VECTROLINK
TECHNOLOGIES

vMT-02

Industrial Modbus Translator & RTU/TCP Converter

User Manual

Installation, Configuration & Operation Guide

Firmware version: 0.3.1

Document version: 1.6

November 13, 2026

Confidential — intended for the customer and operating personnel of this device.

Contents

1 Introduction **3**
- 1.1 About This Document . . . 3
- 1.2 What is the vMT-02? . . . 3
- 1.3 Operating Modes . . . 4
- 1.4 Key Features at a Glance . . . 4

2 Hardware Overview **5**
- 2.1 Platform . . . 5
- 2.2 RS-485 Bus Termination . . . 5
- 2.3 Status LED Indications . . . 5
- 2.4 Push-Button Functions . . . 6
- 2.5 Power and Mounting . . . 7

3 Getting Started **8**
- 3.1 Initial Power-Up . . . 8
- 3.2 Connecting for the First Time . . . 8
- 3.3 Default Login Credentials . . . 8
- 3.4 Network Configuration . . . 9
- 3.5 Quick-Start Checklist . . . 9

4 Web Interface Guide **10**
- 4.1 Dashboard . . . 10
  - 4.1.1 Configuration Backup . . . 10
- 4.2 Translator Mode . . . 10
  - 4.2.1 Mapping Fields . . . 11
- 4.3 Transparent Mode . . . 11
- 4.4 Manual Read . . . 12
- 4.5 User Management . . . 12
- 4.6 Network Settings . . . 13
  - 4.6.1 Wi-Fi Configuration . . . 13
  - 4.6.2 Ethernet Configuration . . . 13
  - 4.6.3 Automatic Firmware Updates . . . 13
  - 4.6.4 Danger Zone: Factory Reset . . . 13

5 Modbus Protocol Reference **15**
- 5.1 Supported Function Codes . . . 15
- 5.2 Modbus Roles . . . 15
- 5.3 Addressing . . . 15
- 5.4 Data Types . . . 16
- 5.5 Byte Order . . . 16
- 5.6 Scaling . . . 16

6 Security Notes **17**

6.1 Device Integrity . . . 17
6.2 Encrypted Web Access (HTTPS) . . . 17
6.2.1 Why Your Browser Shows a Warning . . . 17
6.3 Accounts and Passwords . . . 17
6.4 Network Placement Recommendations . . . 18
6.5 Remote Access via Vectrolink Cloud . . . 18
6.6 Account Permissions . . . 18

7 Troubleshooting **19**
7.1 Common Issues . . . 19
7.2 Getting Further Help . . . 19

8 Specifications **21**
8.1 Capacity Limits . . . 21
8.2 Connectivity . . . 21
8.3 Physical and Electrical . . . 22
8.4 Supported Data Types . . . 22
8.5 Supported Modbus Function Codes . . . 22
8.6 Account Permissions . . . 22
8.7 Security . . . 22

9 API Reference **23**
9.1 Connecting . . . 23
9.2 Authentication . . . 23
9.3 Configuration & Status . . . 24
9.4 Translator Mappings . . . 24
9.5 Transparent Mappings . . . 24
9.6 Manual Read . . . 24
9.7 Network . . . 25
9.8 Users & Sessions . . . 25

Chapter 1

Introduction

1.1 About This Document

This manual describes the installation, configuration, and day-to-day operation of the **Vectrolink vMT-02**, an industrial Modbus translator and RTU/TCP converter. It is intended for technicians, system integrators, and operators who install, configure, or maintain the device on site.

This document covers:

- Hardware overview and physical interfaces
- Initial setup and first boot
- Full walkthrough of the embedded web configuration interface
- Modbus protocol support and data type reference
- Security notes relevant to operators and IT staff
- Troubleshooting common issues

This document does *not* cover internal firmware architecture, source code, or developer-level integration details. That material is provided separately in the *Vectrolink vMT-02 Internal Engineering Reference*, intended for the development and engineering team.

1.2 What is the vMT-02?

The vMT-02 is a compact gateway device that bridges **Modbus RTU** (serial, RS-485) field devices with **Modbus TCP** networks (Ethernet or Wi-Fi). It is designed for industrial and building-automation environments where legacy RTU instruments (sensors, meters, PLCs, drives) need to be integrated into a modern, IP-based SCADA, HMI, or building management system (BMS).

