YZW PRODUCT GUIDE / DETAILED CUSTOMER EDITION

Common maintenance guide

Firmware Upgrade, Backup, Restore and Recovery Guide

Step-by-step operation, evidence, diagnosis and recovery

For PLC, camera, VPN and LoRaWAN/Node-RED installations. Distinguish normal updates, configuration restore and conditional engineering recovery. Each step explains behavior, evidence, remedy and when to continue.

Prepare
Identify and back up

Update
Transfer, validate, write, boot

Diagnose
Behavior, logs and state

Recover
Settings, network and fresh data

Supported Web maintenance is separate from conditional engineering routes; routine customer work requires no SSH.

English • V2.1 • 2026-11-05

Models: MT7628: YZW300X / YZW350L / YZW400 / YZWK001 / YZW1010; MT7621: YZW280 / YZW380 / YZW800L; MT7981: YZW001L / YZW300L / YZW800 / YZW900 / YZW900L / YZW1000

Contents

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

01 | Choose the method for your situation 4
1.1 Current models and relevant differences 4
1.2 How many methods are available? 4
1.3 Match the route to your application 5
02 | Step A: identify the unit, file and local access 5
2.1 Create a maintenance record before choosing an image 5
2.2 Check the file on your computer 6
2.3 Prepare power and the maintenance network 6
03 | Step B: capture evidence before maintenance 7
3.1 Export Event and System logs in Web 7
3.2 What the files mean at each stage 9
3.3 Read-only collection by an authorized engineer 9
04 | Step C: make a recoverable backup 10
4.1 Export committed gateway settings 10
4.2 Include application-specific data 11
05 | Step D: Web image selection and reset choice 11
5.1 Fill fields and submit once 11
5.2 Three outcomes of the reset decision 13
06 | Step E: distinguish upload, validation and writing 13
6.1 Immediately after submission: resource preparation 13
6.2 File transfer: progress and cache are not write results 14
6.3 Image and medium validation: the old OS may still run 14
6.4 Writing/reboot has started: avoid escalation 15
07 | Step F: reconnect and prove the update 15
7.1 Select the correct post-update address 15
7.2 Three checks complete the update 16
08 | Step G: restore settings or a compatible spare 16
8.1 Define the restore scope before import 16
8.2 Choose the original backup and import once 17

8.3 Worked example: the management address changes 17
09 | Scenario: update a remote site through VPN 18
9.1 Prepare for loss of access before updating 18
10 | Conditional route: authorized engineering CLI 18
10.1 Establish why this is not a Web-failure shortcut 18
10.2 Four engineering steps and their checks 19
10.3 Two common tool/file mistakes 19
11 | Conditional route: Bootloader Web recovery 19
11.1 Confirm the actual loader entry 19
11.2 Establish the recovery network and enter the loader 20
11.3 Select the approved object/image in the real loader page 21
12 | Conditional route: TFTP and debug-console recovery 21
12.1 Identify the transfer direction first 21
12.2 Record transfer, validation, writing and boot separately 22
12.3 Diagnose an unreadable or silent console 22
13 | Step H: reboot, factory reset and the button 23
13.1 Choose the right operation while Web still works 23
13.2 Web lost but OS running: use the delivered Reset rule 23
13.3 Factory reset is not complete data erasure 24
14 | Step I: restore and verify the actual application 24
14.1 Restore network, remote access and field traffic in order 24
14.2 PLC/Modbus and cameras: concrete post-maintenance checks 25
14.3 MT7981 Node-RED and local LNS: independent data 25
15 | Scenario: downgrade, failed write or return repair 26
15.1 Confirm compatibility/reset policy before rollback 26
16 | Close maintenance: acceptance and handover 26

01 | Choose the method for your situation

This guide is for field maintainers and platform administrators. Each step includes expected behavior, failure evidence and a remedy. Confirm the current step before proceeding. Decide whether the unit boots and accepts login before choosing an update or recovery path.

1.1 Current models and relevant differences

Platform / models	Differences to check
MT7628: YZW300X / YZW350L / YZW400 / YZWK001 / YZW1010	Use the exact model/NOR layout. Do not cross-flash 300X and the other models. Normal-system Reset has a 15-second patch-clear tier.
MT7621: YZW280 / YZW380 / YZW800L	Record the actual management port and WAN/LAN role. Standard YZW280 and K001 samples do not provide SSH.
MT7981: YZW001L / YZW300L / YZW800 / YZW900 / YZW900L / YZW1000	Check actual NAND/NOR and eMMC configuration. Back up Node-RED/LNS separately. Preserve the PoE power cable when it powers YZW900.

1.2 How many methods are available?

The guide describes five maintenance routes below. **The confirmed common customer system-update entry is route 1, Web upgrade.** Route 2 uses that same Web mechanism. Routes 3–5 require specific engineering or recovery support; they are not five independently available update features on every unit.

Route / situation	Procedure / chapter	Conditions
1 Local Web system update	Boot normally and upload the system package through the confirmed management port; chapters 05–07.	Supported customer route: Web permission, correct SYS package and stable power.
2 Web through VPN/authorized access	Verify upload connectivity and onsite fallback, then use the same update page; chapter 09.	Not another flashing protocol. Have a workable onsite plan for loss of remote access.
3 Authorized engineering CLI	Supplier executes the unit-specific approved preflight/script; chapter 10.	Low-level upgraded is not a supported customer substitute. Generic sysupgrade cannot directly install an .ent package.
4 Bootloader Web recovery	Only where this unit has a loader Web page: enter it and upload its approved recovery image; chapter 11.	Working loader, confirmed entry/file/port/wiring. Do not assume CFE across models.
5 TFTP / debug-console recovery	Transfer, validate and write through the unit-specific approved loader procedure; chapter 12.	TFTP transfers bytes; the serial console controls/records the process. Neither makes a cable-only flashing method.

Automatic USB/SD updates, cloud OTA/bulk deployment, Bootloader replacement and boot-medium conversion are not confirmed common capabilities for these 14 models. A connector, SDK utility or historical CFE chapter does not establish support on this unit.

1.3 Match the route to your application

Customer situation	Decision and completion
YZW280 with PLC, program-only update	Back up the project and gateway. Leave factory reset off when configuration is unchanged. Verify target version, local PLC communication and remote engineering access.
K001 camera sites with 350L at the office	Video/VPN will be interrupted. Arrange onsite support first. Camera recordings and gateway settings have separate backups. Verify fresh video after the tunnel returns.
300L/900L with local LNS or Node-RED	Back up applications independently. Configuration changes require the factory-reset option and reconfiguration. Verify fresh uplinks/application events, not only gateway online.
Old IP fails after restore	Reconnect using the backed-up management address; chapter 08. Do not mistake an address change for flash damage.
Power failed during update; OS does not boot	Check supply and boot evidence first. If the normal system is unavailable, identify the supported recovery conditions in chapters 11–12.

02 | Step A: identify the unit, file and local access

2.1 Create a maintenance record before choosing an image

1. Record the exact label/Web model, hardware/storage and current version. Obtain the target version, applicable hardware, full filename, byte count, SHA256 and expected wait window from the supplier release record.
2. Record the current management IP, HTTP/HTTPS, port, physical interface, PC address, uplink and remote route in the supplied worksheet. 192.168.10.1/24 is an example maintenance plan, not a universal default.
3. Determine whether the new firmware changes configuration. Select factory reset for configuration changes; leave it off for a program-only update with unchanged configuration. Obtain the release decision before submission if unknown.

