SD03405S/04/EN/02.25-00
71753777
2025-12-23

Special Documentation
Security Manual
Field Xpert

Universal, high-performance tablet PC for device configuration

Endress+Hauser
People for Process Automation

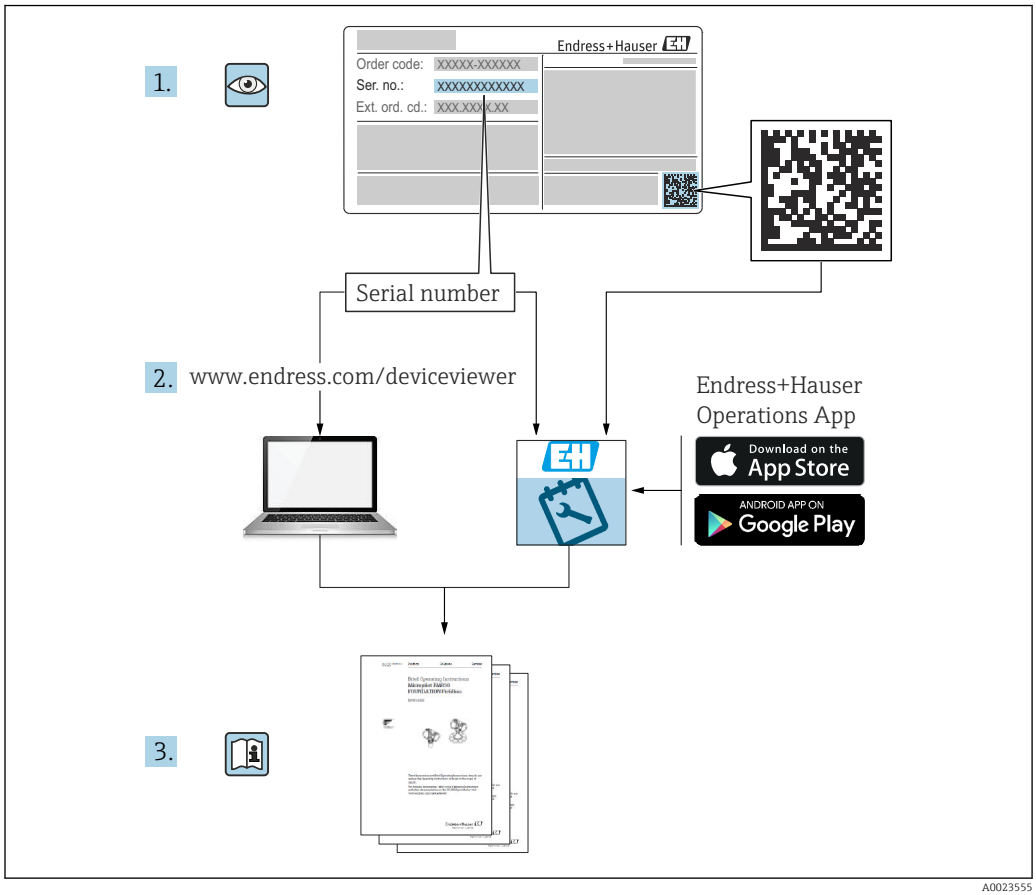

1.
Endress+Hauser
Order code: XXXXX-XXXXXX
Ser. no.: XXXXXXXXXXX
Ext. ord. cd.: XXX XXX-XX XX
Serial number
2. www.endress.com/deviceviewer
Endress+Hauser
Operations App
Download on the App Store
ANDROID APP ON Google Play
3.
A0023555

Table of contents

1 Notification of security vulnerabilities and advisories 4

2 About this document 5
2.1 Document function 5
2.2 Symbols 5
2.2.1 Safety symbols 5
2.2.2 Symbols for certain types of information and graphics 5
2.3 Documentation 6
2.3.1 Further applicable documents 6
2.3.2 Purpose and content of the document types 6

