



# SyncTide

## Administrator Manual

System Configuration & Administration Guide

Version 1.6.0 — April 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 User Admin from the sidebar menu.

### 2.1 Creating Users

1. Click 'Add New User'
2. Enter username (required) and password (required)
3. Set the role: Admin, Operator, or Viewer
4. Select allowed pages from the multi-select (auto-filtered by role)
5. Optionally restrict access to specific equipment categories or devices
6. 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	View	View	View + Export
Reports	View + Download	View + Download	Full control
Messaging Contacts	View	Create/Edit/Delete	Full control
Messaging Rules	View	Create/Edit/Delete	Full control
Messaging Gateways	View	View	Full control
User Admin	—	—	Full control
Equipment Config	—	—	Full control
System Config	—	—	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 Equipment Configuration from the sidebar.

### 3.1 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)

### 3.2 Tag Mapping

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

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

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

### 3.3 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	Starter (100 tags), Professional (500), Enterprise (2000), Unlimited
Modules	Licensed features: base, reports, sms
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

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

### 5.3 Telegram Bot Setup

17. Open Telegram and message @BotFather
18. Send /newbot and follow the prompts to create a bot
19. Copy the bot token (format: 123456:ABC-DEF...)
20. Add the bot to your group chat
21. Send a message in the group, then call the getUpdates API to find the chat\_id
22. 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):

23. Go to Google Account > Security > 2-Step Verification > App Passwords
24. Generate a new app password for 'Mail'
25. 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:

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



## 6. Data Ingestion

### 6.1 CSV File Format

SyncTide ingests CSV files with the following requirements:

Column	Required	Description
<b>time_stamp</b>	Yes	Timestamp of the measurement (multiple formats supported)
<b>tag_name</b>	Yes	Name of the measured parameter
<b>value</b>	Yes	Numeric measurement value
<b>unit</b>	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
<code>backend.log</code>	API server logs	5 MB x 5 backups
<code>messaging.log</code>	Messaging engine logs	5 MB x 5 backups
<code>supervisor.log</code>	Windows service supervisor	5 MB x 5 backups
<code>ingestion.log</code>	Data ingestion worker	10 MB x 3 backups

### 7.3 Service Management

SyncTide runs as Windows services:

- SyncTideBackend — API server (FastAPI)
- Use `services.msc` or PowerShell (`Start-Service`, `Stop-Service`, `Restart-Service`) to manage

The platform supervisor automatically restarts crashed services (up to 5 restarts in a 5-minute window).