Failure / device behavior	Evidence to inspect	Remedy and retest
Only a chip/case model is known; images differ by NOR/NAND	Label, order record and boot medium on the update page; /proc/mtd only with authorized console access.	Have the supplier match the exact layout. Do not submit an unidentified image.
Package applicability differs from the unit	Release record, original filename and actual model/storage.	Obtain the matching package. Renaming cannot change its internal identity.

Failure / device behavior	Evidence to inspect	Remedy and retest
No recorded address/credentials	Delivery record and an existing valid management session; do not guess root credentials.	Establish working local management before scheduling the update.

2.2 Check the file on your computer

The Web system package is normally a supplier-issued `SYS_*.ent` file. Keep its original name. Extract an outer delivery ZIP as instructed, but do not unpack or alter the system package itself. SYS_approved.ent below is a placeholder.

```
Get-Item -LiteralPath '.\SYS_approved.ent' | Select-Object Name,Length
Get-FileHash -LiteralPath '.\SYS_approved.ent' -Algorithm SHA256
```

Compare the complete SHA256 and byte length in PowerShell. Use an existing SHA256 tool on Linux/macOS; do not compare different algorithms. See Microsoft Get-FileHash. A match checks file identity against the release record, not model, source authenticity or configuration compatibility.

File symptom	Diagnosis	Remedy
Zero bytes, incomplete download or different SHA256	Check download completion and the actual disk file, not only a chat preview name.	Download again from the approved source. Verify length and SHA256 before selection.
ZIP, configuration backup, FW_/BOOT_/G_ image or modem firmware selected	Compare the release purpose with the Web SYS-package requirement.	Use the unit’ s system package. Import settings in Config Management; use dedicated recovery/loader procedures for other images.
PowerShell command/path fails	Use PowerShell and quote the actual path with -LiteralPath.	Correct the environment/path. A tool error is not a reason to skip verification.

2.3 Prepare power and the maintenance network

1. Use the confirmed management interface and cable during the maintenance window. Preserve the actual power route. If YZW900 uses WAN PoE input, do not unplug it to leave only LAN.
2. Match the PC subnet to current management. Record VPN/proxy/other adapters to avoid a conflicting private route. Confirm local Web login before proceeding.
3. Notify PLC/camera/platform owners of interruption. Record one known-good live point, video stream or LoRaWAN application event. Avoid concurrent updates, imports, scheduled reboots and other maintenance.

```
ipconfig /all
ping.exe -n 4 192.168.10.1
Test-NetConnection -ComputerName '192.168.10.1' -Port 80
```

Device / PC behavior	Immediate check	Remedy and condition to continue
No link or repeated link loss	Power indication, PoE/DC path, cable and PC adapter; use model-specific LED definitions.	Repair supply/link and confirm stability. A link LED proves only physical connectivity.
Ping fails but Web works	ICMP may be restricted; check the actual HTTP/HTTPS port.	Use successful Web access as the criterion; do not reset solely for failed ping.
Ping works but Web fails	TCP port, protocol, VPN/proxy and access rules. Test-NetConnection tests the chosen TCP port only.	Use the unit’ s actual address/port and log in. TCP reachability does not grant upgrade permission.
Only remote access exists, no onsite person	Post-maintenance address/credentials, fallback and attendance plan.	Arrange onsite recovery conditions before the remote procedure in chapter 09.

See Microsoft Test-NetConnection for diagnostic output. The guide does not execute commands on your PC or unit. Replace example addresses and ports.

03 | Step B: capture evidence before maintenance

3.1 Export Event and System logs in Web

Open **System Management > Log** (some deliveries label it Local/System Log). Export Event first, then select System, refresh and export again. Label files before/after maintenance and record the time zone. Program states in the historical native capture are not this unit’ s update result.

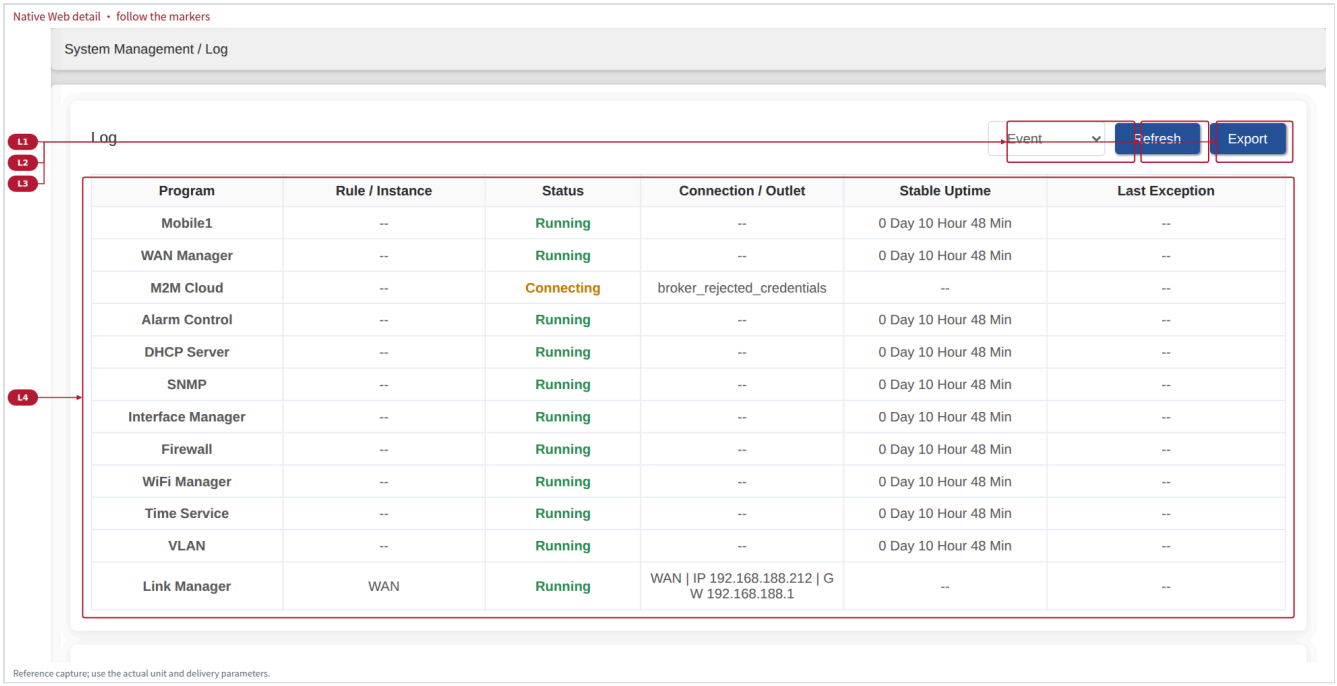


Figure 03 | Log type, refresh, export and runtime state; L1–L4 map to the table.

