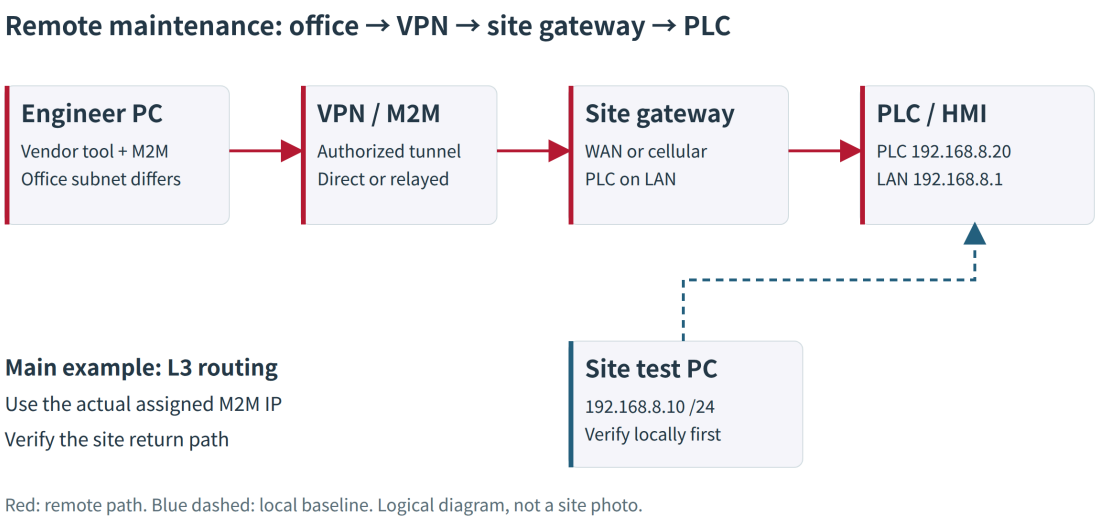
EDGELOR

PLC Data Acquisition and Remote Maintenance Two Platform Paths

Open the correct application and screen first. Then follow the platform and site task. Use the paginated contents and each step's entry path, expected screen and local checks.



Red: remote path. Blue dashed: local baseline. Logical diagram, not a site photo.

Local baseline → authorized remote access → one-point acquisition → receiver verification

English • V1.3 • 2026-11-05 Entry paths for all 29 steps; paginated contents, native screen guides and local fault checks.

Open contents • Find the application and screen

Contents • Tasks and page numbers

Select a chapter/task to jump. Numbers are the physical PDF pages; every footer returns to Contents or entry help.

The Word edition uses PAGEREF fields. After updating all fields in Word/WPS, its own pagination applies.

Chapter / operation	Page
0.1 Entry help: identify the application	4
0.2 Open the gateway Web UI	5
0.3 Find PLC sources, points, monitoring and reporting	6
0.4 Find Modbus devices, commands and global reporting	7
0.5 Open and navigate the M2M desktop client	8
0.6 Vendor-tool online, watch-table and diagnostic entries	9
0.7 Receiver, external collector and evidence locations	10
1 Choose the path that matches your site	11
1.1 Functions and paths in the two parts	12
1.2 Applicability and version records	13
1.3 Preparation and two address plans	14
1.4 Separate remote access from acquisition data	15
2 Shared preparation: verify the PLC locally	16
A1 Wire the PLC, gateway and site PC	16
A2 Select the site PC adapter and address	18
A3 Sign in to the Web UI and verify LAN	20
A4 Connect locally to the correct CPU first	22
A5 Read one known tag and save the baseline	24
3 Part I • MT7981: direct Web PLC acquisition	26
D1 Confirm the Web entry and match the PLC protocol	26
D1 PLC/HMI protocol catalogue • 1	28
D1 PLC/HMI protocol catalogue • 2	29
D1 PLC/HMI protocol catalogue • 3	30
D1 PLC/HMI protocol catalogue • 4	31
D1 Other device protocols • 1	32
P1 Create a PLC source with the exact protocol	33

Contents • Tasks and page numbers • continued

Chapter / operation	Page
P2 Add one read-only point and save each layer	35
P3 Compare monitored value, quality and freshness	37
P4 Configure the PLC-specific MQTT reporting rule	38
P5 Verify a new message at broker and platform	40
4 Part II • MT7628/MT7621: Modbus or an external collector	41
B1 Choose a task when there is no PLC Collect entry	41
S1 PLC supports Modbus TCP: save its device connection	43
S3 Serial acquisition: verify the physical port and ownership	45
S2 Verify one read-only Modbus register	47
B2 Enable and verify reporting in Modbus global settings	49
B3 Run proprietary-protocol acquisition on an external host	51
5 Shared remote maintenance: vendor tools on the PC	53
R1 Confirm the site gateway can reach the platform	53
R2 Configure gateway M2M Cloud and check both states	55
R3 Sign in on the PC and identify the site	57
R4 L3 routing: reach the PLC by its IP	59
R5 L2 bridge: when site discovery is needed	61
R6 Verify the PLC service and actual PC path	63
R7 Go online remotely and verify CPU and tag	65
S4 Remote COM maintenance: release the site port first	67
S5 Treat the HMI as a separate endpoint	69
6 Shared close, recovery and configuration records	70
N1 Close the session in order and retain production acquisition	70
N2 Recover fresh data along the actual path after an outage	71
N3 Export configuration and retain recoverable evidence	73
7 Scenario acceptance and handover	75
7.1 Evidence locations	76
References and revision notes	77

0.1 Entry help: identify the application

First identify the computer and application. The gateway management address, PLC address, M2M endpoint and MQTT broker are different targets; gateway Web and client credentials are also separate.

Task	Open here	Guide entry
Gateway/acquisition setup	PC browser at the current gateway management address.	0.2 Web; 0.3 PLC; 0.4 Modbus.
M2M route/bridge/COM	Launch the delivered Remote Device Manager/M2M desktop client on the engineer Windows PC.	0.5 client; R1–R7/S4.
PLC online/tag read	PLC vendor engineering software; TIA is a Siemens example, not an application inside the gateway.	0.6 vendor tools; A4/A5/R7.
Receiver/external collector	Project MQTT client, platform URL or external collector application.	0.7 receiver; P5/B2/B3.
IP/routes/service tests	Windows ncpa.cpl and PowerShell, not a Web configuration field.	A2/R6; substitute actual values.

0.2 Open the gateway Web UI

> Use the site PC connected to the gateway LAN. Initial Web access does not require M2M or a search inside PLC programming software.

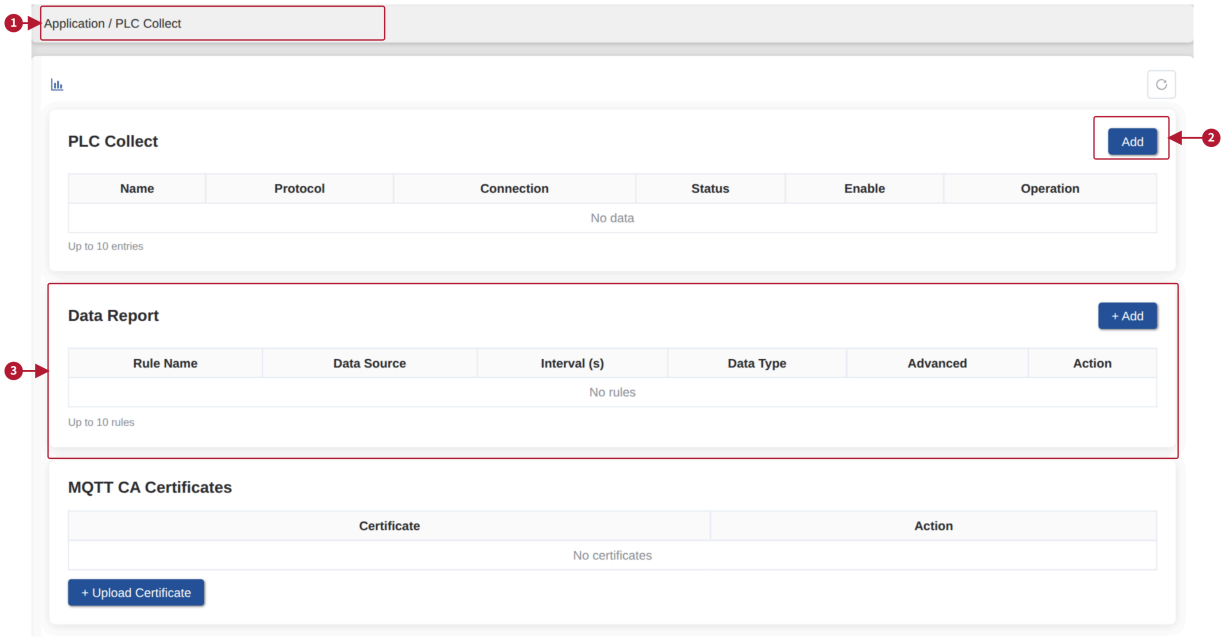
1. Connect the LAN with A1 and establish A2 management access. Obtain the current address from the label, delivery record or administrator; do not reset merely because it is unknown.
2. Launch a browser and enter the current management address in its address bar. http://192.168.8.1 is an isolated example, not a universal factory address; use the delivered HTTPS/port if applicable.
3. Use the delivered Web identity on the gateway sign-in page. After sign-in, expand the left menu and follow the table. For access failure inspect A2, management port and certificate/session before changing PLC points.

Left menu path	Expected screen	Task
Network Settings → LAN	LAN IP/mask and runtime state.	A3
Application → PLC Collect (MT7981)	Source list and its separate lower Data Report section.	D1/P1—P4
Application → Modbus Collect	Global settings and device/command management, not a proprietary PLC driver.	S1/S3/S2/B2
Application → M2M Cloud	Gateway-side remote-access settings.	R2
System Management → Log / Config Management	View/export logs; back up settings.	Local checks / N3

> If a menu is absent, check the platform first. MT7628/MT7621 uses B1 rather than a PLC Collect entry. For another missing expected entry, verify delivery/account/version instead of guessing a hidden URL.

0.3 Find PLC sources, points, monitoring and reporting

Complete 0.2, expand Application and select PLC Collect. The native parent page separates source connections above from reporting below. Empty lists illustrate navigation, not a field result.



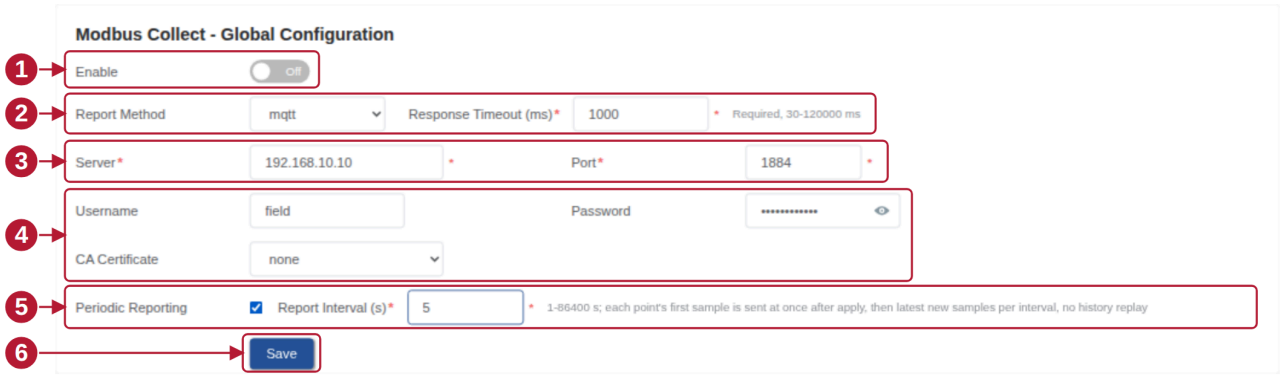
1 confirm PLC Collect; 2 upper Add creates a source; 3 lower Data Report creates a reporting rule.

Window required	From the parent page
D1/P1	Upper PLC Collect section → Add; Edit the existing PLC_A when present.
P2	PLC_A Operation column → Points → Add Point, not merely its name.
P3	PLC_A Operation column → Monitor opens Point Monitor.
P4	Close the dialog → scroll to Data Report → + Add → Advanced.

0.4 Find Modbus devices, commands and global reporting

MT7628/MT7621 does not use the PLC Collect page. In gateway Web open Application > Modbus Collect. TCP and RTU are alternative device paths, not mandatory duplicate connections.

MQTT reporting | Complete steps 1 to 6



Native interface with separate operation markers. Match numbers to the table below.

Native Modbus global example for B2, not PLC Data Report. 1 enable; 2 transport/timeout; 3 server/port; 4 identity/CA; 5 seconds; 6 Save.

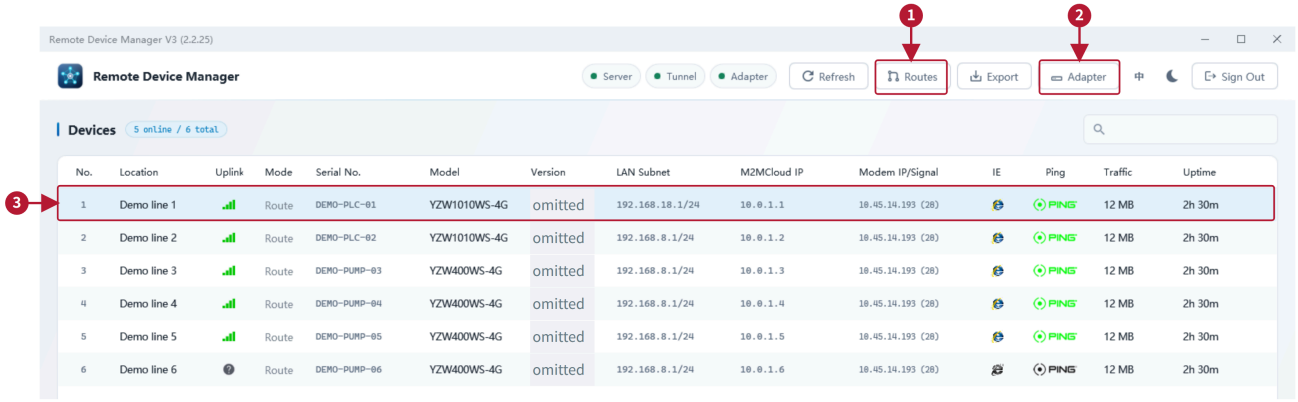
Task	Open and return
S1	Device list → Add Device → TCP; use the PLC service IP/port.
S3	Device list → Add Device → RTU; select the real gateway Serial/line settings.
S2	Inside the selected TCP/RTU device → Add Command; save it and return to Save Device.
B2	Return to the upper global settings; save, then verify messages at the actual receiver.

> Save command → device → global. PLC DB addressing is not Modbus register addressing; MC/S7 requires its own driver or an actual mapped Modbus service.

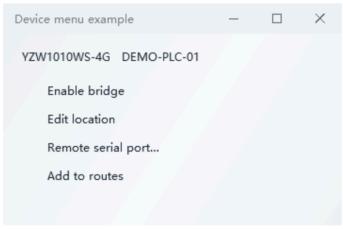
0.5 Open and navigate the M2M desktop client

This is a separate Windows program on the engineer PC. Install the delivered package, then use its Start-menu/desktop shortcut for Remote Device Manager/M2M. The installed name follows delivery; its Routes/Adapter toolbar is not inside gateway Web.

