# SyncTide

## Administrator Manual

System Configuration & Administration Guide

Version 1.4.1 — June 2026

# Table of Contents

(Use Insert > Table of Contents in Word/LibreOffice to auto-generate)

# 1. Introduction

This manual is intended for SyncTide administrators. It covers all administrative functions: user management, equipment configuration, system settings, messaging gateways, and platform maintenance.

Prerequisites: Admin-level access to SyncTide.

## 2. User Administration

Navigate to Users from the navigation bar (admin only).

### 2.1 Creating Users

1. Click 'Add New User'
2. Enter username (required) and password (required)
3. Set the role: Admin, Operator, or Viewer (page access follows the role)
4. Optionally restrict access to specific equipment categories or devices
5. Click Create

### 2.2 Managing Users

The user list shows all accounts with their role (colour-coded), status, and permissions.

- Click the edit button to modify a user's profile, role, permissions, or equipment whitelist
- Toggle Active/Inactive to enable or disable an account
- Use the password section to reset a user's password
- Click Delete to permanently remove a user (requires confirmation)

*Note: You cannot delete your own account or the last active admin account.*

### 2.3 Role Permissions

| Feature | Viewer | Operator | Admin |
|---|---|---|---|
| **Dashboard / Explorer** | View | View | View + Export |
| **Alarms** | View + Acknowledge | View + Acknowledge | Full control |
| **Reports** | View + Download | View + Download | Full control |
| **Messaging Contacts** | — | Create/Edit/Delete | Full control |
| **Messaging Rules** | — | Create/Edit/Delete | Full control |
| **Messaging Gateways** | — | View | Full control |
| **Equipment Config** | — | Create/Edit | Full control |
| **Users** | — | — | Full control |
| **Configuration / Settings** | — | — | Full control |

### 2.4 Equipment Whitelist

Each user can be restricted to specific equipment:

- By Category: User only sees devices in the selected categories (including sub-categories)
- By Device: User only sees specifically listed devices

- Empty whitelist: User sees all devices

The whitelist applies across Dashboard, Reports, Map, and all data endpoints.

# 3. Equipment Configuration

Navigate to the Equipment page from the navigation bar. It has four tabs: Metadata, Tag Mapping, Monitoring & Alarms, and Communication.

## 3.1 Adding Devices

Use the 'Add device' control at the top of the page to register a new device. You set its code, name, alarm category, and the ingestion protocol (CSV, Modbus TCP, OPC UA, IEC 60870-5-104, MQTT/Sparkplug B). You can change the protocol later from the Communication tab.

## 3.2 Device Metadata

Select a device from the dropdown. The Metadata tab lets you edit:

- Equipment name and device code
- Equipment group (used for filtering and organisation)
- Model and serial number
- Latitude and longitude (for map positioning)
- Alarm category assignment (hierarchical)

## 3.3 Communication

The Communication tab configures how SyncTide reads data from the device:

| Protocol | Configuration | Tag addressing |
|---|---|---|
| **CSV** | Optional custom folder_path (blank = raw_data/<code>/) | Via Tag Mapping |
| **Modbus TCP** | host, port, unit_id, timeout_ms, address_offset | 40001 or hr:/ir:/di:/coil:, data_type int16/uint16/int32/uint32/float/bool |
| **OPC UA** | endpoint_url, optional username/password | ns=2;s=TagName or ns=2;i=1234 |
| **IEC 60870-5-104** | host, port (2404), common_address, originator_address | IOA-addressed points (decoded per type, e.g. M_BO_NA_1) |
| **MQTT / Sparkplug B** | broker host, port, topic/namespace, credentials | Sparkplug metric names / MQTT topics |

Each non-CSV device has its own poll interval (1-86400 seconds). The 'Test connection' button probes the device without persisting anything. Polling Modbus TCP, OPC UA, IEC 60870-5-104, or MQTT/Sparkplug B requires a licence that includes the 'protocol_ingestion' module; CSV-only customers are unaffected.