Marker	Action now	Expected result
L1	Event shows program state/events. Select System for lower-level update errors.	The selected source matches the export; available columns vary by delivery.
L2	Refresh and capture the period around the fault.	A current observation rather than a cached pre-maintenance page.
L3	Export to the customer PC. Current reference names: event_log.txt / system_log.txt.	Nonempty file with original text and time record; do not clear logs.
L4	Inspect state, stable uptime and last exception; search System logs for firmware/upload terms.	Running alone does not prove business operation. Interpret raw evidence at the corresponding step.

Problem at this point	Diagnosis and remedy
Empty export or missing incident period	Check selected type, refresh time, clock and time zone. Expand the period. /var/log and /tmp can rotate or disappear on reboot; an empty file does not prove no failure occurred.
Log page fails but other pages work	Record page/HTTP evidence and save version/state elsewhere. Have support extract logs when SSH is unavailable; do not independently enable root.
Rebooted before recording the business failure	Save remaining logs and state that a reboot occurred; supply the earlier export. Capture evidence before deciding to reboot next time.

3.2 What the files mean at each stage

File / access	What it helps establish	Limit
PC SYS package, release record and SHA256	Which original file was selected and whether its length/hash match the release.	Do not rename/edit a package to remove an error.
Exported system_log.txt / event_log.txt	Upload, validation, system failures and program state. The reference lower-level source is /var/log/messages.	Download before maintenance. Mask credentials before sharing; logs may contain accounts/IPs.
/proc/meminfo and /tmp capacity	MemAvailable and RAM-backed staging headroom for the image/runtime.	Authorized console only. Free eMMC space is not free RAM.
/config/startup.conf	Committed startup configuration used for Web configuration backup.	May contain live credentials. Do not publish its contents or overwrite it after text editing.
/tmp/.apid_up*; NAND /tmp/sysupgrade.bin; SPI /tmp/upgrade_cache/	Presence/length of upload staging files helps identify incomplete caching.	Paths may disappear during platform/failed-request cleanup. They are not backups; do not delete, manually copy or re-upload here.
/tmp/.status/upgrade.status; /tmp/.edgelor-sysupgrade-writing; /tmp/.edgelor-upgrade-reboot-pending	Support correlates these with logs, processes and time to identify the maintenance stage.	Presence does not prove active writing; absence does not prove no write occurred. Never edit/delete markers to release a busy state.

3.3 Read-only collection by an authorized engineer

Customers without delivered SSH continue using Web exports. The read-only commands below are for an already authorized shell/debug console. Web admin is not root, and industrial RS485/RS232 is not the debug console. Support can substitute tools available on that build.

```
date -u
cat /proc/uptime
sed -n '1,10p' /proc/meminfo
df -k /tmp /config
cat /proc/mtd
tail -n 100 /var/log/messages
dmesg | tail -n 80
```

Record output and collection/incident times. Inspect MemAvailable, or have support assess older kernels without it; check /tmp and /config separately. /proc/uptime measures system uptime, unlike a program’ s stable-uptime column. Record missing-file/permission errors rather than creating files, installing tools or cleaning directories.

04 | Step C: make a recoverable backup

4.1 Export committed gateway settings

1. Reopen network/application settings and finish row/global saves. Record version and management route.
2. Open System Management > Config Management and use Backup Configuration only. Do not Import, Factory Reset or Reboot here.
3. Save the original downloaded format in the controlled project folder. Check nonzero length/SHA256 and record exact model, version, date and management address.

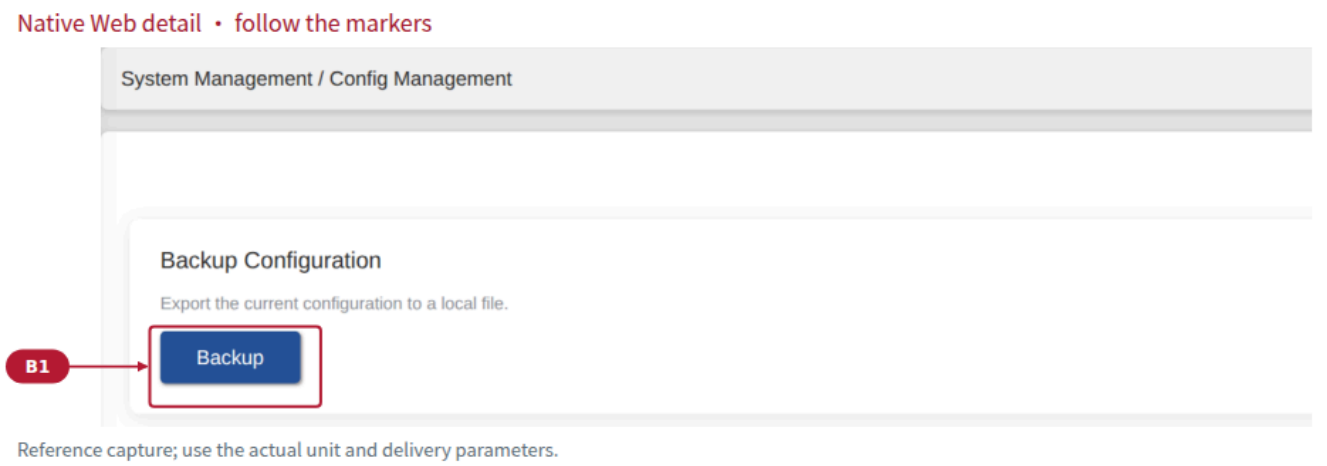


Figure 04 | Native Backup Configuration detail; use only B1 at this step.

Marker	Action	Completion evidence
B1	Click Backup and save the browser download. Do not convert it to ZIP/Word or a generic OpenWrt archive.	Nonempty file on the PC with model/version/date traceability.

Failure	File/behavior to inspect	Remedy and recheck
No download, or an HTML login page was saved	Download history, session and actual file type. HTML is not configuration.	Log in and export again. Record auth errors; do not count cached content as success.
Empty file or export error	HTTP message/system_log.txt; authorized checks of /config capacity and filesystem errors.	Retain evidence, fix authentication/storage and export again. Do not proceed with destructive work without a usable backup.
Recent point/address changes are missing	Reopen the relevant settings and check parent saves. /config/startup.conf is committed state.	Complete saves, export again and update the maintenance record.

4.2 Include application-specific data

Application used	Action before maintenance	If missing
PLC/Modbus, VPN and platform	Save point/project files, rules, certificate/credential recovery and one working result; not just an enabled screenshot.	Have the application owner complete the backup and record the gap.
Cameras/NVR	Back up device addresses/accounts, NVR connection settings and recording policy separately. Follow the customer recording plan.	Gateway configuration cannot restore camera settings or recordings.
Node-RED, if delivered	Export flow JSON; record nodes/runtime and credential/certificate recovery. Also export the application environment where that entry exists.	Flow JSON does not include every dependency/credential. It is not a complete application backup.
300L/900L local LNS, if used	The LNS owner backs up version-compatible databases, tenants/devices/sessions and required keys, plus Broker/region configuration. Use an approved DB backup procedure.	A live directory copy alone is not a consistent database backup. Gateway settings are not the LNS database.
MT7628 custom scripts/patches and separate files	Save original files/dependencies and record their location/recovery process.	The 15-second patch clear has broader impact. A future copy from the device is not a PC backup.

Prove restorability on a compatible same-model spare or in an agreed maintenance window using chapter 08 and real business checks. Importing into an active unit is not a harmless backup test; it changes settings and reboots.