3 System design 8
3.1 Target group 8
3.2 System overview 8
3.2.1 General information 8
3.2.2 System design and system boundaries 9
3.2.3 Communication and data processing . . 9
3.2.4 Operating system 10
3.3 Defining the security level 10
3.4 Typical operating environment of the product 10
3.5 Measures if the required operating environment cannot be provided 11
3.6 Carrying out risk analysis and risk assessment 11
3.7 Recommended risk minimization measures . . 11
3.7.1 Viewing the entire system 11
3.7.2 Training the users 12
3.7.3 Optimizing access management 12
3.7.4 Monitoring device data and device status 12
3.7.5 Updating product software 13
3.7.6 Protecting applications and apps 13

4 Commissioning (Installation and configuration) 14
4.1 Target group 14
4.2 Requirements of the personnel 14
4.3 Installation 14
4.4 Configuration 14
4.4.1 Required security steps during commissioning 14
4.4.2 Configuring the firewall 14
4.4.3 Hardening the product 15
4.4.4 Configuring user data 15
4.4.5 Security-related product settings 15

5 Operation 17
5.1 Target group 17
5.2 Requirements of the personnel 17
5.3 Tasks during operation 17
5.3.1 General recommendations 17
5.3.2 Exporting and printing data 17
5.3.3 Exporting and loading device data . . . 17
5.4 Security aspects during operation 17
5.5 Update management 18
5.5.1 Operating system 18
5.5.2 Field Xpert software 18
5.6 Repeating the risk analysis 18
5.7 Repair and disposal 18

6 Decommissioning 19
6.1 Target group 19
6.2 Requirements of the personnel 19
6.3 Decommissioning the product 19

7 Appendix 20
7.1 Security checklist for the product life cycle . . . 20
7.2 Version history 20

1 Notification of security vulnerabilities and advisories

Endress+Hauser provides information on cybersecurity and security on the following web page: https://www.endress.com/cybersecurity

The web page includes the following information, for example:
- Current security alerts affecting Endress+Hauser products
- Contact information for reporting security vulnerabilities of Endress+Hauser products. PGP provides the option for confidential communication. You can download the public key from the website.
- Subscription option to e-mail service for new advisories on Endress+Hauser products
- Endress+Hauser contact information: PSIRT@endress.com

2 About this document

2.1 Document function

This supplementary Security Manual applies in addition to the product documentation such as Operating Instructions, Technical Information and ATEX Safety Instructions. The supplementary product documentation must be followed throughout the entire life cycle of the product. The additional requirements in relation to security are described in this Security Manual.

2.2 Symbols

2.2.1 Safety symbols

⚠ DANGER
This symbol alerts you to a dangerous situation. Failure to avoid this situation will result in serious or fatal injury.

⚠ WARNING
This symbol alerts you to a dangerous situation. Failure to avoid this situation can result in serious or fatal injury.

⚠ CAUTION
This symbol alerts you to a dangerous situation. Failure to avoid this situation can result in minor or medium injury.

NOTICE
This symbol contains information on procedures and other facts which do not result in personal injury.

2.2.2 Symbols for certain types of information and graphics

Tip
Indicates additional information

Reference to documentation

Reference to graphic

▶
Notice or individual step to be observed

1., 2., 3.
Series of steps

Result of a step

1, 2, 3, ...
Item numbers

A, B, C, ...
Views

2.3 Documentation

2.3.1 Further applicable documents

An overview of the associated documentation is provided in the following:
- *Device Viewer*: Enter serial number from nameplate
  www.endress.com/deviceviewer
- The download area of the Endress+Hauser website
  www.endress.com/downloads

Further applicable documents for Field Xpert

Field Xpert SMT50
- Technical Information TI01555S
- Operating Instructions BA02053S
- Manufacturer Information MI01495S

Field Xpert SMT50B
- Technical Information TI01877S
- Operating Instructions BA02584S
- Manufacturer Information MI01536S

Field Xpert SMT70
- Technical Information TI01342S
- Operating Instructions BA01709S
- Manufacturer Information MI01422S

Field Xpert SMT70B
- Technical Information TI01814S
- Operating Instructions BA02390S
- Manufacturer Information MI01514S

