Supplement to the Radio Equipment Directive 2014/53/EU — Compliance with Articles 3(3)(d) and 3(3)(e) under Delegated Regulations (EU) 2022/30 and 2025/138

Introduction

This supplement contains the necessary information set out in Articles 3(3)(d) and 3(3)(e) of the Radio Equipment Directive 2014/53/EU. The provisions require that:

- (d) Products do not harm the network or its operation, and not misuse network resources.
- (e) Products make sure that personal data and privacy of the user and owner are protected.

Without a PIN, users will not be able to start the related applications. The PIN protection method is used consistently across all relevant Fluke Reliabilty devices and products.

Set PIN (on first use, after factory reset, or production update)

1. When device is initially switched on, a hint to create a PIN is shown.
2. Enter a 4-digit PIN.
3. After the PIN is entered, the user must enter it again to confirm.
4. If both entries match, the PIN is saved and the device PUK is shown.
   - Save the 8-digit device PUK in a safe place, as it is required to recover the device if the PIN is forgotten.

   Continue to log into the application.
5. If the entries do not match, an error message is shown, and the user must repeat the process.

Log into the Application

1. When in the login screen, enter the 4-digit PIN.
2. If the PIN is incorrect:
   - A maximum of 3 attempts is permitted
   - After 3 failed attempts, PIN entry will be temporarily blocked for 1 minute
   - After the timeout period, the attempt counter will reset, and you can try to log in again.

Note: PIN entry is not required when resuming from sleep mode.

Change PIN

1. Within the application, select the item ***Change PIN***.
2. A hint to enter current PIN is shown.
3. If the PIN matches the current PIN, user will be requested to enter and confirm a new PIN.
4. If the maximum of 3 attempts to enter the current PIN is exceeded, PIN entry will be temporarily blocked for 1 minute.

PIN recovery

1. If the user forgets the PIN, select the item ***Forgot PIN*** within the application.
2. User will be requested to enter the device PUK, which was shown when PIN was initially created.
3. If the PUK is correct, user can now set a new PIN.

PN 6105682 - English

PN 6105682 08 2025

Security guidelines

- Do not share your PIN with others unless necessary for use by different teams.
- Avoid easy to guess PINs.
- Change your PIN regularly to enhance security.
- If you suspect a security breach, disconnect the device from Wi-Fi immediately and change your PIN as soon as possible.
- **Keep the PUK in a safe place, as it will be needed to reset the device PIN in case you forget it.**

Personal security information

- To protect personal data and privacy, a PIN and PUK system has been implemented to restrict unauthorized access.
- The devices use these interfaces: Wi-Fi, RFID, Bluetooth, Camera, and USB. These interfaces enable wireless communication, data transfer, identification, image capture, and peripheral connection.
- The Factory Reset function returns the device to its original factory state. It erases user data and settings. It maintains critical system data, license files, identity, and calibration information.
- The devices are equipped with components such as cameras, microphones, USB-C and USB-B ports, and Bluetooth interfaces, which may process or transmit personal data and therefore have implications for user privacy under Article 3(3)(e) of Directive 2014/53/EU.
- PT Device Viewer is a software tool that mirrors the current device display to a PC monitor via Wi-Fi or USB. To safeguard user privacy and prevent unauthorized access, the connection is controlled by an ON/OFF toggle located on the device itself, and screen sharing is only accessible after the user has logged in. Screen sharing is initiated exclusively by the user. This makes sure that the content is transmitted securely and intentionally.