Unlike a simple protocol converter, the vMT-02 allows the register map exposed on the TCP side to be **freely re-mapped and re-typed** from the registers available on the RTU side. This means the gateway can:

- Present RTU device registers at different TCP register addresses than they exist on the field bus.
- Convert between raw register encodings (e.g., two 16-bit registers as a 32-bit float) and the data type used by the downstream SCADA/HMI system.
- Operate as a 1:1 transparent bridge when no translation is required.
- Be polled and re-configured remotely through its built-in web interface.

1.3 Operating Modes

The device supports three operating modes, which can be combined per register mapping:

Translator mode Register mappings are defined between a source (RTU or TCP) and a target, with configurable data type conversion, byte-order handling, and scaling. Mappings can run on a fixed polling cycle (*cyclic*), on incoming request (*on-demand*), or in response to a data-change event (*on-event*).

Transparent mode The gateway forwards requests 1:1 between the Modbus TCP/RTU client and the target RTU/TCP device, with no register remapping. This is the simplest mode and behaves like a classic protocol converter.

Manual Read An on-demand diagnostic mode, operated from the web UI, used to poll a specific register range from a device directly – useful for commissioning and troubleshooting without creating a permanent mapping.

Translator mode and Transparent mode are mutually exclusive at the system level: enabling Transparent mode suspends the cyclic translator polling engine. Manual Read is always available regardless of the active mode.

1.4 Key Features at a Glance

Feature	Description
Dual connectivity	Simultaneous Wi-Fi and Ethernet, with independent network configuration
Embedded web UI	No software installation required – configure entirely from a browser
Register translation	Re-map and re-type registers between RTU and TCP
Data type support	U16, I16, U32, I32, U64, I64, FLOAT32, FLOAT64, BCD
Role-based access	Administrator and standard user accounts with separate permission levels
HTTPS web access	Encrypted access to the configuration interface

Chapter 2

Hardware Overview

2.1 Platform

The vMT-02 runs on a dual-core microcontroller (240 MHz) with the following on-board interfaces:

Interface	Purpose
RS-485 – 2 independent channels (RS485-1, RS485-2)	Two separate Modbus RTU field bus connections (master and/or slave), each with its own baud rate, parity, and stop bits
10/100 Ethernet	Modbus TCP network connection, primary recommended connectivity
Wi-Fi 802.11 b/g/n	Modbus TCP network connection / configuration access, secondary or backup connectivity
Status LED (RGB)	Visual indication of boot state, network activity, and Modbus traffic
Push-button	Temporary Wi-Fi activation and factory reset (see Section 2.4)

2.2 RS-485 Bus Termination

Each RS-485 channel has an on-board termination resistor that can be switched in or out using a jumper: **J5** for RS485-1, **J6** for RS485-2.

Both jumpers ship **open (termination disabled)** by default on every unit.

A correctly terminated RS-485 bus needs a termination resistor at each of its two physical ends, and nowhere else. Fitting the jumper on a device that is not at the end of the bus adds an extra resistor in parallel with the ones already there, which loads the bus and can cause intermittent communication errors that are hard to trace back to this cause.

Fit the jumper for a given channel only if the vMT-02 is physically the last device on that RS-485 segment. Leave it open if the bus continues past the vMT-02 to other devices, or if termination is already provided elsewhere on the segment.

2.3 Status LED Indications

The device has a single RGB status LED that communicates its current state:

The steady background colour reflects overall connectivity; brief pulses for Modbus activity and errors, and yellow/red flashes for button actions, briefly override it and then it returns to whichever background colour currently applies.

LED behaviour	Meaning
White, blinking	Device is starting up / initializing (approximately 10 seconds after power-on)
Green, steady	Normal operation: network connected (Wi-Fi or Ethernet) and Vectrolink Cloud reachable
Orange, steady	Network connected, but Vectrolink Cloud is not currently reachable (check internet access)
Red, steady	No network connection at all (neither Wi-Fi nor Ethernet)
Purple, steady	Access Point mode active – the device is broadcasting its own Wi-Fi hotspot (see Section 2.4)
Cyan, brief pulse	Modbus master activity: the device is reading from a field device
Blue, brief pulse	Modbus slave activity: another device (SCADA, HMI) is reading from the vMT-02
Red, brief flash	Modbus error: timeout, CRC error or exception
Yellow, 1 flash	Push-button: short press recognised
Yellow, 2 flashes	Push-button: double press recognised
Amber, blinking (speeding up)	Push-button: held down, factory reset building up – starts blinking slowly around 2 seconds into the hold and blinks faster the closer it gets to 10 seconds; release before then to cancel
Yellow, 4 flashes, then red 6 flashes	Push-button: long press recognised, factory reset in progress

2.4 Push-Button Functions

The device has a single physical push-button with three distinct actions, depending on how it is pressed:

Short press (press and release quickly) Temporarily enables Wi-Fi in *station* mode for 10 minutes, then automatically reverts to the previous network configuration. Useful if Wi-Fi was disabled and you need temporary access.