05 | Step D: Web image selection and reset choice

5.1 Fill fields and submit once

After normal boot and backup, open **System Management > Firmware Upgrade**. Figure 05-A is a native YZW280 SPI reference; 14 MB is only that capture’ s value. Use this unit’ s medium/limit and release requirements, not another unit’ s screenshot.

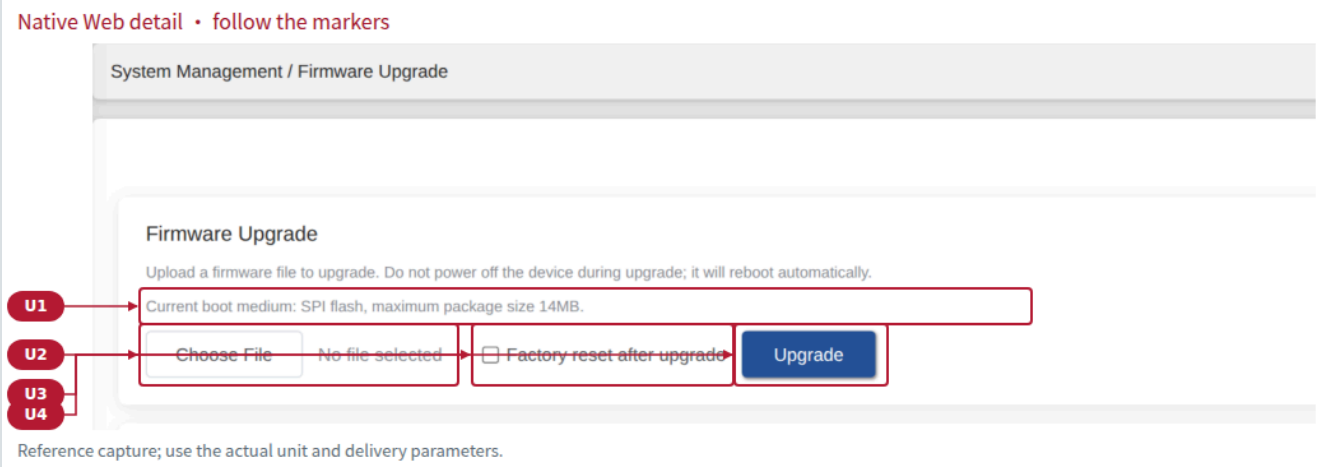


Figure 05-A | Native firmware upgrade detail; check U1–U4.

Marker	Action / value	Immediate check
U1	Read Current boot medium and maximum package size.	This is not free memory. Do not upload while the service is unavailable.
U2	Choose the approved SYS package and verify its disk filename.	Do not rename. Inspect the original file if the page truncates its name.
U3	Configuration changes: select. Program-only update with unchanged configuration: leave off.	Selecting means factory reset after upgrade, not preserving settings.
U4	After backup, wait-window and local recovery checks, click Upgrade and confirm once.	Services may pause from submission onward. Avoid repeated clicks/concurrent uploads.

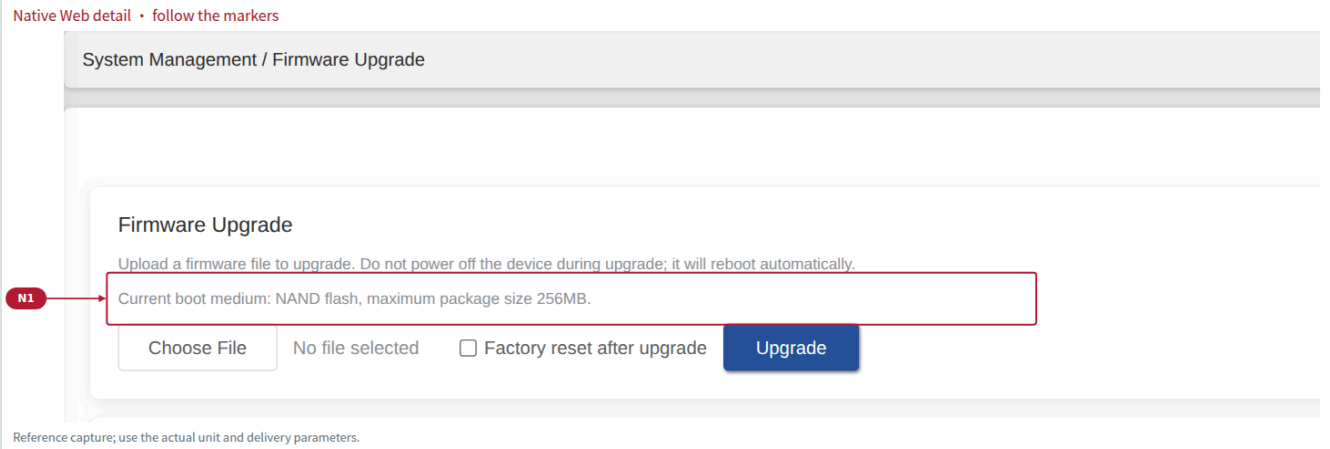


Figure 05-B | Native YZW001L NAND reference. N1 belongs to that reference unit, not NOR models.

Marker	How to use it	Check result
N1	Use the same selection/reset/submission sequence with the correct NAND image and actual unit limit.	eMMC capacity, NAND capacity, upload limit and free RAM are distinct.

5.2 Three outcomes of the reset decision

Update	Customer action	Required follow-up
Program-only fix, configuration unchanged	Leave Factory reset after upgrade off.	Recheck the original IP, VPN and applications. Preserving settings is not an absolute data-retention promise.
Configuration items/schema/defaults changed	Select Factory reset after upgrade.	Reconfigure for the new version. Reimport an old backup only after compatibility confirmation.
Configuration impact unknown	Obtain the release decision before submission.	A larger version/date is not the criterion. Engineering CLI is not a way around this choice.

Failure before submission	Diagnosis	Condition to continue
Upgrade service temporarily unavailable	Check session, homepage/other pages and actual version; export System logs.	Wait until the page reads authoritative medium/limit again. Do not guess upload limits.
Package exceeds boot-medium limit	Compare actual byte count, target model/medium and release record.	Obtain the correct package. Do not shrink, unpack or rename it to bypass checks.
Page uses an inverse label such as Keep settings	Match that delivery’ s actual meaning to the release requirement.	Record the intended choice, then submit once.

06 | Step E: distinguish upload, validation and writing

6.1 Immediately after submission: resource preparation

A normal early state may say resources/storage are being prepared while progress pauses. Collection, Node-RED or LNS runtimes may already be stopped. This does not prove Flash writing has started. Keep power/link stable and record the start time instead of resubmitting.

Behavior / keyword	Where and how to assess	Remedy and retest
Resource/cache failure; tmp_free / mem_available / ENOSPC	Save Web message/system_log.txt. Authorized checks: /proc/meminfo and df -k /tmp. The image and staging consume RAM-related resources.	Stop concurrent maintenance. Support assesses safe load reduction/stale resources. Handle only after ruling out active writing, then rerun preflight. Never rm -rf /tmp.
Large free eMMC but rejection continues	Check /tmp and MemAvailable, not only /flash/eMMC free capacity.	Correct the package/memory pressure; do not copy another image onto the unit.

