



News

01.09.2026

Weintek HMIs Achieve EN 18031-1 Certification

Author

Weintek HMIs Achieve EN 18031-1 Certification



As the Industrial Internet of Things becomes more deeply connected, Weintek continues to treat product cybersecurity as a core part of its R&D approach, working to give industrial customers worldwide a dependable line of defense.

With the EU tightening cybersecurity requirements under the revised Radio Equipment Directive (RED), Weintek's wireless products have now passed testing and received EN 18031-1 certification. Beyond meeting the EU rules that take effect from August 2025, this reflects Weintek's ongoing commitment to device protection and resilience as cyber threats continue to grow.

What EN 18031-1 Certification Means

EN 18031-1 is a harmonised EU standard supporting the cybersecurity provisions of the RED,

setting out baseline security requirements for internet-connected radio equipment. It gives manufacturers a recognized technical path to demonstrate regulatory compliance.

Devices tested and verified under EN 18031-1 gain stronger protection in two key areas:

- **Network resilience:** keeping devices from disrupting normal network operation or being used as an entry point for attacks, helping protect the wider network.
- **Efficient use of communication resources:** preventing misuse or excessive consumption of network resources so that industrial communication stays stable and reliable.

Certified Weintek Products

The following wireless-capable Weintek products now carry EN 18031-1 certification:

- **cMT X series with the [M02 WiFi module](#):** adds WiFi connectivity to cMT X HMIs without compromising on cybersecurity.
- **Models with built-in WiFi:** including the [cMT-SVR-200/202](#) and [cMT-G02X](#).

Weintek applies the same high security standards across its entire lineup, whether devices connect over WiFi or wired Ethernet — all in line with EN 18031-1 requirements for industrial data protection:

- [cMT X Advanced Series](#)
- [cMT X Standard Series](#)
- [cMT X Basic Series](#)
- [cMT X Headless Series](#)
- [cMT X Web Panel](#)
- [cMT Viewer Panel](#)
- [cMT X Handheld Series](#)
- [cMT Headless Series](#)

OS Update: Five Security Improvements

To align with EN 18031-1, Weintek has rolled out a security-hardening update for its OS (V20251118 and later), built around a "secure by default" approach:



1. **Stronger login authentication:** a mandatory secure-password setup on first use, plus tighter account controls across system levels to remove weak-password vulnerabilities from the start.
2. **System hardening:** unused FTP server functions and background services are now disabled by default, with streamlined network transmission to reduce the attack surface.
3. **Stronger encryption:** default use of TLS 1.2 or later for encrypted communication, plus updated legacy protocol settings for better data privacy on site.
4. **Secure device identity:** improved generation and storage of device keys, giving each unit a unique, secure digital identity for more reliable authentication.
5. **Controlled-environment safeguards:** dedicated risk-management measures for devices deployed in controlled industrial network settings.

Weintek's Ongoing Compliance Efforts

This certification reflects Weintek's continued investment in secure product design and testing, and gives customers the technical documentation needed to support exports to the EU market. Users are encouraged to update to the latest OS as soon as possible for a stronger level of protection.

For more on product certifications, see the [Download](#) section and the Declaration of Conformity (DoC) for each product.

[Open the booklet / download PDF](#)