Double press (two short presses within roughly half a second) Temporarily enables Wi-Fi in *access point* mode for 10 minutes – the device creates its own Wi-Fi hotspot you can connect to directly, then automatically reverts afterward. Useful if the device cannot be reached on the existing network at all.

Long press (hold for 10 seconds or more) Performs a **factory reset**: network settings, register mappings, and user accounts are erased and reset to defaults. Starting about 2 seconds into the hold, the status LED blinks amber, speeding up the closer you get to 10 seconds – release before then to cancel without making any changes.

Factory reset erases register mappings, user accounts, and network configuration – this cannot be undone. Export a configuration backup from the Dashboard (Section 4.1.1) before performing a long press. The device's identity (name, serial number) and its connection to Vectrolink Cloud (including its TLS certificate) are *not* affected – you will not need to re-register the device afterward.

2.5 Power and Mounting

Refer to the datasheet supplied with your specific hardware revision for power supply voltage range, connector pinout, and mechanical (DIN-rail / enclosure) mounting details, as these may vary between hardware batches.

Chapter 3

Getting Started

3.1 Initial Power-Up

1. Connect the RS-485 wiring to your Modbus RTU field devices.
2. Connect an Ethernet cable if you intend to use a wired network connection.
3. Apply power to the device.
4. Observe the status LED: it will blink white for approximately 10 seconds while the device initializes, then turn steady green once startup is complete.

3.2 Connecting for the First Time

On first boot, no Wi-Fi network is configured. The device automatically falls back to creating its own access point so that it can always be reached:

1. On your laptop or phone, look for a Wi-Fi network named `vMT-02_<SERIAL>`, where `<SERIAL>` is the 8-character serial number unique to your device (printed on the device label, and also visible in the boot log over USB-serial).
2. Connect to this network using the password `12345678`.
3. Open a web browser and navigate to:

   `http://192.168.4.1`

4. You will be presented with the login page of the embedded web interface.

If your device already has a saved Wi-Fi network or is connected via Ethernet with DHCP, it will instead obtain an address on your existing network. Check your router's DHCP client list for a device named `vMT-02_<SERIAL>` (same serial number as the access-point name above) – most routers show this alongside the assigned IP address. If you cannot locate it, use the push-button (see Section 2.4) to temporarily force the device back into access-point mode.

3.3 Default Login Credentials

The device ships with two pre-configured accounts for day-to-day use:

Username	Password	Access
`user`	`user`	Administrative access (web + API)
`api`	`api`	API access only (no web login)

Change both default passwords immediately after your first login. They are identical on every device of this model until changed, and are publicly documented in this manual. Leaving them unchanged is a significant security risk, particularly if the device is reachable from your office or production network – note in particular that `user`/`user` is itself a full administrative account, not a restricted one. See Section 4.5 for instructions on changing passwords and creating additional accounts.

You may notice a third account named `cloud` in the Users list. It is reserved for the Vectrolink Cloud portal's single-sign-on feature (Section 6.5) and is not meant for direct login – please do not delete or repurpose it, or the "Open Device UI" button in the portal will stop working.

3.4 Network Configuration

After logging in, navigate to the **Network** page to configure how the device should connect to your network:

- **Ethernet** – DHCP (automatic) or static IP address, subnet mask, and gateway.
- **Wi-Fi** – select a network from a scan, or enter SSID/password manually. Wi-Fi can operate in *station* mode (joining your existing network) or *access point* mode (the device hosts its own network), or both simultaneously.

Both Ethernet and Wi-Fi can be active at the same time; the device will respond to Modbus TCP and web requests on whichever interface(s) are reachable.

After changing network settings, the device will apply the new configuration and may briefly become unreachable on its old address while it reconnects. Make a note of the new address (or check your router) before closing the page.

3.5 Quick-Start Checklist

1. Power up the device and connect to it for the first time (Section 3.3).
2. Log in and immediately change all default account passwords.
3. Configure your network connection (Ethernet and/or Wi-Fi).
4. Configure your Modbus RTU bus parameters (baud rate, parity, stop bits) to match your field devices.
5. Add your first register mapping, or enable Transparent mode if no translation is required.
6. Verify communication using the **Manual Read** diagnostic tool before relying on the configured mapping.