Behavior / keyword	Where and how to assess	Remedy and retest
busy, single_flight or code=4004	Use logs/other authorized sessions to identify a running maintenance task.	Allow one task and wait for its known completion. Do not remove state/lock files.
Update rejected, then PLC/MQTT disappears	Preparation may already have stopped applications. Check Event state, application settings and last exception.	After confirming no write is active and maintenance exited, verify recovery; support restores services if required, then test fresh data.

6.2 File transfer: progress and cache are not write results

Upload percentage measures transmission from the PC. Normally the full transfer is followed by validation/update waiting. 100% alone does not prove acceptance or boot success. Do not refresh and resubmit while waiting.

Failure / behavior now	Files and diagnosis	Recheck after remedy
Progress stalls at a percentage	Record percentage/time. Check PC link/VPN. Search System logs for multipart_parse, cache_move or cache_verify.	Keep power. Determine whether the request is still running. Retry once only after explicit failure/no writing and link repair.
Upload/cache error, code=4007 or HTTP 413	4007 is generic request failure, not proof of bad Flash. Compare size with the log stage; authorized checks can inspect staging length and /tmp resources.	Fix the actual stage and reverify the file. Confirm any paused applications resumed.
401, expired session or login redirect	Save message/time; do not share token-bearing URLs/HAR. Open another window for current state if the stage is unknown.	Log in/retry only after confirming the earlier request is not writing. Avoid two uploads.
100% then 0/408/502/503/504 or reset connection	Network loss or transition to reboot are both possible. Check service outage/restart, eventual version and logs.	Keep power for the release wait window and reconnect using chapter 07. No single HTTP status proves success/failure.

6.3 Image and medium validation: the old OS may still run

Log/message example	Possible cause and field behavior	Action at this step
invalid_sys_name / invalid firmware / device mismatch	Name, content, model/medium or integrity mismatch. The old OS often remains accessible.	Check release record, original name/size/SHA256, exact model and medium. Obtain the matching package, not a bypass.
compiled medium / actual; cannot identify flash medium	Actual boot medium differs from the package/build or cannot be identified reliably.	Save update-page state, authorized /proc/mtd and logs. Supplier matches the storage variant; do not change partition flags.

Log/message example	Possible cause and field behavior	Action at this step
invalid FIT / hash check / truncated / size mismatch	Incomplete package or internal-format/image validation failure.	Recheck the original SHA256. If it matches, send the exact error/target record; do not edit the image body.
UBI unavailable / not attached / insufficient reusable_lebs	NAND layout, reusable blocks or attach state failed preflight; writing may not have begun.	Save dmesg/System logs for layout/storage-health assessment. Do not format UBI yourself.

These are search terms from the reviewed implementation, not messages every delivery must print. A generic invalid-file toast cannot establish the root cause. Correlate the incident stage/reason, file checks and actual unit state.

6.4 Writing/reboot has started: avoid escalation

Management may disconnect, services exit, link renegotiate and the unit restart. LED behavior differs by model; a blinking/dark LED cannot establish write completion. Keep power and avoid Reset, forced power cycling or state-marker changes.

Behavior now	Evidence and interpretation	Action
Upgrade did not start / restart not detected, e.g. -5001	The frontend did not observe its expected restart. This is not absolute write-state evidence. Check a new login, version, uptime and logs.	Old version plus confirmed no-write: address the rejection cause. Unknown stage: keep power and contact support instead of resending.
Out of memory / Killed process	Authorized dmesg, /var/log/messages and resource evidence may show a killed validator/application.	Identify write stage first. Resolve load/resources if no write occurred; interrupted writes/no boot use chapters 11–12.
Erase/write/I/O errors or later kernel panic	Save the complete boot/serial log, power conditions and image identity.	Do not try repeated resets or unrelated images. Support assesses recovery, storage or hardware failure.
Beyond the package wait window with no clear state	Retain start/last-activity times, LEDs/link and error. Check address/port using chapter 07 first.	Use loader recovery only after excluding access issues and confirming the OS cannot boot.

07 | Step F: reconnect and prove the update

7.1 Select the correct post-update address

1. Without factory reset, first use the recorded pre-update IP/protocol/port. With reset, use this unit’ s delivered/new-release management settings, not a universal assumed IP.
2. For DHCP, inspect the adapter address/subnet and renew through PC network settings if needed. For static addressing, use the matching subnet without an IP conflict.
3. Open the full URL in another browser window and check VPN/proxy routing. Log in and read the actual version/model instead of trusting the wait-page redirect.

Behavior after reboot	Check	Remedy / pass condition
Link up but old Web address fails	Reset choice, PC address, actual port, HTTP/HTTPS and TCP port.	Reconnect correctly. A working login/target version does not need rescue flashing.
Old page/version shown	Use a fresh/private session and reread the homepage. Verify device identity, not an office gateway.	If genuinely old, correlate chapter 06 logs for rejection/no-write; do not loop uploads.
Login page works but old password fails	Check factory reset/import and the corresponding delivered credentials.	Use credentials for that state. Wrong password is not loader damage.
Remote fails, local works	Uplink, VPN/platform, management rules and return route.	Verify remote access in chapters 09/14. Do not force-flash a locally healthy unit.
Repeated starts, uptime repeatedly resets	Stabilize supply and record cycles; authorized boot logs. A program uptime reset can be a service restart only.	Once full-system restart is proven, support assesses image/storage/boot failure. Do not infer it from LEDs alone.

7.2 Three checks complete the update

Confirm **the target version runs**, **configuration matches the reset/preserve decision**, and **fresh project traffic works** using chapter 14. Ping, login, one normal LED or old retained platform data alone is insufficient. After a reset, reconfigure for the new release rather than importing an incompatible old backup.

08 | Step G: restore settings or a compatible spare

8.1 Define the restore scope before import

Configuration restore changes settings, not the firmware version. Back up the currently usable state first. Confirm model, hardware/storage and configuration compatibility. A replacement also needs identity/MAC, certificates, platform registration and external access rules checked. Do not blindly reimport old settings after a configuration-changing update.

Risk / behavior	Evidence	Remedy
Backup from another platform/storage variant	Maintenance/compatibility record, not just the extension.	Use a compatible backup or reconfigure for the new release; do not force import.
Old LAN address/port/account in the backup	The backed-up management route; authorized review of sensitive settings.	Prepare the resulting PC subnet and credentials before importing.
Only settings exist, no application/project data	The independent-data inventory from chapter 04.	Complete the restore plan. Import cannot be assumed to recover recordings, Node-RED or the LNS database.

8.2 Choose the original backup and import once

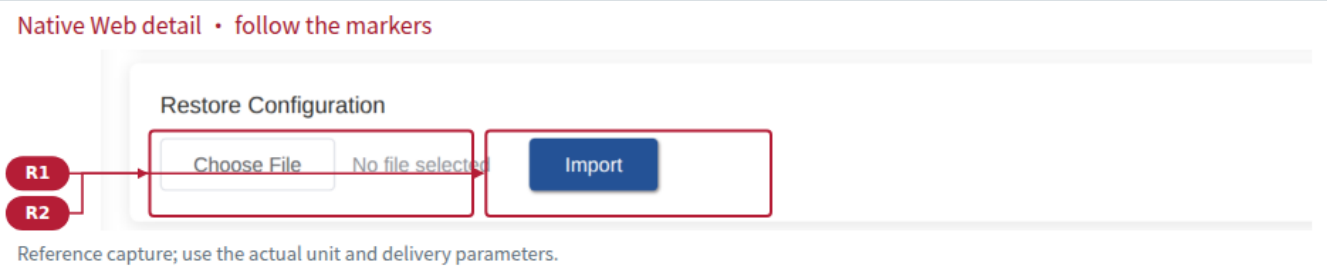


Figure 08 | Restore Configuration: R1 selects a settings backup; R2 imports it.