Field Xpert SMT77
- Technical Information TI01418S
- Operating Instructions BA01923S
- Manufacturer Information MI01440S

Netilion
- Netilion – Terms of Service
  https://netilion.endress.com/legal/terms-of-service
- Netilion – Privacy Policy
  https://netilion.endress.com/legal/privacy-policy
- Netilion – Security Policy
  https://netilion.endress.com/legal/security-policy
- Netilion – Service Level Agreement
  https://netilion.endress.com/legal/service-level-agreement

2.3.2 Purpose and content of the document types

Technical Information (TI)

Planning aid
This document contains all the technical data on the product and provides an overview of everything that can be ordered with the product.

Brief Operating Instructions (KA)

Guide that takes you quickly to the 1st measured value
The Brief Operating Instructions contain all the essential information from incoming acceptance to initial commissioning.

Operating Instructions (BA)

Your comprehensive reference
The Operating Instructions contain all the information that is required in various phases of the life cycle of the product: from product identification, incoming acceptance and storage, to mounting, electrical connection, operation and commissioning through to troubleshooting, maintenance and disposal.

Safety Instructions (XA)

Safety Instructions (XA) are supplied with the product depending on the approval. They are an integral part of the Operating Instructions.

The nameplate indicates the Safety Instructions (XA) that are relevant to the product.

Special Documentation (SD)

Additional information
Special Documentation provides additional information on the product. Additional information can include graphical representation of commissioning, for example, or information on an app.

3 System design

3.1 Target group

This section is aimed at planners and system integrators.

3.2 System overview

3.2.1 General information

The Field Xpert tablet PC for universal device configuration supports a variety of protocols, the Endress+Hauser service protocols, and connection to Endress+Hauser Bluetooth field devices and Endress+Hauser WLAN field devices. You can connect the field devices directly via a suitable interface, such as a modem (point-to-point), a bus system (point-to-bus) or a wireless connection (WLAN/Bluetooth).

The Field Xpert software package is fast, easy and intuitive to use.

The Field Xpert device library already has several thousand pre-installed device and communication drivers. They can be used to operate practically all HART and FOUNDATION Fieldbus devices (FieldComm Group libraries). Furthermore all Endress+Hauser field device drivers are installed. The generic HART DTM and PROFIBUS profile DTMs also enable operation of all the important basic functionalities of the relevant field devices.

In addition, the tablet PC features the FDI Package Manager for the installation of FDI Packages and the IODD DTM Configurator for installing IODDs. You can install new device drivers (DTMs, FDI Packages and IODDs) on the tablet PC at any time.

The connection from the tablet PC to the field devices is established either via an interface, a modem, a gateway, via a wireless local area network or Bluetooth.

You have the option to log the tablet PC directly on to the Endress+Hauser Netilion Cloud. You can upload data such as parameter data records from the tablet PC