## 3.4 Tag Mapping

The Tag Mapping tab links raw CSV tags to standardised system tags:

6. Each row shows an equipment tag name (from the CSV files)
7. Map it to a System Tag (standardised name + unit)
8. Set a scale factor for unit conversion (default: 1.0)
9. Toggle active/inactive to include or exclude tags from monitoring

*Note: Only active, mapped tags count towards the license tag limit.*

## 3.5 Monitoring & Alarms

The Monitoring tab configures alarm detection for each device:

### Communication Timeout

Set the maximum time a device can go without sending data before it is considered offline. Configure in Days, Hours, and Minutes.

- Communication Lost Alarm Enabled: When checked, the system creates an alarm event when the device goes stale. The alarm auto-clears when data resumes.

### Alarm Rules per Tag

For each mapped system tag, configure:

- Alarm Enabled: Toggle alarm detection on/off
- Value Type: Numeric (threshold comparison) or Boolean (true/false)
- Condition Operator: <, <=, =, >, >=, != (numeric only)
- Threshold Value: The setpoint that triggers the alarm (numeric only)

The latest measurement value and timestamp are displayed next to each rule for reference.

*Note: Alarms only trigger for measurements received AFTER the alarm rule was created or last modified.*

# 4. System Configuration

## 4.1 Runtime Configuration

Configure platform paths and ingestion settings:

- Raw Data Folder: Where CSV files are read from
- Reports Output Folder: Where generated reports are saved
- Report Templates Folder: Where Excel templates are stored
- Ingestion Interval: How often (in seconds) the system checks for new CSV files (minimum: 15s)

## 4.2 System Tags

Manage the standardised tag library:

- Add new tags with name and unit of measurement
- Edit existing tags
- Deactivate unused tags

System tags are the standardised names used across all devices via tag mapping.

## 4.3 Alarm Categories

Build a hierarchical category tree for organising devices:

- Create categories with name, icon, and optional parent category
- Assign devices to categories in Equipment Configuration
- Categories are used for the Asset Tree display and category-scoped alarm rules

## 4.4 License Management

View license status and upload new license files:

| Field | Description |
|---|---|
| **Customer** | Licensed organisation name |
| **Tier** | Basic (10 tags), Starter (50), Standard (250), Professional (500), Enterprise (1 000), Industrial (2 500), Unlimited |
| **Modules** | Licensed features: base, reports, messaging, protocol_ingestion |
| **Tags Used** | Current mapped tag count vs. maximum allowed |
| **Maintenance Expiry** | Date until which updates and support are included |
| **MAC Binding** | License is locked to the server's network adapter MAC address |

To install a new license, upload the .lic file in the License tab.

# 5. Messaging Gateway Configuration

Navigate to Messaging Center > Configuration to manage gateways.

## 5.1 Gateway Types

| Type | Use Case | Required Configuration |
|---|---|---|
| **Teltonika RUT241** | SMS via LTE router | Host IP, username, password, modem ID |
| **Twilio** | WhatsApp messages | Account SID, Auth Token, From number |
| **Telegram** | Telegram bot messages | Bot Token (from @BotFather), Parse mode |
| **SMTP** | Email notifications | SMTP host, port, TLS, username, password, from address |
| **Generic HTTP** | Custom webhook/API | URL, method, headers, body template |

## 5.2 Adding a Gateway

10. Click 'Add Gateway' in the Configuration tab
11. Select the gateway type
12. Enter the required configuration fields
13. Set as Active and optionally as Default
14. Save the gateway
15. Use the 'Test Send' feature to verify connectivity

## 5.3 Telegram Bot Setup

16. Open Telegram and message @BotFather
17. Send /newbot and follow the prompts to create a bot
18. Copy the bot token (format: 123456:ABC-DEF...)
19. Add the bot to your group chat
20. Send a message in the group, then call the getUpdates API to find the chat_id
21. Configure the gateway with the bot token and use the chat_id as the contact's Telegram Chat ID

## 5.4 SMTP Email Setup

For Gmail, use an App Password (not your account password):

22. Go to Google Account > Security > 2-Step Verification > App Passwords
23. Generate a new app password for 'Mail'
24. Use smtp.gmail.com, port 587, TLS enabled, your Gmail as username, and the app password