> Use the project platform/service port and client identity. After sign-in the device list appears. These are not the gateway management endpoint or Web administrator credentials. The figures are offline examples from the supplied V3 guide.



Client: 1 Routes; 2 Adapter; 3 target row. Version values omitted for publication; native image retained.



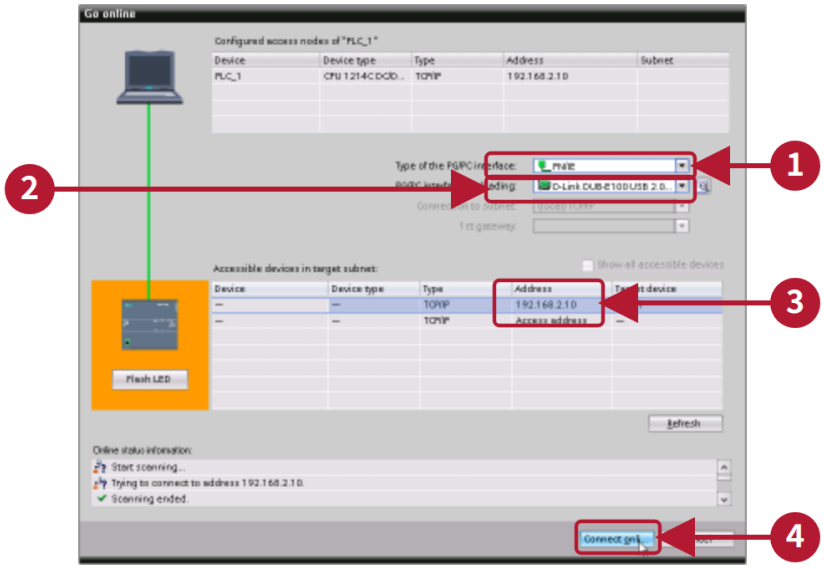
Right-click the target online device row for Enable bridge, Remote serial port and Add to routes; this is not a Web sidebar.

Task	Click here
R4	Right-click target → Add to routes; top Routes opens route management.
R5	Right-click target → Enable bridge; top Adapter opens Adapter Addresses.
S4	Right-click target → Remote serial port…; use its ready public COM in the vendor tool.

> Select R4 or R5 as planned. With an existing independent VPN, follow its supplied setup and continue at R6/R7; no extra M2M client is required, and M2M controls are not a universal VPN UI.

0.6 Vendor-tool online, watch-table and diagnostic entries

Open the compatible PLC project in its vendor tool. In the TIA example, use Project view, select the target PLC and choose Extended go online from Online. This identifies the starting application and menu.



Native TIA reference: open through the menu above, then select 1 interface type, 2 actual adapter and 3 target address; identify the CPU before 4 Go online. Factory addresses differ from this guide.

Task	Project tree/menu
A4/R7	Target PLC → Online → Extended go online; verify remote interface/IP when off site.
A5/R7	Target PLC → Watch and force tables → existing table or Add new watch table; monitor only.
CPU identity/diagnostics	Target PLC → Online & diagnostics; its view contains Diagnostics buffer.
S5	For an HMI use its own vendor tool/project; do not impose TIA menus on another brand.

> Observe an owner-approved safe point only: no modification, forcing or project download. Record real application/menu names for other versions/vendors; the Siemens example is not an all-CPU test.

0.7 Receiver, external collector and evidence locations

The receiver is not inside the PLC source dialog. Obtain the real application/version/launch method, platform URL, broker contract and reception page from the project administrator; do not invent a universal platform menu.

Task	Entry and required evidence
P5/B2	Start the existing MQTT subscriber → open the project broker connection → subscribe to the complete topic → inspect fresh receive time and raw payload. Obtain a platform receiver-log URL/menu from its administrator.
B3	On the assigned always-on host, start the real collector. Its driver/map/service/output screens belong to that application, not gateway Web.
Evidence files	Command TXT files use the current working folder; locate backups via browser Downloads; create the A/P/R screenshots/CSV records yourself.

UI_Entry_Index.csv lists all 29 entries and leaves fields for project addresses, application/version and actual menu names; do not enter passwords. Verify configuration, fresh point reads and received messages separately.

1 Choose the path that matches your site

This guide has two parts. MT7981 uses the PLC Collect entry and protocol tables in Part I. MT7628/MT7621 chooses Modbus, remote tools or external acquisition in Part II. Wiring, local checks and recovery are shared. Each step has expected behavior, precautions and immediately adjacent fault checks. Before acting, read the entire step and its same-code checks page, including precautions.

Customer scenario	Site need	Read in this order	Result
Part I: MT7981 with PLC Collect	The gateway reads a supported PLC driver and continuously reports to the customer platform.	A1–A5 → D1 and protocol tables → P1–P5 → N2/N3	A known point is correct at the gateway; matching fresh data reaches the platform.
Part II: MT7628/MT7621 without PLC Collect	The PLC exposes Modbus; the gateway polls and reports locally.	A1–A5 → B1 → S1/S3 → S2 → B2 → N2/N3	A known mapped register is correct and fresh messages arrive on the Modbus topic.
Part II: proprietary protocol or engineering	No Modbus service is available, or an engineer must go online with a PLC/HMI.	A1–A5 → B1 → R1–R7; S4 for serial; B3 for continuous acquisition	The PC tool verifies the correct CPU; an external application owns continuous polling.
Shared: an existing independent VPN	An approved OpenVPN/WireGuard or other tunnel is already working.	A1–A5 → R6 → R7 → N1/N2; no extra M2M installation is required.	Correct path/CPU and a fresh known-point read; verify discovery separately.

Jump to a named task: A1 Wire the PLC, gateway and site PC • A2 Select the site PC adapter and address • A3 Sign in to the Web UI and verify LAN • A4 Connect locally to the correct CPU first • A5 Read one known tag and save the baseline • D1 Confirm the Web entry and match the PLC protocol • P1 Create a PLC source with the exact protocol • P2 Add one read-only point and save each layer • P3 Compare monitored value, quality and freshness • P4 Configure the PLC-specific MQTT reporting rule • P5 Verify a new message at broker and platform • B1 Choose a task when there is no PLC Collect entry • S1 PLC supports Modbus TCP: save its device connection • S3 Serial acquisition: verify the physical port and ownership • S2 Verify one read-only Modbus register • B2 Enable and verify reporting in Modbus global settings • B3 Run proprietary-protocol acquisition on an external host • R1 Confirm the site gateway can reach the platform • R2 Configure gateway M2M Cloud and check both states • R3 Sign in on the PC and identify the site • R4 L3 routing: reach the PLC by its IP • R5 L2 bridge: when site discovery is needed • R6 Verify the PLC service and actual PC path • R7 Go online remotely and verify CPU and tag • S4 Remote COM maintenance: release the site port first • S5 Treat the HMI as a separate endpoint • N1 Close the session in order and retain production acquisition • N2 Recover fresh data along the actual path after an outage • N3 Export configuration and retain recoverable evidence

The contents includes task names, physical page numbers and links; use the footer to return to Contents or entry help. A/D/P/B/S/R/N are step codes, not menu labels or UI values. Read fault checks with each step.

1.1 Functions and paths in the two parts

Two parts: identify where the PLC driver runs

Part I • MT7981 Web PLC Collect

PLC → gateway driver → MQTT → customer platform
D1 verifies entry/driver; P1–P5 verifies connection, point, read and receiver

Part II • MT7628 / MT7621 without PLC Collect

A • PLC provides Modbus

Gateway polls TCP/RTU
Web: Modbus Collect
S1/S3 → S2 → B2 reports

B • Remote maintenance

VPN → vendor tool on PC
Verify CPU and one tag
R1–R7; S4 for serial

C • Continuous acquisition

IPC/server runs driver
Gateway provides the path
B3; host/service stays on

Shared A1–A5: identify the CPU locally and read the same known point correctly.

Shared N1–N3: retest fresh data at the actual collector, access path and receiver.

Protocol handling needs the matching driver. VPN, DTU and remote COM provide transport.

Choose the platform and task, then follow its steps. The diagram identifies the driver host, gateway path and continuous-operation owner.

Part I: direct MT7981 Web acquisition, D1/P1–P5. Part II: MT7628/MT7621 has no such entry; use S/B2 for Modbus, R/S4 for remote vendor tools or B3 for continuous proprietary-protocol acquisition. A preparation and N recovery are shared. MT7981 remote maintenance also uses R.

1.2 Applicability and version records

Platform	Model examples in this guide	Applicability
MT7628	YZW300X, YZW350L, YZW400, YZWK001, YZW1010	No dedicated PLC Collect entry. Use Part II for Modbus TCP/RTU or remote tools through M2M/VPN.
MT7621	YZW280, YZW380, YZW800L	No dedicated PLC Collect entry. Use Part II for Modbus TCP/RTU; match serial hardware to the delivered model.
MT7981	YZW001L, YZW300L, YZW800, YZW900, YZW900L, YZW1000	Part I: Application > PLC Collect. Check entry/driver at D1; YZW900 has no physical serial port. Shared remote access in Part II also applies.

UI figures come from current model manuals and acquisition guides; the supplied M2MCloud V3/2.2.25 figures are native manual examples. All 64 entries were checked against the MT7981 catalogue, network/serial metadata and driver branches, including PLC, HMI and instrument entries. This is not an all-CPU tested matrix or evidence of those drivers on other platforms. Record actual versions, maps and results; document V1.3 is not firmware.

> Names such as A1_ and R4_ are suggested names for records you create, not existing fixed device paths. Use the actual export from System Management > Log. If the client log location is not confirmed, save its error screen; do not guess an AppData or Linux path.

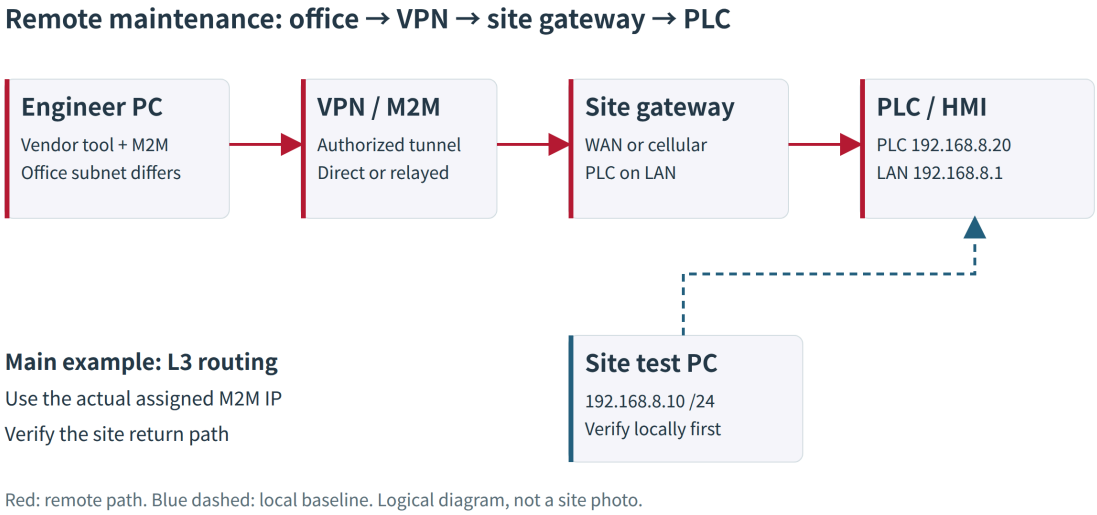
1.3 Preparation and two address plans

Prepare	Actual information to obtain
Gateway and tools	Exact model/firmware, current management address, matching supply/antennas/SIM, Ethernet cables and browser.
PLC and project	CPU order number/name/firmware, compatible tool and project, IP/mask/return path, and a known read-only point map.
Remote maintenance	Platform endpoint/service port, matching Windows client, account, device permission and an L2 or L3 plan.
Continuous reporting	Broker host/port/TLS and CA, MQTT identity/topic permissions and the data mapping contract.

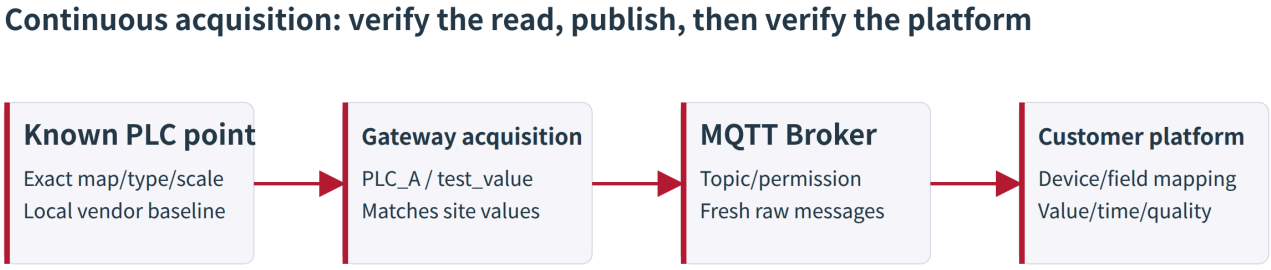
Role	Main L3 example	Separate L2 example
Site subnet/mask	192.168.8.0/24; 255.255.255.0	192.168.18.0/24; 255.255.255.0
Gateway LAN / PLC	192.168.8.1 / 192.168.8.20	192.168.18.1 / 192.168.18.20
Site PC	192.168.8.10; physical Ethernet adapter	192.168.18.10; physical Ethernet adapter
Remote PC path	Route target 192.168.8.0; next hop is the actual gateway M2M IP, e.g. 10.0.1.9.	The client adds a site address, e.g. 192.168.18.240; it must be unused.
PLC return path	Often via 192.168.8.1 when this device routes the return; confirm existing gateway/NAT arrangements.	Same-subnet access does not require changing the existing PLC default gateway.

> Examples are not factory defaults; retain the production plan. Verify one local point first, and skip unnecessary remote-maintenance steps for acquisition-only work.

1.4 Separate remote access from acquisition data



Remote path: PLC on LAN; WAN/cellular for uplink; blue dashed line is the local baseline.



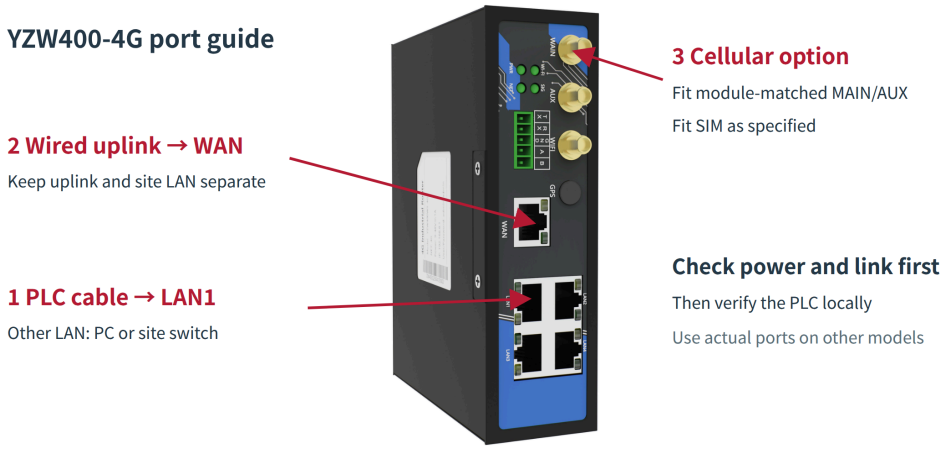
Acquisition path: known site point → gateway monitoring → fresh raw message → customer platform parsing.