Chapter 4

Web Interface Guide

The embedded web interface is the only configuration tool for the device – no desktop software or mobile app is required. This chapter walks through every page of the interface in the order it normally appears in the navigation menu.

4.1 Dashboard

The Dashboard is the landing page after login and gives an at-a-glance overview of device health:

Device Info Device name, serial number, firmware version, and uptime.

Connectivity Current Wi-Fi and Ethernet status, including IP addresses and link state.

Modbus Master Statistics for outgoing Modbus requests: total requests, successful requests, timeout errors, CRC errors, and protocol errors.

Modbus Slave Statistics for incoming Modbus requests: total requests, read requests, write requests, error responses, and active client connections.

Configuration Backup Export and import the entire device configuration as a JSON file.

4.1.1 Configuration Backup

Export Downloads a JSON file containing the complete configuration: all translator mappings, transparent mappings, network settings, and operating modes. The file is named `<device-name>_config_<date>.json`.

Import Restores configuration from a previously exported JSON file. **This overwrites all current mappings and settings, and the device restarts automatically** once the import completes.

> Export a configuration backup before a factory reset, and periodically as part of routine maintenance.

4.2 Translator Mode

This page manages register mappings used in Translator mode.

Enable Translator Master on/off switch for the translation engine.

Mode Global polling strategy applied to mappings: *Cyclic* (periodic polling on a fixed interval), *On-Demand* (a source read is performed only when a client requests the corresponding target register), or *On-Event* (the target is updated only when new data arrives from the source).

Add Translator Opens the mapping editor to create a new mapping.

Reload Configuration Re-applies the current mapping list to the running translator engine without a restart.

Clear All Deletes all mappings. **This action cannot be undone** – export a backup first.

4.2.1 Mapping Fields

Each mapping defines a *source* (where data is read from) and a *target* (where data is written to or made available).

Field	Description
Slave ID	Modbus slave address of the device, 1–247
Register	Starting register address, 0–65535
Port	Physical interface: RS485-1, RS485-2, or Ethernet (TCP)
Protocol	RTU (for RS-485 ports) or TCP (for Ethernet)
Function	Source: Read Coils (FC01), Read Discrete Inputs (FC02), Read Holding Registers (FC03), or Read Input Registers (FC04). Target functions are limited to the same read functions – the target side of a mapping is always read-only from the gateway's perspective.
Data Type	U16, I16, U32, I32, U64, I64, FLOAT32, FLOAT64, or BCD. The number of registers consumed is derived automatically from the type (1 register for 16-bit, 2 for 32-bit, 4 for 64-bit).
Byte Order	BE (big-endian), LE (little-endian), BE-S (big-endian, word-swapped), or LE-S (little-endian, word-swapped) – controls how multi-register values are assembled
Scale / Offset	Numeric transformation applied as $value \times scale + offset$
RTU settings	Baud rate (4800–115200 bps), parity (None/Even/Odd), stop bits (1 or 2) – set independently per source and target if each uses RS-485
TCP settings	IP address and port (default 502) – set independently per source and target if each uses Ethernet

The gateway cannot write to RTU or TCP target field devices. Both the source and target sides of a translator mapping can only be *read* from. If your application requires writing setpoints or commands into a field device through this gateway, this is not currently supported – consult your system integrator about alternative architectures for write/control use cases.

A built-in **Guide** button on this page opens a quick-reference panel summarising these fields directly in the browser.

4.3 Transparent Mode

Transparent mode forwards Modbus requests 1:1 between a client and a target device, without any register remapping or data type conversion. It is the simplest configuration when no translation is needed – for example, exposing an RTU device directly on the TCP network at the same register addresses it already uses.

Enabling Transparent Mode suspends the cyclic Translator Mode polling engine. The two modes are not intended to run simultaneously.

Each transparent mapping defines:

- **Source** – the side of the incoming request to the gateway (the gateway acts as the Modbus slave/server here).
- **Target** – the field device the gateway forwards the request to (the gateway acts as the Modbus master/client here).

The page provides the same Add / Reload Configuration / Clear All actions as Translator Mode.

4.4 Manual Read

Manual Read is a diagnostic tool for reading a register range from a device on demand, without creating a permanent mapping. It is the recommended first step when commissioning a new field device, to confirm wiring, slave address, and register layout before configuring a mapping.

