device not	Target service, subnet conflicts, routes, return path and access rules	Local/remote stage tests and a redacted topology.
Inaccessible after restore/update	Previous/default address, PC lease, scheme and changed port	Before/after model/version, file hash and UI messages.

7.2 MT7628 example: MQTT stops reporting after a restart

1. Verify local LAN management and then actual cellular/wired connectivity. Signal LEDs alone do not establish Internet access.
2. Reopen MQTT and acquisition settings. Check global enable, the point map and all parent entries; saving a map alone does not enable reporting.
3. If settings reverted, supply save time, writable-space information and logs. If settings remain but the connection fails, check server address, DNS, port, authentication and system time.
4. Have the server confirm a new real message with its time and topic. An old retained message or a connected status is insufficient.

Pass condition: after an approved maintenance-window reboot, settings remain, connectivity recovers and the server continues receiving new data.

7.3 Optional read-only checks in an authorized Linux Shell

Only formally authorized Linux-Shell users should run these commands. Ordinary Web users can skip them; a product CLI may not recognize them. Check availability on the unit. These observe state and do not change configuration.

```
uptime
free
df -h
mount
```

Use `uptime` for uptime/load, `free` for working memory, `df -h` for mounted storage and `mount` to distinguish temporary/persistent mounts. Redact internal paths/addresses before sharing. If a command is absent, use Web status or support; do not install tools just to reproduce this list.

08 | Acceptance and support records

8.1 Basic delivery acceptance

Check	Pass condition	Project record
Model and delivery scope	Hardware/storage, interfaces and required applications match the order	Model, hardware and configuration revision.
Local management	Correct LAN access and new-password login work	URL, scheme and port; store passwords separately.
Time/state	Time zone and device clock are correct; status matches real communication	Time, uplink and normal baseline.

Check	Pass condition	Project record
Settings retention	Save, reopen and approved reboot verification pass	Retest time and actual application result.
Recovery preparation	Configuration and independent data are collected; compatibility/restore entry are known	Filenames, hashes and controlled storage location.
Remote access, if used	Tunnel, routes and actual target service pass separately	Targets and results, not merely online.
Lightweight extensions	If used, deployment authorization, dependencies, storage and post-reboot behavior are confirmed	Otherwise mark not applicable; attach deployment and recovery evidence when used.

Platform-specific check: Do not confuse nominal 16/32 MB Flash with free space, or promise Node-RED and arbitrary Python dependencies.

8.2 Send a complete support record

Information	Include
Product	Exact model, hardware/storage, device identifier through a controlled channel.
Software	Actual displayed firmware and application versions, plus update history.
Network	Redacted topology, uplink, CGNAT situation and local/remote subnets.
Symptom	Expected/actual behavior, start time and reproducibility.
Changes	Recent settings, applications, wiring or uplink changes.
Verification	Separate local/remote tests and same-period logs/receiver results.
Recovery	Compatible backups, on-site assistance and available maintenance window.

Do not post plaintext passwords, VPN private keys, full sensitive backups or customer device keys in public messages or screenshots. Use the controlled support method when configuration analysis is necessary.

8.3 Scope and related material

This guide reflects current product documentation and selected read-only source as of November 2026. It explains operation and applicability, not a substitute for the exact model manual, delivery agreement or site acceptance. No new hardware deployment, RF, load or field-application result is claimed.

Related product manual: use the optimized YZW350L manual in the accompanying model folder. Follow its live contents for first login, management access, system administration and application-specific steps; superseded page numbers are not reused. Check the current model specification separately.

OpenWrt background: Filesystems and Flash layout explain general temporary/read-only/writable storage concepts. They are not product-specific instructions for package installation, repartitioning or flashing. Use the model manual and supplier-approved release procedure for actual changes.