2 Shared preparation: verify the PLC locally

A1 Wire the PLC, gateway and site PC

Use case: First installation, or a remote fault requires help at the cabinet.

Application: Site equipment and terminal references
Open: Exact model power/terminal drawing → physical labels, LAN and PLC ports
Check wiring and physical links; this step has no software dialog.
Need help opening it? Return to the application entry guide



A1 Port guide: 1 PLC to LAN1; 2 wired uplink to WAN; 3 cellular antennas. Original product image; follow each model's labels.

Action and save

1. Power each device with its specified supply. Check this model's power/run indication and the PLC state.
2. Connect the PLC to the LAN side. The YZW400-4G example uses LAN1. Attach the site PC to another LAN port or the same switch. Use WAN for a wired uplink, or fit the correct SIM/antennas for cellular.
3. Record ports, switch/VLAN and endpoint IPs. Retain the previously working wiring plan.

Expected behavior / proceed when

Power indications match the model manual and the connected Ethernet ends show a physical link. A2–A5 must still prove the application works.

Continue this step on the immediately following pages with the same code. Complete all its actions/checks before the next step.

A1 Wire the PLC, gateway and site PC

Step checks (following the action)

Take care at this step

Do not copy port positions across models; K001 has one LAN port. A link light is not protocol success. This figure illustrates remote networking, not a dedicated PLC application on YZW400.

Return/proceed: After wiring, continue to A2.

If this step fails

Observed symptom / behavior	Where / which file	Checks and condition to continue
Gateway dark or restarting	Supply label, model specification and A1_wiring.png.	Check polarity, terminal seating and the specified supply first. Measure against the delivered specification. Resume networking after stable operation; do not borrow another model's LED cadence.
No Ethernet link	PLC/gateway link indicators, switch ports and the A1 port plan.	Try a known-good cable; check LAN/WAN roles, disabled ports and VLAN. Compare with the site PC on that port. Continue to A2 after link returns.

Files and screens to check/save

Save A1_wiring.png and A1_network_plan.csv with addresses and ports.

A2 Select the site PC adapter and address

Use case: Wiring is complete, but the PC may not be on the PLC network.

Application: Site Windows PC

Open: Win+R → ncpa.cpl → connected Ethernet adapter → Properties → Internet Protocol Version 4 (TCP/IPv4) → Properties

The adapter IP/mask are visible; open Windows PowerShell separately for checks.

Need help opening it? Return to the application entry guide

Action and save

1. Run ipconfig /all and identify the connected physical Ethernet adapter by name.
2. Open ncpa.cpl with Win+R and edit that adapter's IPv4 properties. In the isolated example use 192.168.8.10 and 255.255.255.0; use 192.168.8.1 as gateway only when this is the intended exit.
3. Recheck ipconfig. Test gateway 192.168.8.1 and PLC 192.168.8.20 separately; substitute the existing site plan in production.

Run these read-only checks in Windows PowerShell. Replace the address/port first; TXT files are saved in the current evidence folder.

```
ipconfig /all > A2_ipconfig.txt
route print -4 > A2_routes.txt
ping 192.168.8.20
```

Expected behavior / proceed when

The intended adapter has its planned address, not 169.254.x.x, and can reach the gateway. Judge PLC ICMP responses separately from the application port.

Continue this step on the immediately following pages with the same code. Complete all its actions/checks before the next step.

A2 Select the site PC adapter and address

> Step checks (following the action)

Take care at this step

> Record the original static/DHCP setting first. Do not change the production PLC to fit the example or duplicate its IP.

Return/proceed: Continue to A3 after confirming adapter/address.

If this step fails

Observed symptom / behavior	Where / which file	Checks and condition to continue
Gateway reachable, PLC not reachable	A2_ipconfig.txt, the A1 plan and the PLC project IP.	Verify PLC address, power, mask and VLAN on site. Compare from a same-subnet PC. If ICMP is blocked, test the confirmed service and vendor tool.
Intermittent access or the wrong device	Address allocation, A2_routes.txt and both device identities.	Check duplicate IPs and overlapping local/virtual subnets. Keep one known test path. Resolve the conflict with the administrator and repeat A2; do not reset the PLC first.

Files and screens to check/save

Check adapter/IPv4/mask in A2_ipconfig.txt; use A2_routes.txt to detect a competing Wi-Fi or VM route.

A3 Sign in to the Web UI and verify LAN

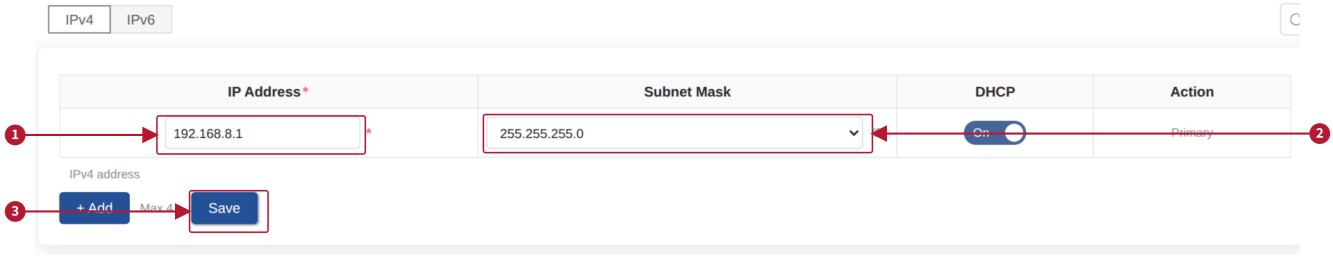
Use case: The PC is on site; confirm the gateway LAN used by the PLC.

Application: Site PC browser, not the M2M client

Open: Enter the current gateway management address and sign in → Network Settings → LAN

The LAN page shows IP, subnet mask and Save.

Need help opening it? Return to the application entry guide



A3 Native LAN page: 1 IP; 2 mask; 3 Save. The fields correspond to this step.

Action and save

1. Sign in at the current management address with delivered credentials. Open Network Settings > LAN and record existing values.
2. Check IP and mask at 1 and 2; the example is 192.168.8.1/24. Click Save at 3 only if a change is required, then reconnect at the new address.
3. Confirm PLC and PC still match the site subnet; renew a DHCP lease if the plan changed.

Expected behavior / proceed when

The UI can be reopened at the expected LAN address; runtime status matches the saved setting.

Continue this step on the immediately following pages with the same code. Complete all its actions/checks before the next step.

A3 Sign in to the Web UI and verify LAN

Step checks (following the action)

Take care at this step

A LAN change can interrupt remote access; arrange on-site recovery first. A DHCP switch does not mean a statically addressed PLC uses DHCP.

Return/proceed: After a LAN change, sign in at the new address.

If this step fails

Observed symptom / behavior	Where / which file	Checks and condition to continue
Web UI disappears after Save	Old/new addresses in A3 and A2_ipconfig.txt.	Try the saved new address. Check whether the PC remains on the old subnet or lease. Restore local access and read back LAN status before another change.
Web works but PLC remains unreachable	A1 port/VLAN plan, PLC project IP and gateway LAN status.	Compare the A2 result. Web access does not fix a wrong port, VLAN isolation or PLC address. Repair the local path first.

Files and screens to check/save

Save A3_lan.png and retain the pre-change backup/address plan when changed. Do not publish configuration backups.

A4 Connect locally to the correct CPU first

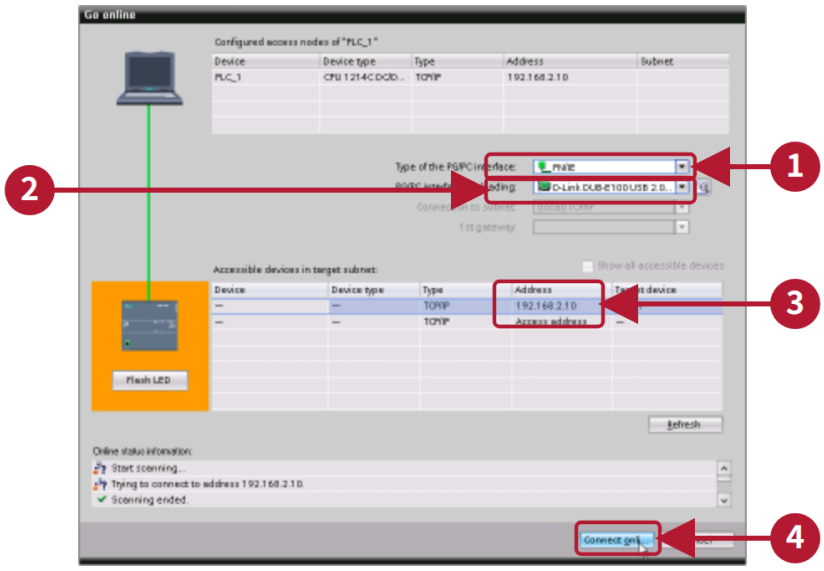
Use case: Create a repeatable local baseline for remote access and acquisition.

Application: Vendor engineering tool on the site PC; TIA example

Open: Open the confirmed project → Project view → select the PLC in the project tree → Online menu → Extended go online

The dialog provides PG/PC interface type, adapter and target address.

Need help opening it? Return to the application entry guide



A4 Original English vendor dialog. 1 interface type; 2 adapter; 3 target IP; 4 Go online. The factory IP differs from this guide.

Action and save

1. Open the project and vendor tool compatible with the site CPU/firmware. In the TIA example select the PLC and open Go online or Extended go online.
2. Select PN/IE at 1, the A2 physical Ethernet adapter at 2 and the actual PLC IP at 3, here 192.168.8.20. Identify the device before Go online at 4.
3. In Online & diagnostics compare CPU order number, name and firmware with the label and project, then record the result.

Expected behavior / proceed when

The tool establishes an online session and reads the correct CPU identity. Connecting does not itself require changing CPU mode or downloading a project.

Continue this step on the immediately following pages with the same code. Complete all its actions/checks before the next step.

A4 Connect locally to the correct CPU first

Step checks (following the action)

Take care at this step

The figure's IP, adapter and CPU are a factory example. Other PLCs do not automatically share S7 ports, addresses or project formats.

Return/proceed: Verify identity in the CPU online diagnostics before A5.

If this step fails

Observed symptom / behavior	Where / which file	Checks and condition to continue
Local device search is empty	PG/PC selection, A2_ipconfig.txt and A1 wiring.	Select the real Ethernet adapter, not PLCSIM/Wi-Fi. Check PLC IP/VLAN and use supported direct-IP access. Make local access work before adding VPN.
CPU identified but online access rejected	Full error, CPU identity, project/tool version; use the diagnostics buffer when accessible.	Check compatibility, access credentials and certificates. If model/site differs, go offline and verify the site; do not download an empty project or clear protection.

Files and screens to check/save

Save A4_cpu_identity.png, the original project/archive and tool version; retain the full error when it fails.

A5 Read one known tag and save the baseline

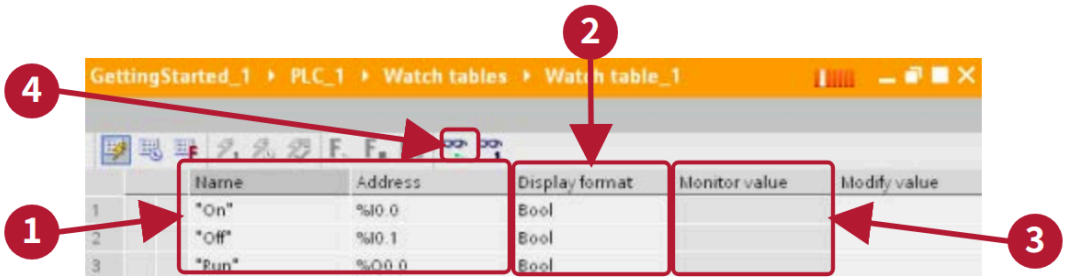
Use case: The site engineer can go online; define the same tag for all later comparisons.

Application: The same PLC engineering tool, not gateway monitoring

Open: TIA Project view → target PLC → Watch and force tables → an existing table, or Add new watch table

Name/address, display format and monitor value are visible; monitor only.

Need help opening it? Return to the application entry guide



A5 Watch table: 1 tag/address; 2 display format; 3 monitor value; 4 monitoring control. The figure is not evidence of a site reading.

Action and save

1. Choose a known read-only observation point from the confirmed map. Record its full address, type, length, scale/unit and current value.
2. Add it to the vendor watch table, select the matching format and start monitoring. Do not enter modify or force values.
3. Observe several updates and compare with natural site changes or a known state. Record time and time zone.

Expected behavior / proceed when

The correct CPU/address yields the expected type and value; current updates can be distinguished from stale display.

Continue this step on the immediately following pages with the same code. Complete all its actions/checks before the next step.

A5 Read one known tag and save the baseline

Step checks (following the action)

Take care at this step

A constant value is not automatically a fault. Check online state, update time and whether the tag should change; do not alter real outputs to manufacture a change. Have the PLC owner select a safe known internal state/test DB. Do not modify, force or probe unapproved direct peripheral addresses.

Return/proceed: Keep the baseline; use D1, B1 or R1 for the selected task.

If this step fails

Observed symptom / behavior	Where / which file	Checks and condition to continue
Blank, grey or non-updating value	Watch-table online state, CPU access rights and the A4 session.	Confirm monitoring and a valid session, then read permission. If a fresh read still fails, retain this point and CPU diagnostics before expanding the map.
Displayed value differs from the site	A5_point_map.csv, project symbolic/absolute addressing and display format.	Compare offset, bit/byte location, type and scale. Correct one same-time reference point before entering R or P.

Files and screens to check/save

Save A5_local_value.png and A5_point_map.csv with address/type/length/scale/value/time.

3 Part I • MT7981: direct Web PLC acquisition

D1 Confirm the Web entry and match the PLC protocol

Use case: An MT7981 gateway must acquire PLC data without an always-on engineering PC.

Application: Gateway Web UI; MT7981 PLC application path

Open: Sign in in the browser → Application → PLC Collect → Add in the upper PLC Collect section

Connection Configuration exposes name/brand/protocol; MT7628/MT7621 uses B1 instead.

Need help opening it? Return to the application entry guide

Action and save

1. Sign in and open Application > PLC Collect. Record model/firmware, page and protocol choices. Confirm the entry before P1.
2. Use the following tables to match brand, exact protocol and network/serial transport. S7/PPI, network MC/serial FX and Modbus TCP/RTU are distinct.
3. Obtain the PLC project/module settings and point map. Match service port or physical serial port, station, model and permissions; then create P1 and verify one read-only P2/P3 point.

Expected behavior / proceed when

The entry opens and the selected driver matches the real PLC and physical connection. Accept the combination only after the known-point read passes.

Continue this step on the immediately following pages with the same code. Complete all its actions/checks before the next step.

D1 Confirm the Web entry and match the PLC protocol

Step checks (following the action)

Take care at this step

Driver choices do not guarantee every CPU from a brand. Ethernet is not automatic protocol conversion; serial drivers still need the correct RS232/RS485 hardware. Reference figures are not live state.

Return/proceed: Match the driver, then perform P1 without duplicating a source.