Field	Description
Connection Type	RS485-1 (RTU), RS485-2 (RTU), or Ethernet (TCP)
RTU Configuration	Baud rate, parity, stop bits (8 data bits is fixed for Modbus)
TCP Configuration	IP address and port
Slave ID	1–247
Function / Register / Count	Function code and register range to read

A built-in **Guide** button is available on this page as well.

4.5 User Management

Any account can see and use this page, but what you can do here depends on your account: only `superadmin` can grant admin privileges or edit/delete the built-in `user`/`api`/`cloud` accounts. Every other account can create and manage the additional accounts it creates (up to 5 total), but the table shows those built-in accounts as *System* (no edit/delete controls) rather than hiding the page entirely.

Create User Creates a new account with a username and password, and independently toggleable *Web access* and *API access* permissions. Up to 5 additional user accounts can be created on top of the built-in default accounts (Section 3.3).

Users table Lists existing accounts and provides per-account actions (edit, delete) for the accounts you're allowed to manage.

To change your own password while logged in as any account, use the password-change option in the account menu – this does not require `superadmin` access.

4.6 Network Settings

4.6.1 Wi-Fi Configuration

Field	Description
Mode	AP Only (device hosts its own network), STA Only (device joins an existing network), or AP + STA (both simultaneously)
Enable Wi-Fi	Master on/off switch for the Wi-Fi radio
Scan Networks	Lists nearby Wi-Fi networks for easy selection
Saved Networks	Up to 5 networks can be stored, each with its own priority (0 = highest); the device automatically connects to the highest-priority network that is available
IP Configuration	DHCP (automatic) or static IP / netmask / gateway / DNS

4.6.2 Ethernet Configuration

Ethernet connectivity is always enabled and cannot be turned off from the interface. As with Wi-Fi, IP addressing can be set to DHCP or a static IP / netmask / gateway / DNS configuration.

> Wi-Fi and Ethernet can both be active at the same time. The device will respond to Modbus TCP and web requests on whichever interface(s) currently have a valid IP address.

After changing any network setting, click **Save Network Settings** to apply the change. The device may briefly become unreachable at its previous address while the new configuration takes effect.

4.6.3 Automatic Firmware Updates

A checkbox labeled **Allow firmware update** appears in the sidebar, above the Restart button, on every account – it is not restricted to administrators. It is **enabled by default**.

When enabled (default) The device automatically downloads and installs firmware updates published by Vectrolink through the Cloud update service (hawkBit), with no action required from you.

When disabled The device stops downloading and applying those updates, but otherwise keeps working exactly as before – Modbus translation, remote access, and every other function are unaffected. You can still install a firmware file manually if needed, and you can re-enable automatic updates at any time.

Turning this off is entirely optional, not a requirement for normal operation. That said, **we recommend leaving it enabled**: it is the simplest way to keep receiving security fixes, bug fixes, and new features as they are released, without having to track firmware versions yourself. Consider disabling it only if you have a specific reason to control precisely when updates land on a device – for example, a maintenance window requirement in your own change-management process.

4.6.4 Danger Zone: Factory Reset

A **Factory Reset** button is available in the sidebar navigation, next to Restart. This has the same effect as the push-button procedure (Section 2.4), triggered from the browser instead, and

asks for confirmation before proceeding. If you are locked out of every account (Section 3.3), this button cannot help you, since it still requires logging in first; use the physical push-button instead.

Chapter 5

Modbus Protocol Reference

5.1 Supported Function Codes

Code	Name	Reading (TCP)	Reading (RTU slave)
FC01	Read Coils	Supported	Supported
FC02	Read Discrete Inputs	Supported	Supported
FC03	Read Holding Registers	Supported	Supported
FC04	Read Input Registers	Supported	Supported
FC06	Write Single Register	Not supported	Supported (writes to internal cache only)
FC10 (16)	Write Multiple Registers	Not supported	Supported (writes to internal cache only)

Write support (FC06 / FC10) is only available on the RS-485 (RTU) slave interface, and writes go to the device's internal register cache – they are **not** forwarded to a downstream RTU or TCP field device through a translator or transparent mapping. The Modbus TCP (Ethernet) slave interface is read-only. Do not design a control/setpoint-writing application around this gateway without first confirming current write capabilities with your system integrator.

5.2 Modbus Roles

The device can simultaneously act as:

- A **Modbus TCP slave (server)** – responding to read requests from a SCADA/HMI client on the network.
- A **Modbus RTU slave** – responding to read/write requests from an RTU master on the RS-485 bus.
- A **Modbus RTU master (client)** – actively polling field devices on the RS-485 bus.
- A **Modbus TCP master (client)** – actively polling other Modbus TCP devices on the network, when a mapping's source or target is configured for Ethernet.