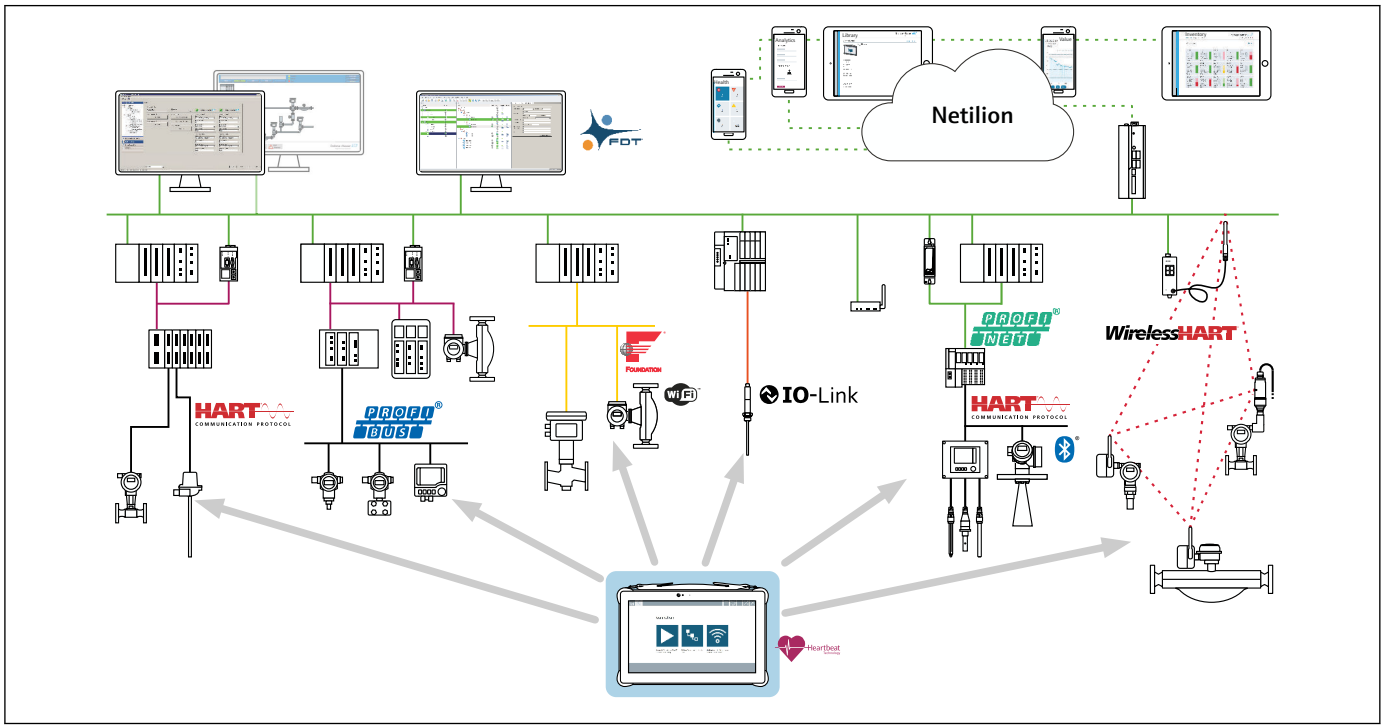
In process plants, the control system is responsible for controlling the plant and for process monitoring. The Field Xpert tablet PC is used only for commissioning and configuring individual field devices - even during ongoing operation.

Supported field devices and protocols
Endress+Hauser field devices and 3rd-party field devices
- HART
- PROFIBUS DP/PA
- PROFINET
- FOUNDATION fieldbus
- Modbus
- IO-Link
- Bluetooth: Endress+Hauser field devices with Bluetooth function
- WLAN: Endress+Hauser WLAN field devices

Supported Endress+Hauser service protocols
- CDI
- IPC
- ISS
- PCP

3.2.2 System design and system boundaries

This Security Manual describes the Field Xpert tablet PC, the Field Xpert software including the Field Xpert utility programs, the pre-installed drivers and the operating system of the tablet PC. Devices connected or linked to the tablet PC, such as field devices, gateways etc., are **not** considered in this Security Manual. The system boundary is marked in blue in the diagram below.



1 *Field Xpert applications, SMT70/SMT70B shown here (the blue marking shows the system boundary for this manual)*

3.2.3 Communication and data processing

Depending on the version of the Field Xpert tablet PC, the tablet PC features the following connections and functions for communication and data processing.

For detailed information, see the Technical Information for SMTxx → 6

Field Xpert SMT50
- Connections such as video and serial ports
- Expansion slots
- USB
- Wireless local area network
- Bluetooth
- Wireless WAN + GPS

Field Xpert SMT50B
- Expansion slots
- USB
- Wireless local area network
- Bluetooth
- Wireless WAN

Field Xpert SMT70
- Connections such as headphone output and microphone input
- Expansion slots
- USB

- Wireless local area network
- Bluetooth
- Wireless WAN + GPS

Field Xpert SMT70B
- I/O ports
- USB
- Wireless local area network
- Bluetooth
- Wireless WAN
- GPS sensor

Field Xpert SMT77
- Ports such as a microSD card slot
- Connection to docking station
- Extension slot for HART add-on module
- USB
- Wireless local area network
- Bluetooth
- Depends on the version, either "WLAN" or "Wireless WAN + GPS"

3.2.4 Operating system

A Microsoft Windows operating system runs on the Field Xpert tablet PC. It is the responsibility of the operator to update the operating system.