If this step fails

Observed symptom / behavior	Where / which file	Checks and condition to continue
MT7981 entry or required driver is absent	Model/firmware, application menu, D1 captures and delivery record.	Check platform, account visibility and delivered version. Do not guess hidden URLs or install another platform package. Confirm the matching release with the supplier; use Part II R for maintenance or S/B2 for an enabled Modbus service.
Driver selectable, but save fails or connection times out	Full D1/P1 error, PLC project/module, both serial settings and gateway log.	Check transport first, then required parameters and the target service. If the vendor tool works locally, verify third-party access and driver/CPU support. Retest the same read-only point in P1/P3.

Files and screens to check/save

Save D1_menu.png, D1_protocol.png and the PLC communication setup/map. Record exact driver, CPU, versions and interface in Project_Parameters.csv.

D1 PLC/HMI protocol catalogue • 1

For Part I. Identifiers match the native choices. Match the actual PLC/module, service and point map; TCP/UDP mode follows the specific network driver.

The MT7981 catalogue has 64 entries: 39 network and 25 serial, including PLC/HMI and later instrument entries. S7 types include S200Smart, S200, S300, S400, S1200 and S1500; verify the actual CPU/firmware and access rights.

Brand/device	Native network choices	Native serial choices	Check when selecting
Siemens	siemensS7	siemensPPI	Match S7 CPU/access; verify PPI port/station.
Mitsubishi	MC-1E, MC-3E	MC-3C, FxLinks, FxSerial	Match MC frame/encoding/station; verify FX serial port.
Generic Modbus	ModbusTCP, ModbusRTUOverTCP, ModbusASCIIOverTCP	ModbusRTU, ModbusASCII	TCP differs from RTU-over-TCP; ASCII is not RTU.
Omron	Fins, HostLink Over TCP, CIP	HostLink	Match Fins TCP/UDP mode; CIP and HostLink are separate.
Inovance	InovanceTCP	InovanceSerial	Verify series/parameters; do not guess defaults.

At this step: this table belongs to MT7981 PLC Collect. For MT7628/MT7621 use Part II local Modbus TCP/RTU; run other drivers on the external collector or vendor-tool host. For a mismatch, use the local D1 checks.

D1 PLC/HMI protocol catalogue • 2

For Part I. Identifiers match the native choices. Match the actual PLC/module, service and point map; TCP/UDP mode follows the specific network driver.

Brand/device	Native network choices	Native serial choices	Check when selecting
Keyence	KeyenceMcNet, KvOld, NanoSerialOverTcp, SR2000SeriesTcp	NanoSerial, SR2000Serial	Match the actual KV/other series; SR2000 is a reader.
Delta	DeltaTcp	DeltaSerial	Verify the actual series, communication setup and one mapped read-only point.
Panasonic	PanasonicMcNet, PanasonicMewtocolOverTcp	PanasonicMewtocol	Verify the actual series, communication setup and one mapped read-only point.
XINJE	XinJEInternalNet, XinJETcpNet	XinJESerial	Verify the actual series, communication setup and one mapped read-only point.
Beckhoff	BeckhoffAdsNet	—	Verify target AMS parameters and PLC routes/access.

At this step: this table belongs to MT7981 PLC Collect. For MT7628/MT7621 use Part II local Modbus TCP/RTU; run other drivers on the external collector or vendor-tool host. For a mismatch, use the local D1 checks.

D1 PLC/HMI protocol catalogue • 3

For Part I. Identifiers match the native choices. Match the actual PLC/module, service and point map; TCP/UDP mode follows the specific network driver.

Brand/device	Native network choices	Native serial choices	Check when selecting
Rockwell/AB	AllenBradleyNet, AllenBradleyConnectedCipNet, AllenBradleySLCNet	AllenBradleyDF1Serial	Verify the actual series, communication setup and one mapped read-only point.
LS	LSFastEnet, LSCnetOverTcp	LSCnet, LSCpu	Verify the actual series, communication setup and one mapped read-only point.
MegMeet	MegMeetTcpNet, MegMeetSerialOverTcp	MegMeetSerial	Verify the actual series, communication setup and one mapped read-only point.
Yaskawa	MemobusTcpNet, MemobusUdpNet	—	Verify the actual series, communication setup and one mapped read-only point.
Fatek	FatekProgramOverTcp	FatekProgram	Verify the actual series, communication setup and one mapped read-only point.

At this step: this table belongs to MT7981 PLC Collect. For MT7628/MT7621 use Part II local Modbus TCP/RTU; run other drivers on the external collector or vendor-tool host. For a mismatch, use the local D1 checks.

D1 PLC/HMI protocol catalogue • 4

For Part I. Identifiers match the native choices. Match the actual PLC/module, service and point map; TCP/UDP mode follows the specific network driver.

Brand/device	Native network choices	Native serial choices	Check when selecting
Vigor	VigorSerialOverTcp	VigorSerial	Verify the actual series, communication setup and one mapped read-only point.
Fuji	FujiCommandSettingType, FujiSPBOverTcp, FujiSPHNet	FujiSPB	Verify the actual series, communication setup and one mapped read-only point.
Cimon HMI	CimonHmiProtocol	—	HMI driver; not all PLCs from this vendor.
Yokogawa	YokogawaLinkTcp	—	Verify the actual series, communication setup and one mapped read-only point.

At this step: this table belongs to MT7981 PLC Collect. For MT7628/MT7621 use Part II local Modbus TCP/RTU; run other drivers on the external collector or vendor-tool host. For a mismatch, use the local D1 checks.

D1 Other device protocols • 1

> For Part I. Identifiers match the native choices. Match the actual PLC/module, service and point map; TCP/UDP mode follows the specific network driver.

These instrument/industry entries share the application; they are listed separately from PLC compatibility.

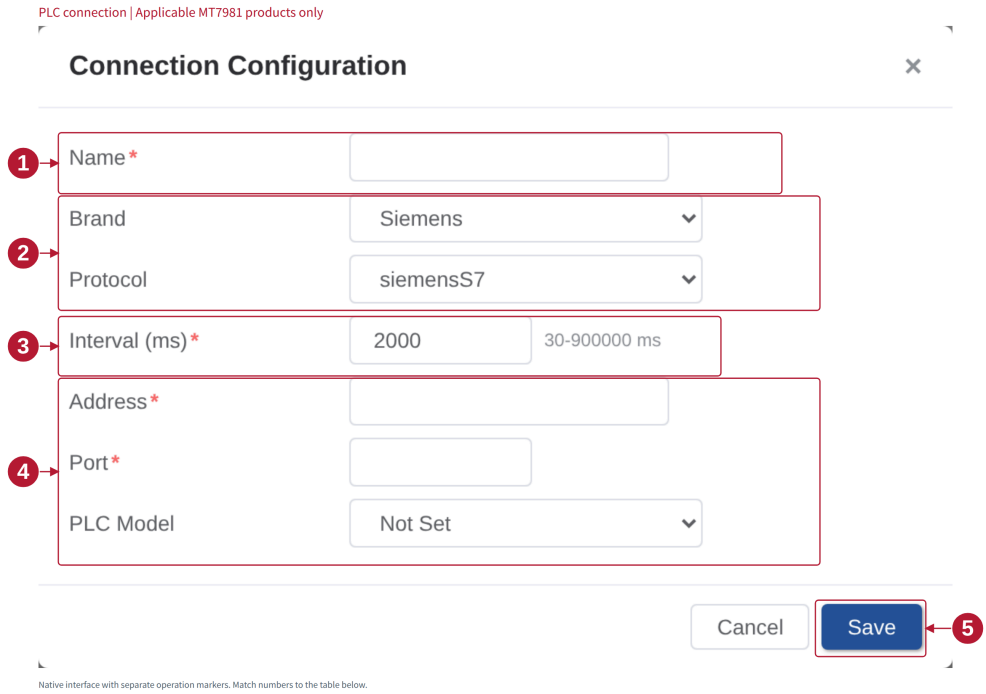
Brand/device	Native network choices	Native serial choices	Check when selecting
CJ/T188 meters	—	CJT188	Verify the actual series, communication setup and one mapped read-only point.
DL/T meters	DLT698TcpNet	DLT645, DLT698	Verify the actual series, communication setup and one mapped read-only point.
IEC104 devices	IEC104	—	Verify the actual series, communication setup and one mapped read-only point.
DTSU6606 meter	—	DTSU6606	Verify the actual series, communication setup and one mapped read-only point.
Temperature devices	TemperatureController OverTcp	TemperatureController	Verify the actual series, communication setup and one mapped read-only point.

> At this step: this table belongs to MT7981 PLC Collect. For MT7628/MT7621 use Part II local Modbus TCP/RTU; run other drivers on the external collector or vendor-tool host. For a mismatch, use the local D1 checks.

P1 Create a PLC source with the exact protocol

Use case: An MT7981 gateway with the delivered PLC application must read a PLC continuously; the engineering PC need not stay online.

Application: MT7981 gateway Web UI
Open: Application → PLC Collect → upper PLC Collect section → Add; use Edit for an existing PLC_A
Connection Configuration opens, not the lower reporting rule.
Need help opening it? Return to the application entry guide



P1 1 source name; 2 brand/protocol; 3 interval in ms; 4 address/port/model; 5 Save.

Action and save

1. Confirm the D1 entry/driver and A4/A5 CPU/point; open Application > PLC Collect > Add.
2. Set 1 Name to PLC_A, 2 exact brand/protocol for the CPU, 3 to 2000 ms as an example, and 4 to the actual PLC IP/protocol port/model parameters.
3. Save the connection at 5. Confirm PLC_A in the list before opening its points.

Expected behavior / proceed when

The source is saved and its parameters match the project. Point acquisition is not yet proven.

Continue this step on the immediately following pages with the same code. Complete all its actions/checks before the next step.

P1 Create a PLC source with the exact protocol

Step checks (following the action)

Take care at this step

The example PLC is 192.168.8.20; port 102 is only for the confirmed S7 example. Do not guess protocol ports, rack/slot or CPU defaults. If PLC Collect is absent, use S1/S2 or check delivery.

Return/proceed: After saving, return to the PLC_A row and open Points.

If this step fails

Observed symptom / behavior	Where / which file	Checks and condition to continue
PLC Collect is absent	Model, delivery list, current application menu and firmware record.	Check platform and delivered MT7981 configuration. Use delivered Modbus or verify the application/runtime with the supplier, not a generic package.
Save fails or all points fail to connect	P1 fields, PLC protocol/port/CPU project, application state and local log.	Check required fields and actual parameters, then the gateway's own LAN path and permission. PC access is not gateway-process permission. Record the time and retry one connection.

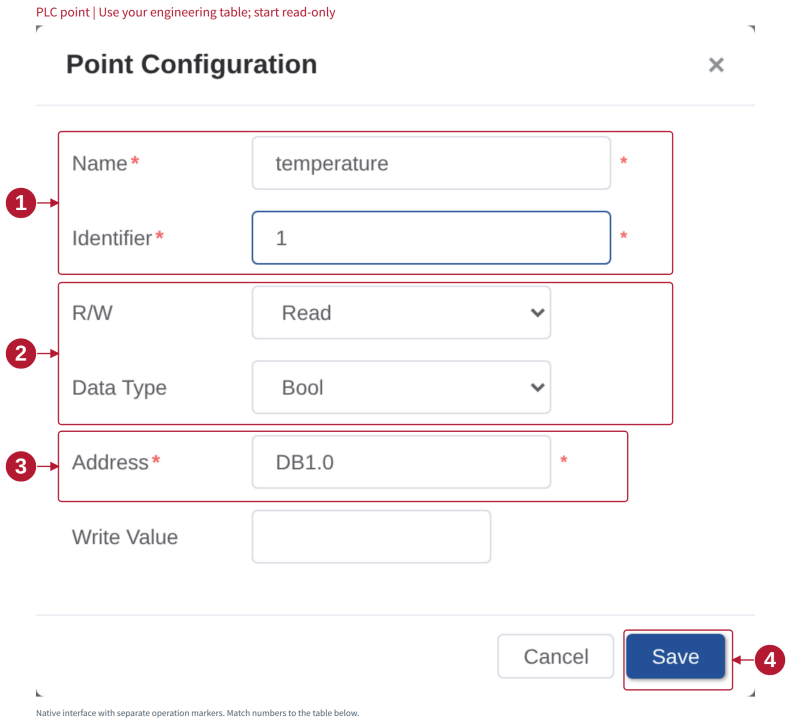
Files and screens to check/save

Save P1_connection.png and retain protocol, CPU/firmware, A5 map and connection parameters.

P2 Add one read-only point and save each layer

Use case: PLC_A exists; validate one point before importing a full map.

Application: MT7981 gateway Web UI
Open: Application → PLC Collect → Operation in the saved PLC_A row → Points → add a point
Open the source point table first, then its point form; verify PLC_A.
Need help opening it? Return to the application entry guide



P2 1 name/identifier; 2 Read and type; 3 full address; 4 Save. Read is selected for the first verification.

Action and save

1. Return to the PLC Collect list, use Points in the PLC_A Operation column, then add a point. Use test_value and identifier 1 if appropriate, for the same real A5 point.
2. At 2 select Read and the project type/length. At 3 enter the full driver-supported address. Leave write values and periodic writing unused.
3. Save the point at 4, close the point window and check connection enable state. Confirm point and connection saves separately.

Expected behavior / proceed when

The point is saved with the intended read mode/type. P3 must verify the real read.

Continue this step on the immediately following pages with the same code. Complete all its actions/checks before the next step.

P2 Add one read-only point and save each layer

> Step checks (following the action)

Take care at this step

> The figure's temperature / Bool / DB1.0 are existing native examples, not a universal temperature map. Identifier is an application point ID, not a PLC register or Modbus station.

Return/proceed: Save the point, check enable state, then use Monitor on the same row.

If this step fails

Observed symptom / behavior	Where / which file	Checks and condition to continue
Point save reports an address/type error	P2 screenshot, protocol point map/import template and project address.	Compare syntax and type/length exactly. Do not borrow a 40001 conversion or another PLC's symbols. Save one valid manual point before importing.
Point exists but acquisition does not run	Point save result, PLC_A enable/state and P1 connection.	Confirm the saved PLC_A, then point/connection saves, application and enable state. Use P3 to inspect actual behavior; do not duplicate the source.

Files and screens to check/save

Save P2_point.png and P2_point_map.csv with address/type/length/scale/access and revision.

P3 Compare monitored value, quality and freshness

Use case: The point is saved; distinguish a correct read from a connected source or stale display.

Application: MT7981 gateway Web UI

Open: Application → PLC Collect → Operation for PLC_A → Monitor

Point Monitor opens; this is neither the TIA watch table nor the dashboard.

Need help opening it? Return to the application entry guide

Action and save

1. In the main PLC Collect list, use Monitor on PLC_A to open Point Monitor for test_value. Record the state/errors/update information actually available.
2. Compare the same CPU/address/type/scale against A5 over several cycles. If no update-time field exists, use simultaneous site reads and subsequent message receive times.
3. Add points in small batches after the first passes. Retain the last working map revision.

Expected behavior / proceed when

Values agree with the site within expected change/latency. Errors and freshness are assessed rather than treating a retained value as healthy.

Take care at this step

Vendor-tool access does not prove third-party-driver access. Confirm CPU protection, DB access and protocol security against the actual driver/project; do not disable protection globally.

Return/proceed: After the known point passes, close monitoring and scroll to Data Report for P4.

If this step fails

Observed symptom / behavior	Where / which file	Checks and condition to continue
All points time out or have no response	P1 parameters, gateway-to-PLC path, CPU access/resources and matching logs.	Verify protocol/IP/port/CPU settings, then gateway-side network and permission. Do not rewrite every point when all fail together.
One point fails or values differ by 10/100 times	P2 offset/bit/type/length/byte order/scale and A5 raw value.	Return to one point, correct raw reading and apply scale in one place only. Restore the last valid batch before P4.