5.3 Addressing

- Slave/unit addresses: 1–247 (standard Modbus range).

- Register addresses: 0–65535 per the configured function code's address space.
- Each device port (RS485-1, RS485-2) operates as an independent Modbus bus with its own transmission parameters.

5.4 Data Types

The translation engine can interpret raw Modbus registers as the following data types when building a target value from a source register range:

Type	Registers	Description
U16	1	Unsigned 16-bit integer
I16	1	Signed 16-bit integer
U32	2	Unsigned 32-bit integer
I32	2	Signed 32-bit integer
FLOAT32	2	IEEE 754 single-precision floating point
U64	4	Unsigned 64-bit integer
I64	4	Signed 64-bit integer
FLOAT64	4	IEEE 754 double-precision floating point
BCD	Variable	Binary-coded decimal

5.5 Byte Order

Multi-register values can be assembled in four different register/byte orderings, to match the convention used by your field devices:

Code	Meaning
BE	Big-endian – most significant register first, in standard byte order
LE	Little-endian – least significant register first, in standard byte order
BE-S	Big-endian with word-swap
LE-S	Little-endian with word-swap

If a configured mapping produces a value that looks "scrambled" or wildly out of range (but is otherwise updating), the most common cause is a byte-order mismatch between the gateway's setting and the field device's actual encoding. Try the other byte-order options before assuming a wiring or addressing problem.

5.6 Scaling

Numeric values can be linearly transformed between source and target using:

$$value_{\text{target}} = value_{\text{source}} \times scale + offset$$

This is commonly used to convert raw sensor counts into engineering units (e.g., converting a raw temperature register to degrees Celsius).

Chapter 6

Security Notes

6.1 Device Integrity

The device runs only firmware signed by Vectrolink (Secure Boot): modified or foreign firmware is rejected, also when it is uploaded through the web interface or delivered as an update. The configuration and the stored passwords are kept in encrypted memory.

6.2 Encrypted Web Access (HTTPS)

The web interface is served over HTTPS. The device generates its own unique, self-signed TLS certificate the first time it starts – there is no central certificate authority involved, and no internet connection is required for this.

6.2.1 Why Your Browser Shows a Warning

Because the certificate is self-signed rather than issued by a publicly trusted certificate authority, your browser will show a warning similar to *"Your connection is not private"* or *"This site is not secure"* the first time you connect to the device. **This is expected behaviour for this class of device** – the same thing happens with most routers, managed switches, and industrial IP devices that you configure over your local network.

To proceed:

1. Click **Advanced** (or equivalent, depending on your browser).
2. Click **Proceed to <device IP> (unsafe)** or **Continue**.

The connection is still encrypted – the warning relates only to the browser being unable to verify the certificate's issuer, not to the strength of the encryption itself.

> If you want to remove this warning permanently across your organisation's computers, your IT department can import the device's certificate into the trusted certificate store of the browsers/computers that need access. Ask your system integrator for the procedure, as this requires access to the device's certificate file and is typically a one-time setup per device.

6.3 Accounts and Passwords

- Change **all** default account passwords immediately after first login (Section 3.3). They are the same on every unit until changed.
- Use strong, unique passwords – they are not subject to any complexity policy enforced by the firmware, so this is your responsibility.

- Create individual accounts for each technician or operator who needs access, rather than sharing one login, so that access can be revoked individually if needed.
- After 5 failed login attempts from the same source, the device temporarily locks out further attempts from it for 5 minutes. This slows down automated guessing but is not a substitute for strong, unique passwords – avoid placing the device's web interface directly on the public internet regardless.

6.4 Network Placement Recommendations

- Place the device on an isolated operational-technology (OT) network segment where practical, separate from general office IT traffic.
- Do not expose the device's web interface directly to the public internet with port forwarding. If remote access is required, use **Vectrolink Cloud** (Section 6.5) or a VPN provided by your IT department.
- Restrict network access to the device to the systems and personnel that genuinely need it (SCADA/HMI servers, maintenance technicians).

6.5 Remote Access via Vectrolink Cloud

When the device has internet access, its Web UI and REST API can be reached remotely through the Vectrolink Cloud portal, without a VPN and without forwarding any port on your router or firewall. The device only makes an outbound connection to the Cloud relay; no inbound port is ever opened on your network.