Marker	Action	Expected behavior
R1	Choose the verified original settings backup, not a SYS package.	The selected filename is shown; the object is configuration.
R2	Click Import, read the apply/reboot prompt and confirm once.	After validation the configuration applies and the unit reboots; disconnection can be expected.

Import behavior / log	Diagnosis and files	Remedy and retest
Invalid file; cli_format, wan, lan or resource error	Web detail, system_log.txt and backup provenance. Exclude HTML, firmware or a hand-edited damaged file.	Use the original compatible backup; support handles conversion. Do not publicly share credential-bearing contents.
Some features reset / reset_features	Record exact feature names; this is not proof of complete restoration.	Reconfigure each listed feature after login and test it. Do not force past protected-network rejection.
persistent_storage_unavailable or space/read-only error	Authorized /config and storage-log checks. A read-only squashfs root can be normal.	Support distinguishes normal root mounts from failed writable storage. Repair before retry; do not remount/delete configurations casually.
Connection lost after submission	Use the backed-up route and check reboot/configuration.	Do not repeat import because the old URL disconnected. Capture evidence when the stage is uncertain.

8.3 Worked example: the management address changes

Example: the current gateway/PC are 192.168.10.1/24 and 192.168.10.10. The backup uses 192.168.20.1/24 with HTTP port 80. After restore/reboot, set the maintenance adapter to 192.168.20.10/24 and open http://192.168.20.1. Use the actual backup values, not these example addresses.

```
Test-NetConnection -ComputerName '192.168.20.1' -Port 80
```

If TCP works but login fails, check the backed-up credentials/access policy. If TCP fails, check interface role, PC subnet, restored address/port and route. Consider factory reset in chapter 13 only after these checks leave no usable configuration-access route while the OS still runs.

09 | Scenario: update a remote site through VPN

9.1 Prepare for loss of access before updating

Example: K001 at a camera site and YZW350L at the office. The update still uses the device Web upload; VPN/authorized access only supplies the route. Updating does not remove mobile CGNAT or create direct public access. Do not expose public management just to upload an image.

1. Verify the target identity, login, backup download and a stable transfer over the existing remote route. Distinguish the field unit from the office unit.
2. Assign onsite staff, power/wiring, post-maintenance addressing and wait window. Deliver new network/APN/VPN settings onsite before any factory-reset update.
3. Maintain one device at a time, starting with a controlled-impact unit. Do not update both the site and its office access gateway simultaneously.
4. Use chapters 05–07. After remote disconnection, onsite staff reconnect and verify version, local network, uplink and VPN, then the office verifies fresh video/PLC requests.

Remote-stage behavior	What onsite/office staff inspect	Remedy and completion
VPN disappears; remote Web is lost	Onsite: local login/version. Office: tunnel, route and target address.	If local OS works, restore remote configuration. Do not reset merely for lost VPN.
Transfer interrupted; stage unknown	Onsite keeps power and records LEDs/link. Save matching times, logs and browser state.	Identify the original task before retrying. Do not reboot before confirming writing ended.
Tunnel online but camera/PLC unavailable	Verify the same target locally, then remote route/return path, port and permissions.	Repair the failed segment and confirm fresh office data. An online badge is insufficient.

10 | Conditional route: authorized engineering CLI

10.1 Establish why this is not a Web-failure shortcut

The reviewed source explicitly describes upgraded as a thin platform wrapper, not a supported customer update entry. Web authenticates, pauses relevant runtimes and checks memory/tmp before receiving a large image. Direct low-level invocation is not equivalent. Standard K001/YZW280 samples do not provide SSH; this chapter does not ask customers to enable root.

This chapter defines the engineering sequence/checkpoints, not an unapproved universal partition-write command. Execution requires an authorized entry, runtime stop/restore plan, resource criteria and one-time script supplied for the exact unit. Without them, use the supported Web route or service

recovery.

10.2 Four engineering steps and their checks

Engineering step	Required checks	Failure at this step and remedy
1 Read current state	Use chapter 03: version, /proc/mtd, MemAvailable, /tmp, applications and maintenance markers.	Stop for active maintenance, unidentified medium or incompatibility. Do not bypass busy/validation through CLI.
2 Prepare image and conditions	Approved integrity, one staging location, headroom, downtime and rollback plan. Avoid duplicate large RAM copies.	Transfer itself uses RAM. Resolve capacity first, not through a lower-level writer.
3 Execute the unit-approved script	An authorized engineer runs the maintenance-record command and retains complete output/result plus stage times.	ret=0 does not replace reboot/version/business checks. Keep power while the stage is unknown.
4 Restore and verify	Read version/settings and test local/remote applications using chapters 07/14; save logs.	Restore the affected runtime/dependency before considering another flash.

10.3 Two common tool/file mistakes

Misuse	Why it fails	Correct handling
Treating upgraded’ s second argument as factory reset	The reviewed wrapper accepts a file and reboot flag; SYS handling passes factory=0. It does not expose the Web reset choice.	For changed configuration use the supported reset-aware route, not a different reboot argument.
Sending .ent directly to generic sysupgrade/mtd	The product package has its own validation/wrapper plus medium/image/layout checks.	Use the approved product process. Do not force-write partitions or erase the loader.
Using MT7628 patch clearing to fix upgrade failure	It deletes extension content; it does not correct package compatibility.	Diagnose the failed stage. Clear extensions only under the exact approved engineering plan.

11 | Conditional route: Bootloader Web recovery

11.1 Confirm the actual loader entry

Use this only when the OS cannot boot and the unit’ s loader actually provides an independent recovery Web page. **Do not assume CFE on every model or reuse historical WAN/IP/button timing/app.lix/SYS instructions.** Current YZW280 maintenance scope does not establish CFE support from an old chapter.

Obtain a confirmed unit-specific recovery sheet before entry. Chapter 13 Reset timing applies after normal boot; it does not define power-on loader entry. If the loader/version is unconfirmed, preserve the observed state while the supplier identifies the appropriate recovery route.

Required recovery-sheet field	Provider / purpose
Model, hardware/storage, loader version and supported route	Supplier matches the exact unit and establishes loader Web, TFTP or production recovery.
Entry sequence and expected state	Specific power/button/console timing and identifiable result; no universal all-LEDs-on assumption.
Physical port, power and IP	Unit-specific recovery interface, PC address/mask, device address and complete URL.
Recovery file	Original name, length, SHA256, allowed target and data impact; confirm separately from the Web system package.
Wait/completion/failure criteria	Expected wait, completion log/reboot, post-recovery address and stop/return conditions.