Files and screens to check/save

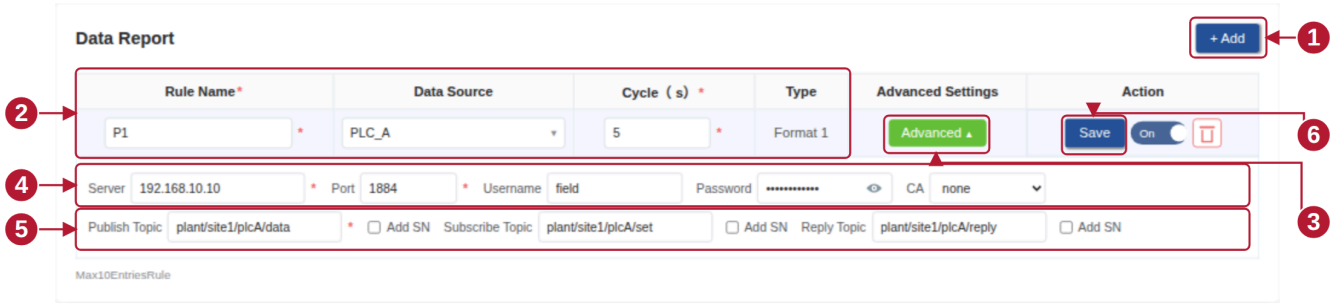
Save P3_monitor.png, same-time A5 evidence and the local log; record result/time in the map.

P4 Configure the PLC-specific MQTT reporting rule

Use case: Gateway monitoring is correct; send PLC_A to the customer platform.

Application: MT7981 PLC Web page
Open: Application → PLC Collect → scroll down to Data Report → + Add → Advanced
Expect rule/source/seconds/advanced settings, not the upper connection form.
Need help opening it? Return to the application entry guide

PLC reporting | Local example on the native form



Native interface with separate operation markers. Match numbers to the table below.

P4 1 Add; 2 name/source/seconds; 3 Advanced; 4 server/authentication; 5 topics; 6 enable/Save.

Action and save

1. Return to Application > PLC Collect, scroll to Data Report and use its + Add, not the upper connection Add. Select verified PLC_A, a rule name and a sample 5-second period.
2. Expand Advanced at 3. Enter the real broker/port/authentication/CA at 4 and publish topic plant/site1/plcA/data at 5, plus other required project topics.
3. For the first check, leave SN suffixes off if suitable. Enable and Save the rule at 6; read back source and topics.

Expected behavior / proceed when

The rule is saved/enabled for PLC_A. P5 independently proves reception.

Continue this step on the immediately following pages with the same code. Complete all its actions/checks before the next step.

P4 Configure the PLC-specific MQTT reporting rule

Step checks (following the action)

Take care at this step

Acquisition at 2000 ms is separate from reporting every 5 seconds. The figure's P1 rule, 192.168.10.10:1884 and test account are not delivery values. Do not publish controls in a read-only task.

Return/proceed: Read back source/topic after Save; verify reception in the external P5 receiver.

If this step fails

Observed symptom / behavior	Where / which file	Checks and condition to continue
Monitoring works but no source is selectable or the rule does not run	PLC_A save/enable state and rule source/enable/save state.	Save a valid connection, reopen the rule and select PLC_A. Do not confuse it with Modbus global MQTT. Save/enable and check reception in P5.
Authentication/certificate failure or repeated disconnects	Actual broker/port, device time, CA, broker connection log and P4 settings.	Check hostname/transport, trust chain, identity validity and permissions. Changing to 8883 alone does not configure TLS. Correct the contract mismatch and observe several cycles.

Files and screens to check/save

Save P4_report.png, actual full topics/SN suffixes and platform connection sheet; obtain broker administrator logs for authentication errors.

P5 Verify a new message at broker and platform

Use case: Prove data reached the platform rather than relying on an existing rule or retained message.

Application: Receiver-side MQTT application or customer platform

Open: Open the project MQTT client → actual broker connection → subscribe to the full P4 topic; use the administrator-supplied platform URL

Inspect fresh topic/time/raw payload; a gateway rule is not a receiver result.

Need help opening it? Return to the application entry guide

Action and save

1. Use an existing MQTT client/platform receiver log on the same broker and subscribe to the full P4 publish topic with the appropriate permission.
2. Observe several reporting cycles and record receive time/topic/raw payload. Locate PLC_A and identifier 1 or the actual point name.
3. Compare with P3/A5 at the same time, then map actual JSON paths, types, scale and time in the platform.

Expected behavior / proceed when

Fresh messages arrive continuously for the correct device/source/point; platform display agrees with the raw payload and site.

Take care at this step

PLC format 1 includes deviceId/deviceName/params/status and values may be strings. Do not use a flat Modbus path; a retained message does not prove a live source.

Return/proceed: Retain the raw message before platform mapping; no universal platform menu is assumed.

If this step fails

Observed symptom / behavior	Where / which file	Checks and condition to continue
No new broker message	P4 enable/source/full topic, publish-permission logs and P3 freshness.	Prove the source updates, then inspect rule/topic/SN suffix. Distinguish no connection from denied publish. Keep the working PLC map.
Broker has messages, dashboard blank or wrong	P5 raw JSON, platform binding/path/type, scale and seconds/milliseconds.	Locate the real source/point and fix parsing, duplicate scale or time units. Validate the next new message, not just an interface success code.

Files and screens to check/save

Save P5_message.json, P5_receive.csv with receive time/topic, broker connection/rejection logs and platform parsing errors.

4 Part II • MT7628/MT7621: Modbus or an external collector

B1 Choose a task when there is no PLC Collect entry

Use case: An MT7628/MT7621 customer cannot find PLC Collect and needs PLC access.

Application: MT7628/MT7621 Web UI and project plan

Open: Sign in in the browser → Application → inspect delivered Modbus Collect, DTU and M2M Cloud entries

No PLC Collect entry is expected here; do not search for it in the M2M client.

Need help opening it? Return to the application entry guide

Action and save

1. Check the actual Modbus Collect, M2M/VPN and DTU/serial entries and record model/ports. No PLC Collect entry is the expected starting point here.
2. For continuous reporting from an enabled Modbus PLC, follow S1 or S3, S2 and B2. For remote viewing/engineering, use R1–R7, with S4 for serial tools.
3. For continuous S7, MC, FINS or another proprietary protocol, use B3: a PC, IPC or server runs the matching driver; the gateway provides networking or a confirmed serial path.

Expected behavior / proceed when

The plan identifies the driver host, continuous poller and MQTT publisher; both the known point and receiver can be verified.

Continue this step on the immediately following pages with the same code. Complete all its actions/checks before the next step.

B1 Choose a task when there is no PLC Collect entry

Step checks (following the action)

Take care at this step

Local Modbus Collect on MT7628/MT7621 uses TCP/RTU. Do not apply the MT7981 64-entry catalogue. DTU/remote COM carries data; it does not automatically convert S7/MC/FINS into Modbus.

Return/proceed: Use S1/S3 for Modbus, B3 for an external driver or R1 for maintenance.

If this step fails

Observed symptom / behavior	Where / which file	Checks and condition to continue
No PLC entry is mistaken for broken firmware	Model/platform, application menu and delivery record.	For MT7628/MT7621, choose a path here; do not reset for a missing MT7981 entry. If Modbus is absent too, confirm the delivered firmware before applying S.
PLC has Ethernet but no Modbus service	PLC module/project services, register map and local vendor-tool result.	Confirm an actual Modbus server and map. Otherwise use remote maintenance R or an external B3 driver; do not enter DB or MC addresses as Modbus registers.

Files and screens to check/save

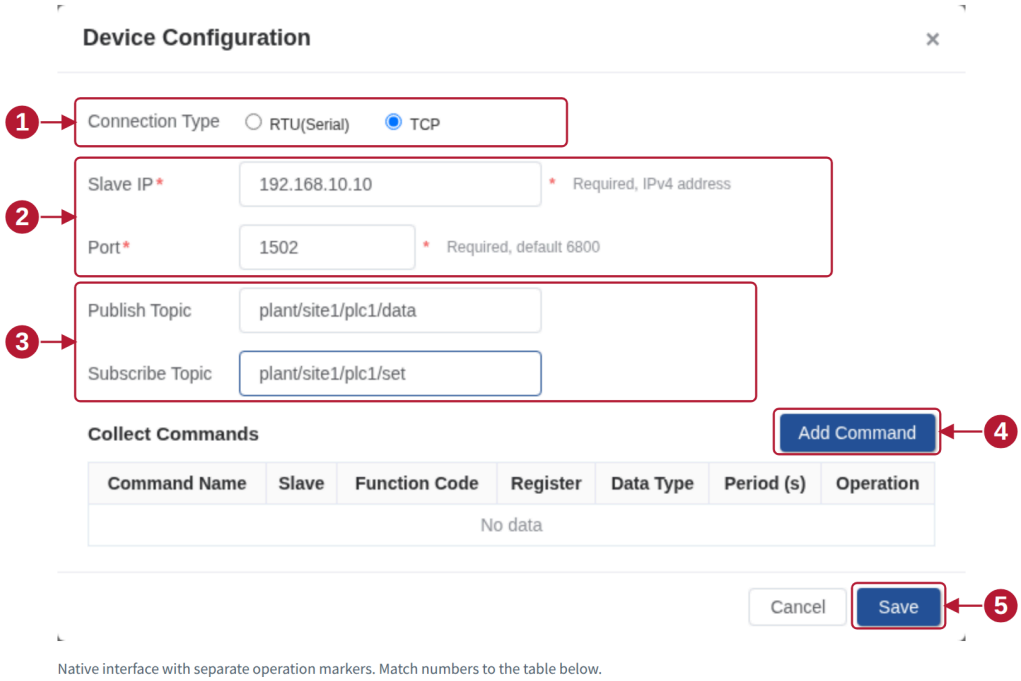
Save B1_apps.png and B1_plan.csv: task, PLC service, driver host, interface and owner.

S1 PLC supports Modbus TCP: save its device connection

Use case: Use the PLC's enabled Modbus service on MT7628/MT7621/MT7981 rather than a dedicated PLC driver.

Application: Gateway Modbus Collect, not the dedicated PLC driver
Open: Application → Modbus Collect → device list → Add Device → TCP connection
The TCP device form contains PLC IP/port, topics and Add Command.
Need help opening it? Return to the application entry guide

TCP device | Save the command before step 5



Native interface with separate operation markers. Match numbers to the table below.

S1 1 TCP; 2 PLC IP/port; 3 topics; 4 command; 5 device Save.

Action and save

1. Confirm the PLC Modbus TCP server is enabled and obtain IP, actual port, Unit ID and register map. An S7 service is not automatically Modbus.
2. Open Application > Modbus Collect > Add Device. Choose TCP at 1, actual PLC IP/port at 2 and project publish/subscribe topics at 3.
3. Add and save the S2 command, then return and Save Device. Complete B2 global settings for reporting. Use S3 for RTU.

Expected behavior / proceed when

The connection and command are saved under the correct device, ready for read-only and receiver checks.

Continue this step on the immediately following pages with the same code. Complete all its actions/checks before the next step.

S1 PLC supports Modbus TCP: save its device connection

> Step checks (following the action)

Take care at this step

> PLC IP is not broker IP. The pictured port 1502 and old lab IP are not site defaults; even common port 502 requires confirmation. Modbus global reporting differs from P4 PLC reporting.

Return/proceed: Open S2 inside this device; save command/device, then B2 global settings.

If this step fails

Observed symptom / behavior	Where / which file	Checks and condition to continue
TCP port unreachable	PLC service settings, A2 network, actual port and policy.	Test the same IP/port locally. If that fails, fix service/network. If only the gateway fails, inspect its initiating path rather than changing registers.
Device exists but command is missing/inactive	Command, device and global saves/enables.	Read back all layers and save command → device → global as in S2. An existing row alone does not prove acquisition is running.

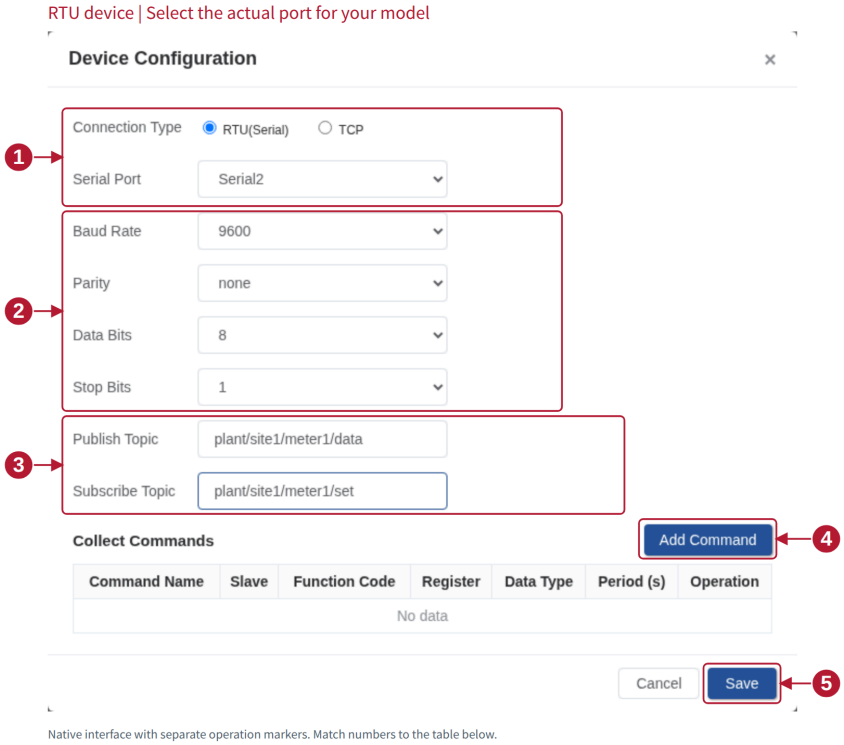
Files and screens to check/save

Save S1_tcp.png, the PLC Modbus service settings and S1_register_map.csv; retain the actual service-port test on failure.

S3 Serial acquisition: verify the physical port and ownership

Use case: A legacy PLC or instrument uses serial communication and the gateway will poll it.

Application: Gateway Web UI and exact-model serial references
Open: Application → Modbus Collect → Add Device or edit the intended device → RTU → actual Serial port
Serial/baud/data/parity/stop settings appear, not PC COM numbering.
Need help opening it? Return to the application entry guide



S3 1 RTU/actual port; 2 matching line parameters; 3 topics; 4 command; 5 device Save.

Action and save

1. Wire from the exact gateway terminal diagram, PLC pinout and Serial mapping. Do not wire RS232 as RS485 A/B; match each vendor's actual A/B or polarity definition.
2. Ensure DTU, remote COM, PLC driver or another application does not own the port. Select RTU and the correct Serial port in the Modbus connection.
3. Match baud, data bits, parity and stop bits. Add a read-only S2 command, then save command → device → B2 global settings.

Expected behavior / proceed when

Correct physical/line settings produce valid protocol replies and a known register; merely opening a COM is insufficient.

Continue this step on the immediately following pages with the same code. Complete all its actions/checks before the next step.