From the portal, clicking **Open Device UI** logs you into the device's web interface automatically – the portal signs you in on your behalf using a dedicated, restricted service account, so you are not prompted for the device's own login a second time. This does not replace or bypass individual user accounts on the device itself (Section 3.3); it only skips a redundant login step for someone who has already authenticated to the portal.

> Vectrolink Cloud access is a separate service from the device hardware itself. Ask your Vectrolink representative about enabling it for your account if it is not already active.

6.6 Account Permissions

Accounts can be granted *Web access*, *API access*, or both, independently. Any logged-in account can change network settings, perform a factory reset, and create/manage additional accounts of its own. **Granting admin privileges, and editing or deleting the built-in `superadmin`/`cloud`/`user`/`api` accounts, is restricted to the `superadmin` account only.** See Section 4.5 for details.

Chapter 7

Troubleshooting

7.1 Common Issues

I cannot reach the web interface after changing network settings. Use the push-button (Section 2.4): a short press temporarily re-enables Wi-Fi in station mode for 10 minutes, a double press temporarily creates a Wi-Fi access point for 10 minutes. Either lets you reconnect and review/correct the network configuration.

My browser shows a security warning when opening the device's web page. This is expected – see Chapter 6, Section "Encrypted Web Access (HTTPS)", for an explanation and the steps to proceed safely.

I forgot my account password and cannot log in with any account. There is no password-recovery mechanism. The only way to regain access is a factory reset via a long press of the push-button (10 seconds or more), which erases all configuration, including user accounts, and restores all default account credentials (Section 3.3). Restore your configuration from a backup afterward if you have one (Section 4.1.1).

Firmware upload fails with "Invalid firmware file". You most likely selected a merged/wrapped binary image instead of the raw application `.bin` file. Re-download the correct firmware file from your vendor and confirm it is the plain application image, not a combined flash image.

A mapped register shows a value that updates, but the number looks wrong or "scrambled". This is almost always a byte-order mismatch for multi-register data types (32-bit/64-bit integers or floats). Try the other Byte Order setting (BE/LE/BE-S/LE-S) for that mapping – see Chapter 5, Section "Byte Order".

A mapped register never updates, or reads as zero. Check, in order: (1) the Slave ID matches the field device's configured address, (2) the RTU baud rate/parity/stop bits match the field device exactly, (3) the wiring polarity and, if the vMT-02 is at the physical end of the bus, that the termination jumper (J5/J6, Chapter 2, Section "RS-485 Bus Termination") is fitted, (4) the register address and function code are correct for that device (consult its own Modbus register map documentation), (5) use Manual Read to isolate whether the problem is the mapping configuration or the underlying communication with the device.

Modbus communication appears intermittent or slow under heavy load. Reduce the total number of active cyclic mappings, or increase polling intervals, particularly if many mappings are configured close to the device's stated capacity limits (see Chapter 8).

7.2 Getting Further Help

If an issue persists after the steps above, collect the following before contacting support:

- Firmware version (visible on the Dashboard).
- Device serial number.
- A copy of the **System Logs** (System Administration page, administrator accounts only).
- A description of the affected mapping(s), including source/target configuration.

Chapter 8

Specifications

8.1 Capacity Limits

Resource	Maximum	Recommended working range
Translator mappings	512	64–256
Transparent mappings	256	32–128
Additional user accounts (beyond defaults)	5	–
Saved Wi-Fi networks	5	–
Registers per FC03/FC04 request	125	40–80
Bits per FC01/FC02 request	2000	200–1000

The "Recommended working range" column leaves headroom for retries and momentary traffic spikes. Configurations near the hard maximum are technically supported but leave less margin for response-time consistency under load. If you operate close to these maximums, monitor the Dashboard's Modbus statistics for an increase in timeout or error counts.

8.2 Connectivity

Interface	Specification
RS-485	2 independent channels; 4800–115200 bps, parity None/Even/Odd, 1 or 2 stop bits, 8 data bits
Ethernet	10/100 Mbps, DHCP or static IP
Wi-Fi	802.11 b/g/n 2.4 GHz, built-in antenna, station and/or access point mode, DHCP or static IP
Modbus TCP server	Port 502, up to 4 concurrent clients

8.3 Physical and Electrical

Property	Specification
Power supply	10–24 V DC, less than 3 W
Protection rating	IP20, reverse-polarity protected
Operating temperature	−20 °C to +70 °C
Housing	DIN-rail (35 mm TS), 2-module width
Terminal wire gauge	24–12 AWG
Indicators	1 multicolour status LED (power / activity / cloud) – see Chapter 2, Section "Status LED Indications"
Certifications	CE

8.4 Supported Data Types

U16, I16, U32, I32, U64, I64, FLOAT32, FLOAT64, BCD. See Chapter 5 for details.