11.2 Establish the recovery network and enter the loader

1. After support rules out an unknown active write and approves recovery, connect the specified port/power route. The normal Web LAN interface is not automatically the recovery port.
2. Set the maintenance adapter’ s IPv4 address/mask from the recovery sheet and avoid conflicting VPN/adapter routes. Use any gateway setting specified there; do not guess public DNS.
3. Use the exact power/button/console entry sequence. Open the sheet’ s URL and verify the actual loader/target. Select an image only after the real recovery page appears.

Entry behavior	Immediate diagnosis	Remedy / stop criterion
No Ethernet link	Power/PoE direction, specified port, cable and PC adapter; loader roles may differ.	Fix confirmed wiring before any transfer.
Ping works, loader page fails	Full HTTP/HTTPS URL/port, VPN/proxy and whether normal OS is running. Test TCP on the actual Web port.	Repeat only the confirmed entry once. No page means stop; ping is not recovery success.
Normal system login appears	The OS booted or recovery entry was not taken.	If login works, use normal Web update. Avoid repeated power/button attempts merely to force flash.
Confirmed entry gives no loader/console response	Save boot behavior/time and compare the sheet with actual loader version.	Support decides TFTP/production/hardware recovery. Do not guess addresses or hold buttons longer.

11.3 Select the approved object/image in the real loader page

1. Recheck length/SHA256 of the recovery-sheet image and select only the approved target. BOOT, factory/calibration and identity regions are not ordinary system targets.
2. Use that page’ s real selection/submission controls. Leave any unapproved target/format untouched.
3. Submit once, record the stage and keep power stable. Wait for completion, then boot as specified on the recovery sheet.
4. After normal boot, verify model, identity, medium and version before restoring compatible settings/application data using chapters 08/14.

Failure here	Evidence	Remedy
Loader rejects the file	Complete message, selected target, original image name/length/SHA256.	Reconfirm format/purpose. Do not strip headers, combine/rename images or switch targets to pass.
Transfer ended, no write completion/boot result	Page stage, console/write log. Upload/TFTP success proves arrival only.	Maintain power for the specified window. Do not resubmit/power off before support identifies the state.
Wrong identity/MAC/RF calibration or repeated write failures	Recovery log, label, version and controlled identity records.	Stop writes. Supplier assesses identity/calibration/storage and return repair. Do not copy another unit’ s factory data.

12 | Conditional route: TFTP and debug-console recovery

12.1 Identify the transfer direction first

TFTP transfers data; it does not choose a correct partition or guarantee boot. The debug console records startup and runs unit-approved loader steps; it is not industrial RS485/RS232. Obtain pinout, voltage, baud, terminal settings and grounding for the unit. Do not apply PC RS232 levels or external supply to unknown pins.

Recovery-sheet direction	PC preparation	Expected evidence
Loader client retrieves from PC	Start the approved TFTP server, bind the maintenance IP, place the exact file in its root and allow isolated transfer.	A read request from the unit, exact filename and matching byte count.
Unit provides a receive service; PC uploads	Confirm the unit is actually listening, then use the sheet’ s binary/octet client transfer to the specified target.	Device-side byte count/validation and subsequent write-stage evidence.
Console records logs; Web performs recovery	Use approved wiring/terminal settings and record startup to failure without write commands.	Text identifies whether execution reached the loader, kernel load or storage mount.

TFTP uses UDP. Test-NetConnection -Port 69 tests TCP, not TFTP readiness. Allow actual transfer/return traffic, not only a UDP 69 rule. TFTP provides no general user authentication; restrict recovery to the isolated maintenance network. See RFC 1350.

12.2 Record transfer, validation, writing and boot separately

Stage	Specific evidence	Failure and remedy
1 Prepare transfer	Actual PC adapter IP, server binding/root, case-sensitive filename and SHA256; save TFTP logs.	No request: check loader mode, transfer direction/port/subnet before changing the image.
2 Complete transfer	Compare reported byte counts and validate the loaded image as the sheet requires.	File not found: root/name. Timeout: link/firewall/return traffic. Integrity mismatch: obtain the original file again.
3 Approved write	Engineer runs only the unit-approved target/script and captures erase/write/verify output.	Stop if addresses/offsets/partitions are unconfirmed. Transfer is not writing; do not assemble generic flash commands.
4 Boot normally	Verify model/identity/version and management after the sheet’ s boot procedure.	Write errors, restart loops or failed storage detection need support; production tools/return repair may be required.

12.3 Diagnose an unreadable or silent console

Console behavior	Evidence	Remedy
No output	Actual debug connector, PC port/driver, RX/TX/ground and power; note whether output exists only early in boot.	Correct from the unit pinout. A silent industrial serial port is not proof of CPU failure.
Garbled/intermittent text	Unit-specific baud/data/parity/stop settings, voltage and grounding.	Match settings and record readable logs. Do not blindly change loader variables.
Only load/mount errors	Capture startup from power-on and identify the last successful stage.	Support matches the recovery target/image. Do not send only the final line.

13 | Step H: reboot, factory reset and the button

13.1 Choose the right operation while Web still works

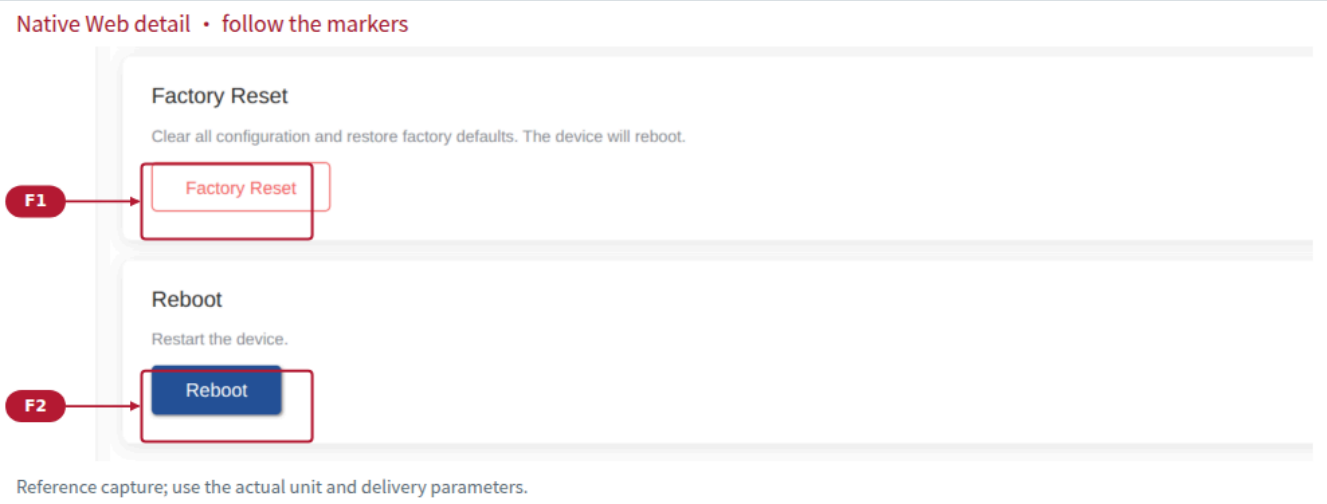


Figure 13 | Factory Reset and Reboot in Config Management; F1 and F2 are different.