S3 Serial acquisition: verify the physical port and ownership

Step checks (following the action)

Take care at this step

The YZW1010 reference maps Serial1 to RS232 and Serial2 to RS485. Check the actual YZW280/K001 order. YZW900 has no physical serial port. Follow the bus design for termination, shield and reference ground.

Return/proceed: After serial checks, use S2 and save command → device → B2 global settings.

If this step fails

Observed symptom / behavior	Where / which file	Checks and condition to continue
Every slave times out	Both electrical pinouts, Serial map, ownership, baud/parity/station and a site-tool comparison.	Check power, electrical type, wiring and ownership, then line parameters. Prove a response with a compatible site tool. Do not rewrite registers for a completely silent bus.
Corrupt data, CRC errors or intermittent timeout	Error times, both line settings, cable and bus layout.	Match line settings, secure wiring and review the bus design. Compare one known device in isolation; observe several good cycles before restoring all nodes.

Files and screens to check/save

Save S3_wiring.png, S3_serial.png, PLC serial settings and the port ownership record.

S2 Verify one read-only Modbus register

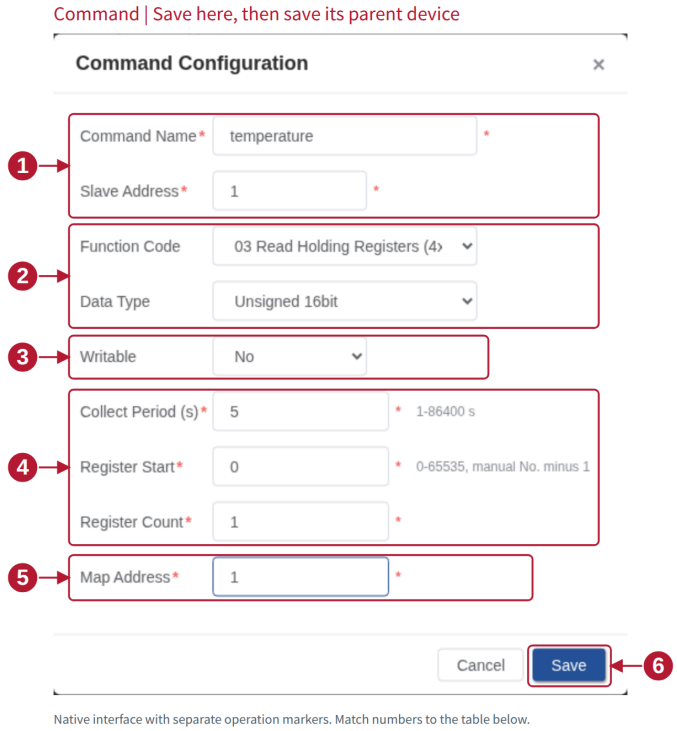
Use case: TCP or RTU is selected; avoid confusing function, address and type.

Application: The selected TCP or RTU device form

Open: Application → Modbus Collect → edit the S1/S3 device → Add Command, or edit its existing command

The command form shows slave/function/type/start/count and Writable.

Need help opening it? Return to the application entry guide



S2 1 name/slave; 2 function/type; 3 Writable: No; 4 seconds/start/count; 5 application mapping address; 6 Save command, then save device.

Action and save

1. In Add Command enter point name, actual Unit ID/slave, function and type. Select No for writable on the first test.
2. Copy interval, start and count from the PLC map. An isolated example contract is slave 1/FC03/PDU start 0/count 1/UInt16; use it only when the PLC actually maps that register.
3. Save command → device → global enable/reporting. Compare the raw value with the map before applying scale.

Expected behavior / proceed when

The read succeeds with the known count/type. Only a mapped scale of 0.1 makes a raw 255 correspond to engineering value 25.5.

Continue this step on the immediately following pages with the same code. Complete all its actions/checks before the next step.

S2 Verify one read-only Modbus register

Step checks (following the action)

Take care at this step

Reference numbers such as 40001 may differ from zero-based PDU addressing; follow the PLC map. Do not insert a dedicated-driver DB address. Mapping/IEC104 addresses are not register starts.

Return/proceed: Save command/device, then return to Modbus global B2; do not validate by writing.

If this step fails

Observed symptom / behavior	Where / which file	Checks and condition to continue
Exception 01 or 02	Raw error, function, start/count and PLC register map.	For 01 check the supported function; for 02 check address/range and zero/one-based convention. Correct one evidenced mismatch and reread one command.
Wrong number, sign or byte order	S2 register count, UInt/Int/Float, byte order and known raw value.	Check register count/type, then word/byte order. Apply scale last and avoid duplicate conversion downstream.

Files and screens to check/save

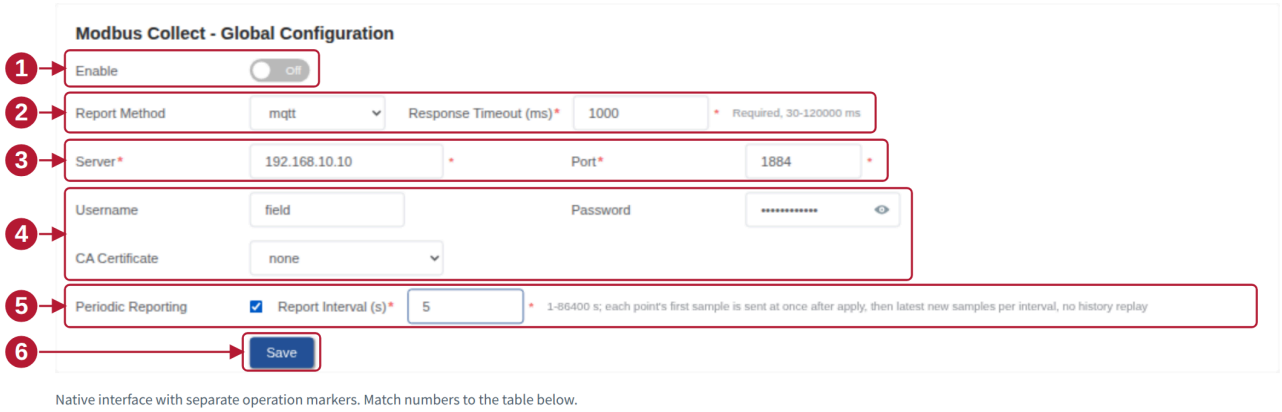
Save S2_command.png, the source register map and S2_read.csv with raw value/type/scale/time.

B2 Enable and verify reporting in Modbus global settings

Use case: S1/S3 and S2 work on a platform without PLC Collect; the gateway must report register values continuously.

Application: Gateway Modbus global settings
Open: Application → Modbus Collect → upper global settings section
Enable/transport/broker/port/period appear; this is not PLC Data Report.
Need help opening it? Return to the application entry guide

MQTT reporting | Complete steps 1 to 6



Native interface with separate operation markers. Match numbers to the table below.

B2 1 enable; 2 MQTT/response timeout; 3 server/port; 4 identity/CA; 5 periodic reporting/seconds; 6 Save.

Action and save

1. Open Application > Modbus Collect global settings. Enable at 1; set MQTT/response timeout at 2 and actual broker/port/identity/CA at 3–4.
2. At 5 enable periodic reporting as required, e.g. every 5 seconds, then Save at 6. Read back the saved device/command and actual S1/S3 publish topic.
3. Subscribe to the complete topic using an existing customer receiver or log. Compare fresh payloads over several cycles with S2 raw values, then map field/type/scale/update time in the platform.

Expected behavior / proceed when

The command remains valid; the broker receives fresh gateway publications and platform values match the PLC at the same time, even after the engineering PC exits.

Continue this step on the immediately following pages with the same code. Complete all its actions/checks before the next step.

B2 Enable and verify reporting in Modbus global settings

Step checks (following the action)

Take care at this step

This is Modbus global MQTT, separate from P4 PLC rules. Periodic reporting does not guarantee backfill. Response timeout is in milliseconds; reporting is in seconds. Do not copy the demonstration broker/account; configure TLS through the actual supported controls.

Return/proceed: After global Save, inspect the actual Modbus topic at the project receiver.

If this step fails

Observed symptom / behavior	Where / which file	Checks and condition to continue
S2 reads, but the platform receives no fresh data	Device/command/global saves and enables, topic/SN, gateway log and broker connection/ACL.	Read back all three configuration layers, then topic, uplink, broker port and identity rights. Distinguish no connection from denied publish. Fix the failing layer and observe several cycles; retain the correct register map.
Broker receives values, but the dashboard is wrong or stale	B2 raw JSON/receive time/retained flag, S2 map and platform mapping/scale.	Parse the real Modbus payload instead of P5 PLC params. Compare raw values before type/scale, and check new sample and ingestion times. Accept recovery using a fresh message.

Files and screens to check/save

Save B2_global.png, B2_message.json, B2_receive.csv, effective topic and System Management > Log export; obtain matching broker authentication/ACL logs when rejected.

B3 Run proprietary-protocol acquisition on an external host

Use case: MT7628/MT7621 has no PLC Collect and the PLC exposes no Modbus service, but continuous acquisition is required.

Application: Continuously running external IPC/server

Open: Start the delivered external collector → its PLC driver/connection setup → confirmed point map and platform output

The driver runs externally; no extra local S7/MC/FINS page is implied.

Need help opening it? Return to the application entry guide

Action and save

1. Assign a site IPC or continuously available PC/server with compatible acquisition software and the PLC driver. First reproduce the A4/A5 known-point read locally.
2. A site collector on the PLC LAN connects directly. A remote server first needs a persistent authorized R1–R6 path. For serial transport also verify S4 compatibility; network serial is not suitable for every vendor protocol by default.
3. Configure the PLC target, known-point read and MQTT/platform output in that external application. Record service startup/reconnect behavior. Close temporary engineering tools, observe continued acquisition and verify N2 recovery.

Expected behavior / proceed when

The external host runs the poller continuously and the platform receives identifiable fresh values; the gateway provides the configured network/serial path.

Continue this step on the immediately following pages with the same code. Complete all its actions/checks before the next step.

B3 Run proprietary-protocol acquisition on an external host

Step checks (following the action)

Take care at this step

On MT7628/MT7621, the external application runs the proprietary-protocol driver. Continuous acquisition needs more than a temporary vendor-tool session. Keep the collector host and required path available; shutdown, sleep or an ended VPN session can interrupt data.

Return/proceed: Record the real application/menu/service and owner; no fictional common UI is supplied.

If this step fails

Observed symptom / behavior	Where / which file	Checks and condition to continue
Reporting stops when the PC closes or sleeps	Actual poller host, power plan, application process/service and VPN state.	Identify the poller/publisher. Keep its host/service available and configure supported reconnect behavior. A temporary maintenance client is not an unverified 24-hour production path. Verify the first fresh recovered value.
VPN connects but the external driver cannot read	R6 port/path, external driver error, CPU/firmware, map and A5 local result.	Separate reachability from protocol rejection. After service reachability, verify driver version, CPU support, credentials and address syntax. Restore one read-only point before batching; repeated VPN setup or MQTT-topic changes do not fix a protocol error.

Files and screens to check/save

Save B3_architecture.csv, external software configuration export/version, B3_service_log.txt exported by that application, raw payloads and freshness/recovery times.

5 Shared remote maintenance: vendor tools on the PC

R1 Confirm the site gateway can reach the platform

Use case: The engineer is off site and the device is offline or being connected for the first time.

Application: Site gateway Web UI, with the site operator
Open: Overview → Network Settings → WAN or Mobile; for faults use System Management → Log
Inspect the actual uplink state; follow the delivered model ports/module.
Need help opening it? Return to the application entry guide

Action and save

1. Ask the site operator to open Overview and the active uplink page. Use WAN for wired access or the delivered Mobile page for cellular.
2. For wired access check IP/gateway/DNS and the upstream network. For cellular check SIM, antenna, APN, registration and dialing.
3. Then check the gateway's path to the delivered platform host/service. Review System Management > Log and save it before restarting.

Expected behavior / proceed when

The actual uplink has a valid address and reaches the required platform. The PC's own internet access does not prove the gateway path.

Continue this step on the immediately following pages with the same code. Complete all its actions/checks before the next step.

R1 Confirm the site gateway can reach the platform

> Step checks (following the action)

Take care at this step

> Use the real model's uplink; do not assume a separate WAN on K001. Obtain APN and allow-list settings from the project, not a generic example.

Return/proceed: After uplink checks use R2 for M2M, or R6 after the approved independent VPN works.

If this step fails

Observed symptom / behavior	Where / which file	Checks and condition to continue
Cellular registration or dialing keeps failing	Mobile status, SIM/plan/APN and matching log time.	Check SIM validity, matching antennas and operator parameters, then signal/service errors. Continue to R2 after registration/dialing and address recovery.
An address exists, but platform access times out	Gateway DNS/uplink and server connection exceptions in its log.	Check platform host/port, DNS and upstream policy. Ask the administrator to check the listener; distinguish refusal from timeout. Do not change PLC addresses for this fault.

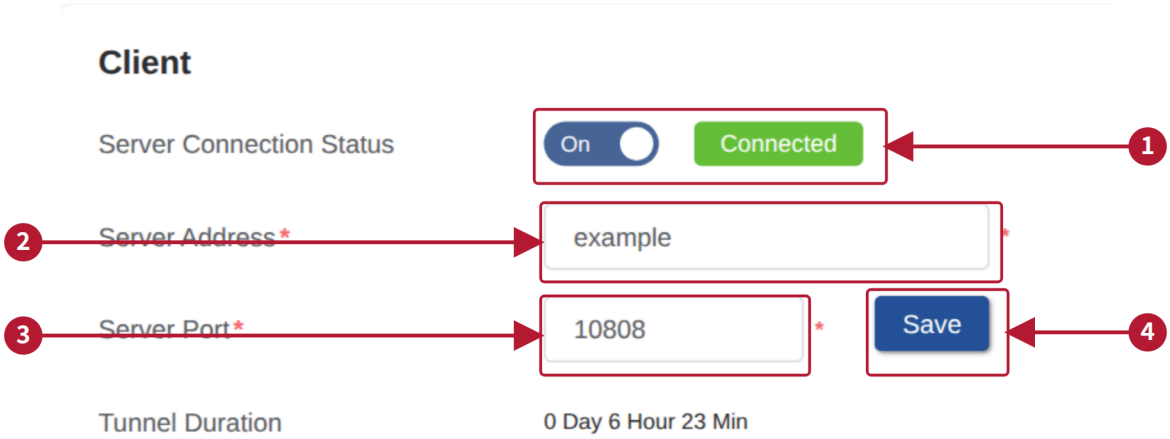
Files and screens to check/save

Save R1_uplink.png, the actual log export and fault time; inspect WAN/Mobile/link entries first.

R2 Configure gateway M2M Cloud and check both states

Use case: The uplink works; the gateway must join its authorized remote network.

Application: Gateway Web UI, not the Windows sign-in dialog
Open: Sign in to the site gateway in a browser → Application → M2M Cloud
Enable/server/port/tunnel status appear under the gateway Web identity.
Need help opening it? Return to the application entry guide



R2 1 control switch/state; 2 host; 3 port; 4 Save. Check tunnel state separately lower on the page.

Action and save

1. Open Application > M2M Cloud. Enable at 1, enter the delivered host/service port at 2–3 and Save at 4.
2. Have the administrator verify device identity/permission. Check server connection, tunnel type/state and the actual M2M IP separately.
3. Use the project's L3 or L2 mode. Configure remote subnets separately only when the gateway needs another remote network.

Expected behavior / proceed when

Control connection is healthy, the business tunnel is available and a virtual address is assigned. Awaiting authorization or server connection alone is not PLC readiness.

