Critical Product Security Information for Installers, Commissioning Engineers and Users

VESDA® E™

Intelligent VESDA-E VEP, VEU and VEA Series Detectors

WARNING: Failure to comply with the requirements below exposes the system to malicious interference which could disable alarm reporting

Commissioning Requirements

- All wiring and connection ports must be secured against unauthorized access.
- Ethernet and Wi-Fi ports must ONLY be connected to networks which are secure and physically or logically separate from business IT infrastructure.
- Any provision of remote access to Intelligent VESDA-E detectors must be subjected to a full cyber security risk assessment and regular review.
- WPA-2 encryption must be used whenever Wi-Fi is enabled.
- Restrict access to Intelligent VESDA-E detectors to authorized personnel only.
- Passwords must be chosen in line with the guidelines in the detector user guide and provided to trusted users only.
- Default PIN codes must be changed as part of the initial configuration

System Maintenance Requirements

- Do NOT use the USB port for long-term monitoring or allow it to be permanently wired to building infrastructure. It is only to be used for configuration and maintenance by authorized personnel.
- If a detector requires firmware upgrade, ensure that the upgrade package is genuine and obtained directly from the manufacturer.