

GETTING STARTED

Logs and diagnostics data

Every log MergenHub writes: file logs, event log, audit log, historian database, installer log; retention and locations.

Online: mergenhub.envest.com.tr/docs/logs

ON THIS PAGE

Overview	Historian data
Application file log	Device diagnostics and packet traces
Event log	Retention settings
Audit log	Sending logs to support
Alarm history	

MergenHub keeps several kinds of logs, each with its own purpose, location and retention. All of them live under the data folder `C:\ProgramData\MergenHub`.

Overview

LOG	WHERE	WHAT IS IN IT	RETENTION	WHERE TO VIEW
Application file log	<code>logs\mergenhub-YYYYMMDD.log</code>	Everything the core process logs: startup, driver connections, errors, stack traces, API requests	One file per day; old files pruned automatically	Any text editor; attach to support requests
Event log	<code>events.db</code> (SQLite)	Operator-facing events: device connected/lost, timeouts, service start/stop, OPC UA sessions, alarms raised	7 days by default (<i>Settings › Retention</i>)	<i>... › Event Log</i> in the web UI, with filter, search and <i>Export to text</i>
Audit log	<code>audit.db</code>	Who changed what: every configuration write (POST/PUT/DELETE), OPC UA and REST writes to tags, logins, MCP tool calls, license actions	90 days by default	<i>Settings › Audit</i> (chip filters by category, user, time)
Alarm history	inside the project store	Every alarm transition: raised, acknowledged, cleared, by whom	90 days by default	<i>Alarms › History</i>
Historian	<code>logs.db</code> (SQLite) or your ODBC database	Tag values recorded by log groups	Until you delete or downsample	<i>Historian › Trend</i> , CSV/Excel export, OPC UA HistoryRead
Device diagnostics	in memory	Raw request/response frames (hex) per device, last error, timing	Rolling buffer	<i>Device › Diagnostics</i> ; Wireshark-style trace export

LOG	WHERE	WHAT IS IN IT	RETENTION	WHERE TO VIEW
Installer log	%TEMP%\MergenHub-Setup.log	Every installer step, service and firewall commands	Until you delete it	Text editor
Windows Event Viewer	Application log, source MergenHub	Service lifecycle, unhandled crashes	Windows policy	eventvwr.msc

The Event Log window in MergenHub displays a list of events. The columns are ZAMAN (Time), SEVİYE (Level), KAYNAK (Source), and MESAJ (Message). The events are filtered by level (Bilgi, Uyarı) and source (ChannelWorker, ConfigApi, OpcUaServerService, Kestrel, ScanEngineService, MergenHub). The messages include connection status, login attempts, configuration changes, and server listening events.

The Event Log window – filter by level, search, export, and the Application Report button

Application file log

The core writes a rolling text log to `C:\ProgramData\MergenHub\logs\`. Each line has a timestamp, level (`INF` , `WRN` , `ERR`), the source component and the message. Typical entries:

```
2026-09-05 10:14:02.117 INF Web API listening on http://0.0.0.0:8090
2026-09-05 10:14:03.402 INF OPC UA server started: opc.tcp://0.0.0.0:48010/MergenHub
2026-09-05 10:14:05.930 INF ChannelWorker Connected: Pumping_Station.PLC_1
2026-09-05 10:20:41.008 WRN ModbusTcp Read timeout 10.0.0.5:502 unit 1 (block 40001..40064),
retry 1/3
2026-09-05 10:20:44.012 ERR ChannelWorker Device Pumping_Station.PLC_1 marked Bad: 3 consecutive
failures
```

Settings › *Retention* controls how many days are kept. For a support case send the file of the day the problem happened.

Event log

Events are what an operator needs to see without reading log files: connection state changes, timeouts, service restarts, OPC UA client sessions, configuration reloads, licence/trial messages. Open it from the top-right ... menu › **Event Log**.