Continue this step on the immediately following pages with the same code. Complete all its actions/checks before the next step.

R2 Configure gateway M2M Cloud and check both states

Step checks (following the action)

Take care at this step

The displayed example host/port only locate the fields. Do not add the gateway's own PLC LAN as its remote subnet.

Return/proceed: Save and check permission/tunnel, then switch to the engineer PC M2M client for R3.

If this step fails

Observed symptom / behavior	Where / which file	Checks and condition to continue
Waiting for server authorization	M2M page, device identity and administrator permission list.	Confirm the same platform/device, complete authorization and refresh. Do not repeatedly create different identities.
Server connected, tunnel waiting or no virtual IP	Tunnel state/type, R2 screenshot and M2M log.	Check the authorized network, mode and platform business channel. Resolve the tunnel error with the administrator before R3; server online is not tunnel acceptance.

Files and screens to check/save

Save R2_m2m.png. In the local log inspect the M2M program, connection state, last exception and time.

R3 Sign in on the PC and identify the site

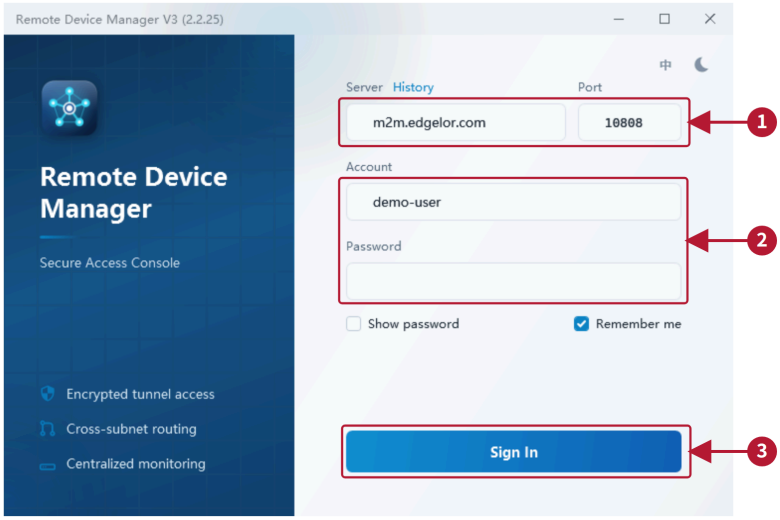
Use case: An engineer is about to connect to an authorized site from the office.

Application: M2M client on the engineer Windows PC

Open: Start menu or desktop → delivered Remote Device Manager/M2M shortcut → sign-in dialog → device list

The desktop window shows device rows and Routes/Adapter controls, not the gateway Web page.

Need help opening it? Return to the application entry guide



R3 1 platform/port; 2 client credentials; 3 Sign In. Native offline example from the supplied V3 manual.

Action and save

1. Install the delivered client, start it as instructed and confirm M2MCloud Virtual Adapter is available. The V3 reference commonly uses 64-bit Windows 10/11 and .NET Framework 4.8.
2. Enter the project platform at 1, client account/password at 2 and Sign In at 3. This is separate from the gateway Web identity.
3. Identify the site by device ID, location and LAN subnet; check platform, tunnel and device-online states separately.

Expected behavior / proceed when

The correct device is visible, the virtual adapter is healthy and platform/tunnel are available. Identical names still require identity checks.

Continue this step on the immediately following pages with the same code. Complete all its actions/checks before the next step.

R3 Sign in on the PC and identify the site

Step checks (following the action)

Take care at this step

Demo credentials are not production credentials. Do not run a conflicting old client alongside this one. Green platform/tunnel indicators are not PLC acceptance.

Return/proceed: Identify the site; select routed R4 or bridged R5 as planned.

If this step fails

Observed symptom / behavior	Where / which file	Checks and condition to continue
Sign-in fails or the target device is absent	Full error, platform endpoint, account group and device permission.	Distinguish authentication failure from timeout. Verify platform/permissions, remove wrong filters and refresh; do not change the PLC address.
Virtual adapter missing or driver error	Device Manager > Network adapters; R3 version/error screenshot.	Repair the driver/installation using the delivered package and sign in again. Retain the error code. Do not remove other VPN adapters or invent a client log directory.

Files and screens to check/save

Save R3_client.png, the actual client version and adapter state/error code from Windows Device Manager.

R4 L3 routing: reach the PLC by its IP

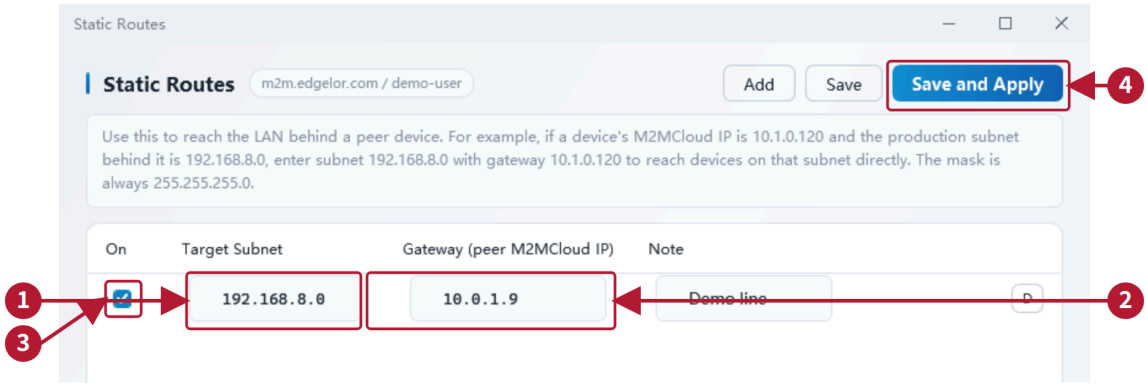
Use case: The tool supports IP access and office/site subnets differ; use the routed option.

Application: Windows M2M client

Open: Device list → right-click the intended online row → Add to routes; use Routes in the top toolbar for manual inspection

The route window exposes the site subnet, M2M next hop and enable state.

Need help opening it? Return to the application entry guide



R4 1 site network; 2 gateway M2M IP; 3 On; 4 Save and Apply.

Action and save

1. Read the actual gateway M2M IP; 10.0.1.9 is an example. The target site subnet is 192.168.8.0/24.
2. Right-click the intended online row and choose Add to routes. Use Routes in the top toolbar to inspect/edit manually: 1 subnet, 2 M2M next hop, 3 On, 4 Save and Apply.
3. Read back Static Routes and route print -4. Ensure a valid PLC return path, then run R6 for 192.168.8.20.

Run these read-only checks in Windows PowerShell. Replace the address/port first; TXT files are saved in the current evidence folder.

```
route print -4 > R4_routes.txt
```

Expected behavior / proceed when

The target subnet uses the intended virtual path/next hop and the PLC service can reply. Broadcast discovery is not required.

Continue this step on the immediately following pages with the same code. Complete all its actions/checks before the next step.

R4 L3 routing: reach the PLC by its IP

> Step checks (following the action)

Take care at this step

> This V3 route screen uses /24; confirm support for other masks. Enter the network .0, not PLC .20. The next hop is not the gateway LAN IP. Do not add a 0.0.0.0 default route.

Return/proceed: Save and Apply, return to the list and run R6 in PowerShell.

If this step fails

Observed symptom / behavior	Where / which file	Checks and condition to continue
Gateway virtual IP reachable, PLC unreachable	R4_routes.txt, PLC return gateway and the A2 local result.	Read back target/next hop/On/application. If local PLC access works, check the return path. Have the administrator review existing gateway/NAT settings rather than overwriting them.
Office access changes after adding the route	Office/VM IPs and matching prefixes in R4_routes.txt.	Check overlapping subnets and accidental default routes. Disable the temporary route, restore the original path and add only the planned site prefix.

Files and screens to check/save

Save R4_routes.png and R4_routes.txt; retain PLC gateway/existing NAT details in the plan.

R5 L2 bridge: when site discovery is needed

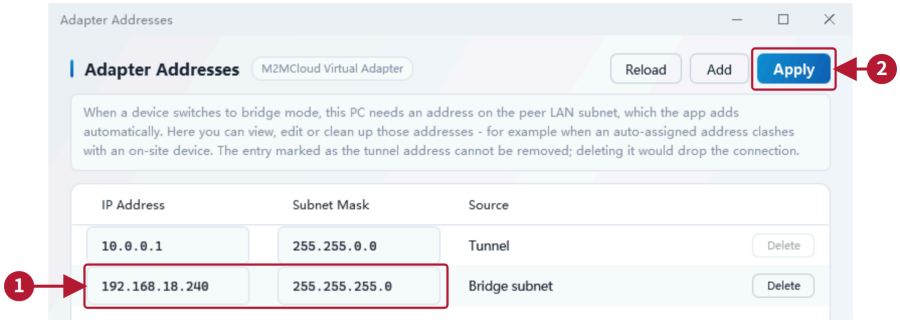
Use case: The tool needs same-subnet discovery and the delivered plan supports L2. This alternative uses 192.168.18.0/24.

Application: Windows M2M client; L2 alternative

Open: Device list → right-click the intended online row → Enable bridge; then use Adapter in the top toolbar

Mode changes and Adapter Addresses shows an unused site address.

Need help opening it? Return to the application entry guide



R5 1 added bridge address; 2 Apply to Adapter. The displayed tunnel range is not a universal allocation.

Action and save

1. Leave the engineering session. Right-click the correct online device, choose Enable bridge and wait for mode/status confirmation.
2. Use Adapter in the client top toolbar to open Adapter Addresses. At 1 confirm an added site address such as 192.168.18.240; choose a planned unused address for a conflict, then apply at 2.
3. Use PLC 192.168.18.20 for this option and select the M2M adapter in the tool. Cancelling the bridge should remove its site address.

Expected behavior / proceed when

Bridge mode is shown and the virtual adapter has an unused site address. R7 must still verify discovery with the actual tool.

Continue this step on the immediately following pages with the same code. Complete all its actions/checks before the next step.

R5 L2 bridge: when site discovery is needed

Step checks (following the action)

Take care at this step

Do not mix this with the L3 .8.20 address or assign the PLC IP to the PC. Start with one known site when several sites reuse a subnet.

Return/proceed: Do not mix the alternative L3 plan; verify the address before R6/R7.

If this step fails

Observed symptom / behavior	Where / which file	Checks and condition to continue
Bridge selected but no site address	Mode/status bar, Adapter Addresses and device-online state.	Refresh actual state and check permission/adapter. Retain explicit errors. Do not hide failures with repeated switching; search only after the address exists.
Office devices become unreachable while bridged	R5 subnet versus the office subnet; route/interface selection.	Cancel the bridge to restore office access, then resolve overlap. Check address ownership separately; do not rely on random metric changes.

Files and screens to check/save

Save R5_mode.png, R5_adapter.png and PC ipconfig; retain address allocation.

R6 Verify the PLC service and actual PC path

Use case: The client is online, but PLC reachability is not established.

Application: The Windows environment that runs the vendor tool
Open: Start menu → Windows PowerShell → run the read-only checks in your evidence folder
Read target, actual interface/source and TcpTestSucceeded.
Need help opening it? Return to the application entry guide

Action and save

1. Check platform control, business tunnel and device identity; test gateway virtual address and PLC address separately.
2. Run Test-NetConnection for the confirmed protocol port: 102 for the confirmed S7 example; use the PLC's actual Modbus TCP port for Modbus.
3. Read InterfaceAlias, SourceAddress and TcpTestSucceeded; ensure traffic is not using an unintended office/Wi-Fi/VM path.

Run these read-only checks in Windows PowerShell. Replace the address/port first; TXT files are saved in the current evidence folder.

```
route print -4 > R6_routes.txt
Test-NetConnection 192.168.8.20 -Port 102 -InformationLevel Detailed > R6_port.txt
```

Expected behavior / proceed when

The service test is True with the intended source/interface; R7 must still verify CPU identity and tool rights.

Continue this step on the immediately following pages with the same code. Complete all its actions/checks before the next step.

R6 Verify the PLC service and actual PC path

> Step checks (following the action)

Take care at this step

> ICMP may be blocked. An open port does not prove tool permissions or driver compatibility. A host test does not replace a test inside the VM.

Return/proceed: If the tool is in a VM, test inside that VM too; then use R7.

If this step fails

Observed symptom / behavior	Where / which file	Checks and condition to continue
Port test is False	R6_port.txt/R6_routes.txt, PLC service settings and the A2 test.	If local also fails, inspect PLC service/port. If only remote fails, check R4/R5, return path and target-port policy. Change one cause and retest.
True, but engineering access fails	Actual tool adapter, full error and CPU/project compatibility record.	Continue at R7 with interface, CPU identity, rights and versions rather than disabling all firewalling or resetting the gateway.

Files and screens to check/save

Save R6_routes.txt, R6_port.txt and fault time; compare failures with A2.

R7 Go online remotely and verify CPU and tag

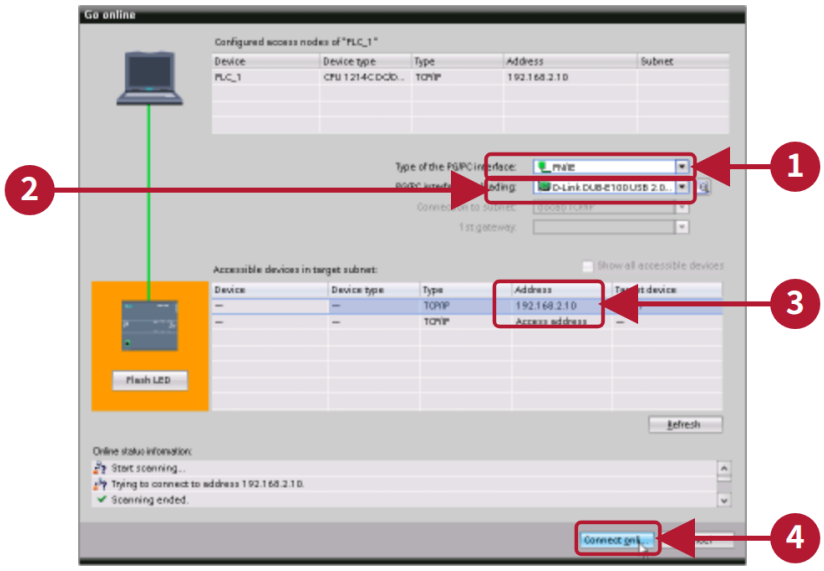
Use case: R6 proves service reachability; reproduce A4/A5 with the vendor tool.

Application: Vendor PLC tool on the engineer PC

Open: Select the correct project PLC in TIA → Online → Extended go online → actual remote interface/target IP

Use the A4-style dialog, then verify CPU diagnostics and the watch table.

Need help opening it? Return to the application entry guide



R7 The same factory figure locates the controls as in A4; select the actual remote interface and target address.

Action and save

1. Use the locally verified project. At 1 choose PN/IE, at 2 check M2MCloud Virtual Adapter against the actual route, and at 3 enter this site's PLC IP.
2. Prefer direct IP in L3. For L2 discovery, confirm the bridge address and search on the virtual adapter. Identify the CPU before Go online at 4.
3. Check CPU identity in online diagnostics, then monitor the same A5 point read-only and compare at the same time.

Expected behavior / proceed when

Remote access reads the same CPU identity and tag as the site; online state and updates are healthy.

Continue this step on the immediately following pages with the same code. Complete all its actions/checks before the next step.