8.5 Supported Modbus Function Codes

- Read: FC01 (Read Coils), FC02 (Read Discrete Inputs), FC03 (Read Holding Registers), FC04 (Read Input Registers)
- Write (RS-485 slave interface only, to internal cache): FC06 (Write Single Register), FC10/16 (Write Multiple Registers)

8.6 Account Permissions

Administrator and standard user accounts, with independently toggleable Web and API access – see Chapter 6.

8.7 Security

- Secure Boot: only firmware signed by Vectrolink runs on the device; configuration stored encrypted.
- HTTPS web interface with a per-device, self-signed TLS certificate generated on first boot.
- Password-based authentication with session tokens; temporary lock-out after repeated failed logins.

Chapter 9

API Reference

Everything available in the web interface is also available as a JSON HTTP API, which you can use to integrate the device with your own systems (e.g. a SCADA platform, a provisioning script, or a fleet management tool). This chapter is intended for system integrators and developers; day-to-day operators can use the web interface described in Chapter 4 instead.

9.1 Connecting

All endpoints are served over HTTPS. Because the device uses a self-signed certificate (Chapter 6), your HTTP client or script will need to either trust that specific certificate or disable certificate verification for this host, depending on what your tooling allows and your organisation's policy.

9.2 Authentication

1. Obtain a session token by logging in:

   ```
   POST /api/auth/login
   {"username": "<username>", "password": "<password>"}
   ```

   On success, the response contains a session token.

2. Include the token on every subsequent request:

   ```
   Authorization: Bearer <token>
   ```

3. Some endpoints require an account with administrator-level access; a few (firmware upload, system logs) require the device's single highest-privilege account specifically. See Section 3.3 for the accounts available out of the box, and create dedicated API-access accounts for integration use rather than reusing an interactive login (Section 4.5).

> If you only need machine-to-machine API access (no need to log into the web UI with that account), grant *API access* without *Web access* when creating the account, and use a username/password your integration owns exclusively.

9.3 Configuration & Status

Endpoint	Description
`GET /api/config`	Full configuration (mappings, modes, network) as JSON. The same data the web UI's "Export" feature downloads.
`POST /api/config`	Replace the full configuration. The device restarts automatically once applied.
`GET /api/status`	System status: uptime, free memory, Modbus master/slave statistics.
`POST /api/system/restart`	Restart the device.

9.4 Translator Mappings

Endpoint	Description
`GET /api/mappings`	List mappings (supports pagination).
`POST /api/mappings`	Add a mapping.
`PUT /api/mappings`	Edit a mapping by index.
`POST /api/mappings/delete`	Delete a mapping by index.
`POST /api/mappings/clear`	Delete all mappings.
`POST /api/translator/enable`	Enable/disable the translator engine.
`POST /api/translator/mode`	Set the global mode (0=cyclic, 1=on-demand, 2=on-event).
`POST /api/translator/reload`	Reload mapping configuration without restarting.
`GET /api/translator/stats`	Live per-mapping statistics.

See Section 4.2.1 for the meaning of each mapping field (slave ID, register, data type, byte order, scale/offset, etc.).

9.5 Transparent Mappings

Endpoint	Description
`GET /api/transparent_mappings`	List (supports `offset`/`limit`).
`POST /api/transparent_mappings`	Add.
`PUT /api/transparent_mappings`	Edit.
`DELETE /api/transparent_mappings`	Delete.

9.6 Manual Read

Endpoint	Description
`GET /api/manual_read`	On-demand register read.

9.7 Network

Endpoint	Description
`GET /api/network`	Read network configuration.
`POST /api/network`	Write network configuration.
`GET /api/wifi/scan`	Scan for nearby Wi-Fi networks.
`GET /api/wifi/networks`	List saved Wi-Fi networks.
`POST /api/wifi/networks`	Add a saved network.
`DELETE /api/wifi/networks/*`	Remove a saved network.

9.8 Users & Sessions

Endpoint	Description
`POST /api/auth/login`	Authenticate, returns a session token.
`POST /api/auth/logout`	Invalidate the current session.
`GET /api/auth/session`	Validate/inspect the current session.
`GET /api/auth/users`	List accounts.
`POST /api/auth/users`	Create an account.
`PUT /api/auth/users`	Edit an account.
`DELETE /api/auth/users`	Delete an account.
`POST /api/auth/password`	Change a password.