- Filter **All / Warning / Error**, free-text search, pause auto-refresh.
- **Export to text** saves the current view.
- **Application Report** builds a single text file with version, settings summary, channel/device health and the last events — the fastest thing to attach to a support ticket.
- Events are persisted in `events.db` for the configured number of days (default 7) and survive restarts.

Audit log

Every change made through the web UI, the REST API, OPC UA writes or an MCP tool is recorded with user, IP, time, action and target. Open *Settings* › *Audit*. Examples of what you will find:

- `channel.create`, `device.update`, `tag.delete`, `project.import`
- `tag.write` from OPC UA or REST with old and new value
- `user.login`, `user.login_failed`, `user.password_change`
- `license.activate`, `license.release`, `settings.update`

Retention is 90 days by default (*Settings* › *Retention*). Audit records are never editable from the UI.

Settings › Audit – filter chips by category, user and time; every configuration change is listed

Alarm history

Every alarm transition (raised, acknowledged, cleared) with timestamp, value, user and comment is kept for the alarm-history retention (default 90 days) and shown under *Alarms > History*. It is also available to OPC UA Alarms & Conditions clients.

Historian data

Log groups write to `logs.db` (SQLite) by default or to any ODBC database (SQL Server, MySQL/MariaDB, PostgreSQL, Oracle). When the target is unreachable, records are buffered on disk (**store-and-forward**) and written later. Trends, downsampling and CSV/Excel/PNG export are in the *Historian* module; see [Historian](#).

Device diagnostics and packet traces

Select a device and open **Diagnostics**: the last request/response frames in hex, byte counts, timing and the last error text. For cache-based protocols (DNP3, IEC 104, IEC 61850) the raw TX/RX tap shows the actual link traffic. A trace can be saved for analysis. See [Troubleshooting](#).

Retention settings

Settings > Retention:

SETTING	DEFAULT
Event log days	7
Audit log days	90
Alarm history days	90
File log days	rolling, automatic

MergenHub
OPC UA Gateway - v3.1.19

Ayarlar

24/24 aktif tag Deneme 24/500

PROJE +

- Bağlantılar
 - Simulation Examples 24
 - Functions 24
- Ekentiler
 - Virtual Tag'ler
 - Tag Kısayolları
 - Alarmlar
 - Veri Logları
 - Data Bridge
 - MCP (AI)

admin
Root (super-admin)

TR TR

OPC UA SUNUCU

- OPC UA Sunucu
- OPC UA Kullanıcıları
- Güvenilen Client'lar
- Sunucu Sertifikası

WEB & BAĞLANTI

- Web & REST API
- Data Bridge

BİLDİRİMLER

- E-posta
- SMS
- İletişim Merkezi

GÖRÜNÜM

- Marka

SİSTEM

- Lisans
- Denetim
- Saklama**
- Servisler

ERİŞİM

- Kullanıcılar

Detaylı yardım

Saklama

Loglar/geçmiş verilen günden eski olunca sistem OTOMATİK siler (saatlik). 0 = süresiz sakla.

Denetim Günlüğü - 7 kayıt Kim ne yaptı (audit.db) — güvenlik izi	90	≈ 3 ay
Olay Günlüğü - 10 kayıt Sistem/iletişim olayları (events.db)	7	7 gün
Alarm Geçmişi - 0 kayıt Geçmiş alarm olayları (raise/clear/ack)	90	≈ 3 ay

Veri Logları (historian) kendi saklama süresini her log grubunda ayrı tutar.

Kaydet Şimdi Temizle

0 gidersen o günlük hiç silinmez.

Settings > Retention – how long events, audit and alarm history are kept

Sending logs to support

1. ... > *Event Log* > *Application Report* — save the file.
2. Add the day's `logs\mergenhub-YYYYMMDD.log`.
3. For a device problem add the *Diagnostics* trace of that device.
4. Send them through the customer portal (*Support*) or by e-mail.