R7 Go online remotely and verify CPU and tag

Step checks (following the action)

Take care at this step

An industrial IP router is not a TIA S7 routing station. If the adapter is absent, check its driver and tool support rather than selecting a random interface.

Return/proceed: Keep the check read-only; finish with N1 without downloading or changing CPU mode.

If this step fails

Observed symptom / behavior	Where / which file	Checks and condition to continue
Discovery fails but direct IP works	L2/L3 mode, selected adapter and R6 service result.	Use direct addressing in L3. Validate L2/tool support only when discovery is required. Discovery failure does not imply a fully broken tunnel.
Access denied, version mismatch or wrong CPU	R7 error, A4 identity/project and accessible CPU diagnostics buffer.	Go offline to verify site/model. Check compatible software, credentials/certificates and connection resources. Resume maintenance only after correct identity and read-only monitoring return.

Files and screens to check/save

Save R7_cpu.png, R7_value.png and full errors; when online access is available, inspect events/times in Online & diagnostics > Diagnostics buffer.

S4 Remote COM maintenance: release the site port first

Use case: An engineer's serial software must reach site equipment; the gateway is not polling it in this task.

Application: Windows M2M client and vendor serial tool

Open: M2M device list → right-click target online row → Remote serial port… → actual Serial → Open; select the ready public PC COM in the vendor tool

The serial dialog identifies the site Serial and public PC COM separately.

Need help opening it? Return to the application entry guide



S4 1 site port; 2 line settings; 3 public PC COM; 4 Open. Close the tool COM before closing its client mapping.

Action and save

1. Verify the R path and a free physical port. Under the site plan, stop the acquisition/DTU owner and retain a restoration record.
2. Choose Remote serial port on the online device. Set 1 actual Serial port, 2 PLC line settings, 3 the public COM allocation and 4 Open.
3. Wait for the public COM-ready message and select that COM in the vendor tool. Use a compatible echo tester or a real read-only protocol test, not arbitrary strings sent to a production PLC.

Expected behavior / proceed when

The COM opens and correct bidirectional protocol replies are received from the intended device/port.

Continue this step on the immediately following pages with the same code. Complete all its actions/checks before the next step.

S4 Remote COM maintenance: release the site port first

Step checks (following the action)

Take care at this step

PC COM numbering differs from gateway Serial numbering. Pictured 115200 and COM4 are examples. Use only the public COM, not its internal companion. Transport does not convert the vendor protocol.

Return/proceed: Close the tool COM before its client mapping and restore ownership with N1.

If this step fails

Observed symptom / behavior	Where / which file	Checks and condition to continue
Open fails or reports in use	Client/other-PC sessions and software/acquisition ownership of the port.	Close the owning session/application and confirm release, then open once. Do not delete COM nodes. Confirm delivered remote-serial support/components.
COM ready but no reply	Electrical wiring, Serial map, line settings and vendor protocol log.	Prove a response locally, then compare the public COM and protocol settings. Retain latency/timeout errors and verify tool support for network serial access.

Files and screens to check/save

Save S4_com.png with actual COM/Serial/settings, vendor errors and port ownership/restoration records.

S5 Treat the HMI as a separate endpoint

Use case: The PLC is reachable, but a separate HMI must be maintained or remains inaccessible.

Application: HMI vendor software, not the PLC tool

Open: Start software matched to the HMI → open its HMI project → its supported connection/device-information or monitoring entry

Verify the HMI identity; different brands do not share a universal TIA menu.

Need help opening it? Return to the application entry guide

Action and save

1. Obtain HMI model/firmware/IP/service ports and matching tool from its label/project. An illustrative HMI IP is 192.168.8.30; use the real site value.
2. Read HMI identity/allowed monitoring locally first, then repeat over R4/R5 with the correct adapter/target IP.
3. Compare identity, project version and allowed functions. Perform project transfer separately under the vendor procedure and site maintenance plan.

Expected behavior / proceed when

The correct HMI, tool and service are reachable with corresponding local and remote results.

Take care at this step

Do not reuse PLC ports, credentials or project formats for the HMI. Web access does not prove project transfer; PLC online does not prove HMI return routing.

Return/proceed: Record the real application/menu; project transfer is outside this read-only check.

If this step fails

Observed symptom / behavior	Where / which file	Checks and condition to continue
PLC reachable, HMI service not reachable	HMI IP/mask/return path, VLAN and actual HMI service settings.	Test the HMI locally on its own. Fix local service/wiring if it fails; otherwise inspect remote/return routes and HMI-port policy.
Network works, vendor tool refuses access	HMI model/firmware/tool/project, permissions and tool error.	Use the compatible tool/project and HMI-specific permission. Do not substitute PLC CPU parameters. Read identity successfully before maintenance.

Files and screens to check/save

Save S5_hmi_identity.png, HMI project/version and local/remote service tests with exact errors.

6 Shared close, recovery and configuration records

N1 Close the session in order and retain production acquisition

Use case: Remote checks are complete and the site must retain its intended operation.

Application: Current engineering tool, M2M client and production service

Open: Stop monitoring/go offline in the vendor tool → close public COM → close its client mapping and temporary bridge/routes

End only temporary maintenance; retain the intended CPU and production acquisition.

Need help opening it? Return to the application entry guide

Action and save

1. Stop monitoring and go offline in the vendor tool; do not stop the CPU merely to end a session.
2. For remote COM, close the tool COM before closing the client mapping and confirm release.
3. Remove temporary bridge/routes within the task scope, restore the PC IP and paused site applications, and retain paths/rules required by continuous acquisition.

Expected behavior / proceed when

Engineering/temporary COM sessions end; CPU/production acquisition match the plan and office networking is restored.

Take care at this step

Check ownership before removing settings. Do not delete a production platform path as a temporary test. Cancelling a bridge removes its site address; the tunnel may remain as delivered.

Return/proceed: Verify production and fresh data; retain any path it needs.

If this step fails

Observed symptom / behavior	Where / which file	Checks and condition to continue
COM close reports in use	Vendor/terminal software, other remote sessions and S4 records.	Close the actual COM owner first, then the mapping. Do not remove companions or reboot the PLC. Restore original polling after release.
Office access or acquisition not restored	Original A2 IP, R4/R5 temporary settings, S3/S4 ownership and original acquisition settings.	Restore from the change list, read back routes/addresses/enables and verify a fresh value. Do not overwrite working settings with an unknown old backup.

Files and screens to check/save

Save N1_close.csv with close time, removed temporary settings, restored applications and owner.

N2 Recover fresh data along the actual path after an outage

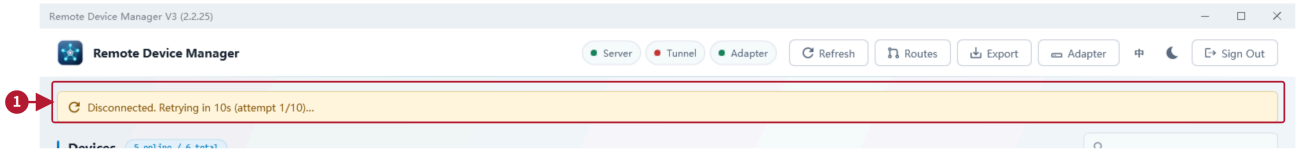
Use case: A wired/cellular outage, PC sleep or network change stops the session/reporting.

Application: Return to the applications used by the actual path

Open: Gateway uplink R1 → required M2M/VPN and R4/R5 → P3/S2 or external B3 → receiver P5/B2

Check current state and the first fresh value at each layer; local polling does not require VPN.

Need help opening it? Return to the application entry guide



N2 Native tunnel-outage example from the supplied client guide. Verify each layer after recovery.

Action and save

1. Record outage time/current screen and preserve gateway logs. Restore the R1 uplink first.
2. For maintenance check R2/R3 then R4/R5; update a changed M2M next hop. For local acquisition check the PLC link and actual broker path; restore VPN only when that path needs it.
3. Reconnect vendor software with R7; check P3/P5 for PLC Collect, S2/B2 for Modbus or B3 for external acquisition. Record recovery and first-valid-fresh-data times.

Expected behavior / proceed when

The actual collector, required path and receiver recover in order. Reads and received messages are fresh; stale values are not accepted as new samples.

Continue this step on the immediately following pages with the same code. Complete all its actions/checks before the next step.

N2 Recover fresh data along the actual path after an outage

Step checks (following the action)

Take care at this step

Automatic client reconnect does not imply automatic TIA session recovery or historical backfill. Confirm any required queue/backfill/time-order contract separately.

Return/proceed: Retain timed outage evidence and repeat the known-point test.

If this step fails

Observed symptom / behavior	Where / which file	Checks and condition to continue
Tunnel recovers but PLC access fails	Current M2M IP, route/bridge, R6 path/port and R7 tool selection.	Read back current addresses/paths rather than assuming the old state. Re-select the interface and reconnect after service reachability; identify the CPU.
Platform retains old values/messages	P3/S2/B3 source updates, P5/B2 receive time/retained flag and platform freshness rules.	Prove fresh sampling and publishing, then mark stale/recovered data by time/quality. Replaying an old message is not recovery acceptance.

Files and screens to check/save

Save N2_outage.png, N2_recovery.csv, original logs/errors and the first fresh recovered payload.

N3 Export configuration and retain recoverable evidence

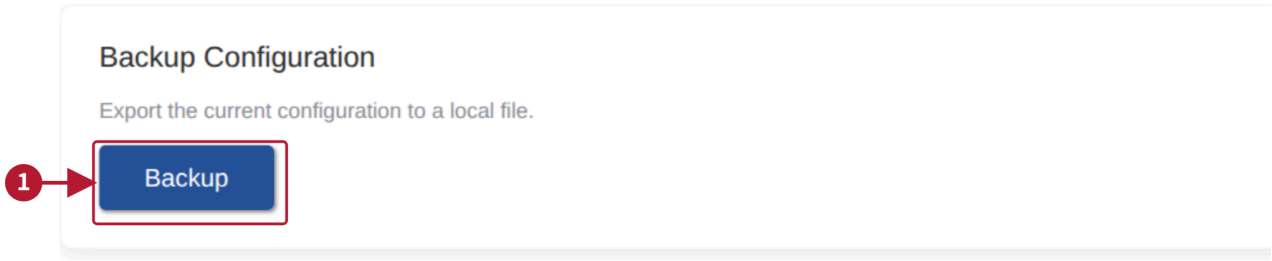
Use case: A workflow is accepted and must be handed over for future maintenance.

Application: Gateway Web UI and PC downloads

Open: Sign in to the gateway → System Management → Config Management → Backup; locate the file through browser Downloads

Confirm an actual downloaded backup; do not select Restore, Factory Reset or Reboot.

Need help opening it? Return to the application entry guide



N3 Use only Backup at 1 in this area; Restore, Factory Reset and Reboot are different actions.

Action and save

1. Open System Management > Config Management and use Backup at 1. Keep the downloaded name/extension and record device/version/time.
2. Retain PLC/HMI project, point map, actual topics, certificate storage reference and per-step records. Do not enter passwords in shared forms.
3. Confirm the backup exists, has a plausible size and matches this revision. Confirm restoration against a matching device/version, not by importing an unknown backup into production.

Expected behavior / proceed when

The accepted configuration, project/map and evidence can be located, with time and owner for actual results.

Continue this step on the immediately following pages with the same code. Complete all its actions/checks before the next step.

N3 Export configuration and retain recoverable evidence

Step checks (following the action)

Take care at this step

Backups can contain credentials; control access and share only relevant redacted errors/necessary fields with support.

Return/proceed: Keep the downloaded name/extension under controlled access and record the handover.

If this step fails

Observed symptom / behavior	Where / which file	Checks and condition to continue
Backup clicked, no file	Browser downloads, current Web session and page feedback.	Check blocked downloads or a different save folder, then retry once with a valid session. Do not substitute Import, Factory Reset or Reboot.
Backup/project version is unclear	File time, model/firmware record, A4 project and N3 parameters.	Retain working files and document version/source. Isolate old backups and confirm compatibility before restoring; a filename alone is insufficient.

Files and screens to check/save

Retain the downloaded backup, Project_Parameters.csv, Step_Check_Record.csv and A/D/P/B/S/R/N step evidence files.

7 Scenario acceptance and handover

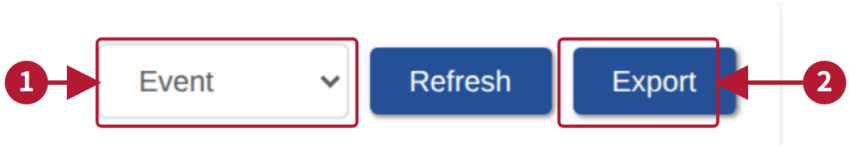
Complete only the scenarios used. Leave untested items blank. Use the evidence defined at each step; this form does not pre-approve a result.

Scope	Steps	Complete on site
Local baseline	A1, A2, A3, A4, A5	Actual result: _____ Time: _____ Owner: _____
Remote/serial/HMI maintenance	R1, R2, R3, R4, R5, R6, R7, S4, S5	Actual result: _____ Time: _____ Owner: _____
Part I: Web PLC acquisition	D1, P1, P2, P3, P4, P5	Actual result: _____ Time: _____ Owner: _____
Part II: Modbus/external acquisition	B1, S1, S3, S2, B2, B3	Actual result: _____ Time: _____ Owner: _____
Close/recovery	N1, N2, N3	Actual result: _____ Time: _____ Owner: _____

Use Project_Parameters.csv for actual versions, addresses, protocol/map and platform details; Step_Check_Record.csv records each symptom, evidence file, action and retest.

7.1 Evidence locations

Where to obtain gateway logs



Log export controls: 1 log category; 2 Export. On the full page also inspect Program, Status, Connection/Outlet and Last Exception.

System Management > Log: refresh, match fault time to M2M Cloud, WAN/Mobile/Link Manager or the relevant program actually present, then export. Retain filename/extension and save with R/P/B screenshots and time zone. Do not infer missing program rows or log paths.

Evidence source	What to retain
Windows networking	TXT output from A2/R4/R6, actual adapter and service port.
PLC/HMI	Original project/map and CPU identity; retain buffer events/times when accessible, otherwise the tool error.
Client	Actual version, device/tunnel state, full error and Windows adapter error code. No fixed log path is assumed.
Broker/platform	Topic/time/raw message, administrator connection/authentication/ACL logs and parsing errors.

References and revision notes

- Siemens S7-1200 V4.4 Chinese manual (11/2019), pp.1387/1398
- Siemens S7-1200 V4.4 English manual (11/2019), pp.1269/1280
- TIA Portal V20: online connection
- STEP 7 V20: PG/PC interface and device address
- STEP 7 V20: CPU diagnostics buffer
- Microsoft: Test-NetConnection
- Modbus Organization: Application Protocol V1.1b3 (PDU addressing and exceptions 01/02)
- STEP 7 V20: creating a watch table
- STEP 7 V20: monitoring tags and CPU-specific cautions

This revision refines current manuals, acquisition guides and the supplied bilingual M2M V3 guide, with MT7981 native protocol/driver evidence. Each language uses native UI and separate annotations. V1.0/V1.1/V1.2 are retained; this revision adds application entry help, step paths and paginated contents.

This work produces and checks documents offline; it does not operate customer gateways/PLCs or change platform firmware source. Confirm actual firmware/CPU/tool combinations on site. Document layout/fonts/navigation and real application acceptance are separate; native Windows Office pagination was not tested.