## 5.5 Escalation Flow

When an alarm triggers and matches an alarm rule:

25. The system queues messages for Level 1 contacts in the assigned escalation list
26. Messages are sent with an ACK token for acknowledgment
27. If no acknowledgment is received within the response timeout (default: 300 seconds), the system escalates to Level 2
28. Escalation continues through all levels, including parent list members if configured
29. Escalation stops when someone acknowledges or the maximum escalation level is reached
30. The cooldown period prevents repeat notifications for the same ongoing alarm

# 6. Data Ingestion

SyncTide supports several ingestion modes, configured per device on the Communication tab of the Equipment page:

- Protocol polling (Modbus TCP, OPC UA, IEC 60870-5-104, MQTT/Sparkplug B) — SyncTide connects to the device or broker and reads each configured register/NodeId/point/metric at a configurable interval. One worker process per protocol ensures a misbehaving driver cannot affect the others.
- CSV ingestion — drop files into the configured raw-data folder (locally or via FTP); the ingestion worker picks them up and imports them.

*Note: Protocol polling requires a licence that includes the 'protocol_ingestion' module.*

## 6.1 CSV File Format

SyncTide ingests CSV files with the following requirements:

| Column | Required | Description |
|---|---|---|
| **time_stamp** | Yes | Timestamp of the measurement (multiple formats supported) |
| **tag_name** | Yes | Name of the measured parameter |
| **value** | Yes | Numeric measurement value |
| **unit** | No | Unit of measurement (optional) |

Supported delimiters: comma, semicolon, pipe, tab (auto-detected).

Supported timestamp formats: ISO 8601, DD/MM/YYYY HH:MM:SS, and many other common formats.

## 6.2 File Placement

Place CSV files in the configured Raw Data Folder. The ingestion worker automatically picks up new files at the configured interval.

- Files are tracked by SHA-256 hash — the same file is never imported twice
- Duplicate measurements (same device + timestamp + tag) are automatically skipped
- Invalid rows (bad timestamps, non-numeric values) are dropped with logging

## 6.3 Folder Structure

Organise files by device using subfolders:

- raw_data/DeviceCode_1/file1.csv
- raw_data/DeviceCode_2/file2.csv

The folder name is used as the device code. Devices are created automatically on first file import.

# 7. Backup & Maintenance

## 7.1 Database Backup

Use PostgreSQL pg_dump for database backups:

```
pg_dump -U synctide -d synctide_db > backup_YYYYMMDD.sql
```

Schedule regular backups using Windows Task Scheduler or a cron-equivalent.

## 7.2 Log Files

SyncTide maintains rotating log files in the logs/ directory:

| Log File | Contents | Rotation |
|---|---|---|
| **backend.log** | API server logs | 5 MB x 5 backups |
| **messaging.log** | Messaging engine logs | 5 MB x 5 backups |
| **health_monitor.log** | Service health monitor | 5 MB x 5 backups |
| **ingestion.log** | CSV ingestion worker | 10 MB x 3 backups |
| **modbus_poller.log** | Modbus TCP poller | 5 MB x 5 backups |
| **opcua_poller.log** | OPC UA poller | 5 MB x 5 backups |

## 7.3 Service Management

SyncTide runs as eleven NSSM-managed Windows services:

- SyncTideBackend — API server (FastAPI), also serves the web UI at /ui
- SyncTideAlarms — real-time alarm evaluator
- SyncTideIngestion — CSV/FTP file ingestion worker
- SyncTideModbus — Modbus TCP poller
- SyncTideOPCUA — OPC UA poller
- SyncTideIEC104 — IEC 60870-5-104 poller
- SyncTideMQTT — MQTT/Sparkplug B subscriber
- SyncTideProxy — Caddy reverse proxy serving the app + UI on the LAN
- SyncTideTelegramInbound — inbound Telegram acknowledgment listener
- SyncTideHealthMonitor — service health monitor
- SyncTideBackup — scheduled database/volume backups
- Use services.msc or PowerShell (Start-Service, Stop-Service, Restart-Service) to manage

NSSM automatically restarts a crashed service. The health monitor watches service state and surfaces failures.