Marker	Purpose / action	Expected result and caution now
F1	For required configuration clearing: back up, confirm the delivered default route, then Factory Reset once.	Settings are rebuilt; reconfigure afterward. This does not downgrade firmware.
F2	For restart only: choose Reboot and confirm.	The existing management route normally remains. Reboot is not a reset or a repair for a wrong image/power hardware.

13.2 Web lost but OS running: use the delivered Reset rule

These rules come from the current normal-system button scripts and require a matching delivery/working button. They are neither power-on loader entry nor completion-time guarantees. No button was tested on a device in this work. Record evidence/backups and rule out active firmware writing first.

Platform / hold then release	Action	Caution at this step
MT7628: under 5 s	Reboot.	Does not clear settings.
MT7628: at least 5 s, under 15 s	Factory-reset settings, then reboot.	Use the unit instructions for ordinary reset; avoid reaching 15 s.
MT7628: at least 15 s	Clear patches/extensions and related settings, then reboot.	Broader impact; use only under the explicit support plan, not as a more thorough restart.
MT7621 / MT7981: under 5 s	Reboot.	Interrupts applications and remote sessions.

Platform / hold then release	Action	Caution at this step
MT7621 / MT7981: at least 5 s	Reboot after successful factory processing.	Applications/identities have separate retention; this is not secure erasure.

Behavior after release	Evidence	Remedy and retest
No immediate reboot	Processing may still be active; record elapsed time and console/system output.	Wait for the unit window; do not repeatedly press. Do not assume settings cleared.
FACTORY RESET ABORTED / FAILED or PATCH RESET ABORTED	Authorized console/button-log collection: reference /patch/syslog on MT7628/MT7981; /config/patch/syslog on MT7621.	Quiescing, mounts or persistence may have failed. Preserve state for support; do not hold longer or delete markers.
Old address/password remains, or no access	Confirm a reset actually ran, the right unit is connected, and PC/default addressing is correct.	Reconnect using chapter 07 and reread settings, rather than trying patch clear.

13.3 Factory reset is not complete data erasure

Factory reset neither restores an older firmware nor guarantees removal of LNS tenants/sessions/keys, remote identities or every separate file. Use the supplier’ s unit-specific transfer/erasure procedure when needed. After reset, establish management credentials, then network, remote access and applications. Do not clone another unit’ s identity/calibration region.

14 | Step I: restore and verify the actual application

14.1 Restore network, remote access and field traffic in order

Verification step	How to verify	Failure and remedy at this step
1 Local management	Correct model/version, actual port login and configuration matching the reset choice.	Use chapters 07/08 for address/credential issues. An application-offline badge is not a management test.
2 Actual uplink	Real SIM/APN or Ethernet uplink, IP, DNS and routes; reach the project target.	Signal does not prove a mobile data session. Fix uplink before VPN/MQTT.
3 Remote route	Reach the gateway from the office, then the field target; check routes/return path and permissions.	Tunnel online/target down: test the target locally to isolate gateway versus device configuration.
4 Source to platform	Trace a fresh point, video stream or LoRaWAN application event.	Cached pages, old recordings or retained messages do not prove fresh operation. Preserve matching evidence at both ends.

14.2 PLC/Modbus and cameras: concrete post-maintenance checks

Application	Perform in this order	Handle failure at the failed step
PLC/Modbus collection	Reopen source/point/global enable → read a known read-only point → check address/type/scale/fresh time → inspect platform telemetry.	No local value: PLC, serial contention or network. Local value/no telemetry: Broker/topic/credentials/report enable. Do not reflash to fix parsing.
Remote PLC engineering	Verify local PLC communication, then office route/permission, then the original customer project.	Reachable IP/discovery failure: software interface, target CPU and broadcast needs. Gateway backup is not a PLC project backup.
Camera/NVR	Verify camera power/IP → fresh local video → remote route → reconnect NVR and check fresh display/recording policy.	Tunnel works/black or stale video: credentials, stream address, routes and NVR settings. Router updates cannot recover lost recordings.

14.3 MT7981 Node-RED and local LNS: independent data

Object	Files/UI and action	Remedy for failure
Node-RED service and flows	Check the delivered application service, then editor flows/nodes/credentials/deployment and fresh Debug messages.	Missing nodes: restore listed dependencies. Auth errors: restore credentials. Busy serial: identify competing collectors.
NAND ordinary-update retention	The reviewed implementation archives /overlay/node-red and /overlay/node-npm to /tmp/node-red-sysupgrade.tgz. factory=1 skips that archive.	Only specified application directories, not the entire overlay. Restore separate backups for other paths/versions/custom files. Do not assume retention.
NOR/eMMC separate storage	Match the actual package and mounts to data location, service and dependencies.	A surviving disk is not a working application. Fix mount/version/credentials separately; do not import the NAND rule.
300L/900L local LNS	Preserve current database/state → check service, region/sub-band and Gateway EUI → fresh frame/join → application up → Broker receipt.	Gateway frames/no up: identity/keys/session/region. up/no MQTT: integration/topic/authentication. Do not repeatedly reset the database.
Reconfigured control flows	Verify non-actuating inputs/readback, then reconnect under the approved customer control plan.	Check startup Inject and queued/retained commands after reboot. Deployment alone is not field feedback.

Database/session formats may not support cross-version rollback. Back up current post-update data and have the supplier define migration/restore compatibility before reverting. Do not downgrade and import an old database merely to recover an older UI.

15 | Scenario: downgrade, failed write or return repair

15.1 Confirm compatibility/reset policy before rollback

1. Record the current working version/settings and independent data; keep incident evidence.
2. Supplier confirms the old release for current hardware/medium, configuration and databases, supplying the original package/reset policy/fallback.
3. Use the approved update/recovery route. Configuration changes require factory reset, and backup compatibility is separate.
4. Verify the actual version/fresh application traffic using chapters 07/14, then export a new traceable backup.

Behavior during rollback/recovery	Action
Old package rejected	Preserve the validation reason and reconfirm compatibility. Do not use the loader/force flags as a version-check bypass.
Repeated write/verify or boot-storage failures	Confirm stable power and save complete logs. Stop writes for supplier assessment of Flash/loader/hardware or production repair.
Neither normal Web nor confirmed recovery works	Supply the recovery sheet, image checks and boot/wiring evidence; arrange return repair. Longer Reset holds cannot repair a damaged loader.

16 | Close maintenance: acceptance and handover

This chapter records results already verified at the operating steps; it is not a consolidated troubleshooting chapter. Return to the corresponding step for any failed item. Use the supplied worksheets and store passwords/private/root keys separately under access control.

Final check	Recorded pass evidence
Unit and version	Exact model/hardware/medium; actual target version and correct identity.
Configuration policy	Whether configuration changed/reset was selected and actual reconfiguration/compatible-restore outcome.
Management and network	Local management, real uplink and remote route pass separately; onsite confirmation.
Applications	Fresh PLC/video/LoRaWAN/Node-RED data/feedback for each used function; mark unused items N/A.
Archive	Before/after configuration, image name/length/SHA256, both logs, key times/time zone and outcome.

The maintenance worksheet records target, files, backups and stage results. The unit-specific recovery sheet lets the supplier confirm loader/ports/image/entry. Neither contains a firmware image, preset credentials or a universal loader-write command.