For detailed information, see the Technical Information for SMTxx → 6

3.3 Defining the security level

Both the system and the products installed in the system must meet different levels of requirements depending on the required security level. You must first define the required **security level** from SL1 to SL4 for the system. Depending on the security level, you define the requirements for the system in accordance with DIN IEC 62443-3-3 and the requirements for the product in accordance with DIN EN 62443-4-2.

3.4 Typical operating environment of the product

Analysis of the operating environment for the product should give information on the security requirements that must be provided by the environment. For example, you may observe a denial-of-service attack.

Example of a typical operating environment of the product:
- The product is a system component.
- The product is supplied with at least one interface, for example Ethernet-based interfaces and/or wireless interfaces such as WLAN or Bluetooth. See the system overview section for information on interfaces.
- The product is operated in an industrial environment.
- Access to the product is regulated. Only authorized persons have access to the product.
- Personnel have been trained in how to use the product and the related security risks.
- The product has an optional HTTPS-protected data connection that leaves the production area, e.g., for updates and the Netilion Cloud.
  The security of all network components used is ensured by the operator.
- The automation network is protected against attacks from the outside, such as a denial-of-service attack, by means of perimeter protection.

- The product is operated in an Ethernet network that is intended for industrial purposes only. The network is either fully separated from the rest of the company's network or protected by firewalls.
- Passwords for the product are only known by authorized personnel.
- Only authorized personnel can access the product via the associated Human Machine Interface (HMI).

Since the computing power of the product under consideration is limited, it can only withstand attacks to a limited extent.

3.5 Measures if the required operating environment cannot be provided

If the specified requirements for the operating environment cannot be met, alternative measures may need to be put in place. This may involve, for example, mechanical protection of the product against tampering, mechanical protection of the cabling, or organizational measures.

To minimize the risk of unauthorized access, the Field Xpert tablet PC should not leave the factory premises.

Carry out the following if there is any suspicion of unauthorized access:
- Compare the checksum with a reference installation.
- Restore the Field Xpert tablet PC to its factory settings using the recovery partition.

3.6 Carrying out risk analysis and risk assessment

When planning a system, you must carry out a risk assessment for the entire system taking a holistic approach. You can follow the guidelines in the VDI 2182 standard when carrying out a risk assessment on systems.

You carry out a risk/threat analysis during the course of the risk assessment.

Take the following aspects into account for the risk analysis:
- Interfaces of the product that allow communication with the product or enable access to the product
- Product data flows within the system
  - Incoming data to the product
  - Outgoing data from the product
- Product data flows that leave the area of the system and go through firewalls if necessary

You can define risk minimization measures based on the risk analysis.

In addition to the risk assessment, the planning process should also include specifications on how the product is to be configured during commissioning. This includes, for example, switching off interfaces and/or services that are not required or changing default passwords etc. These measures are explained in the following sections.

3.7 Recommended risk minimization measures

3.7.1 Viewing the entire system

The Field Xpert tablet PC is used in a production system for commissioning and configuring individual field devices. If necessary, the tablet PC can also be logged on to the Endress+Hauser Netilion Cloud IIoT ecosystem to save data there.

Due to their decentralized and modular structure, systems such as production systems and/or IIoT ecosystems, can quickly become a patchwork of different terminals. Due to the heterogeneous nature of these overall solutions, each divergent product represents a new

source of danger that compromises security at the interfaces and can result in insecure data transmission paths.

The device under consideration in this manual is Endress+Hauser's Field Xpert tablet PC. Additional analyses are required for the entire system.

- Hardening the product: → 15
- Update management: → 18

Network

Pay particular attention to the network components used, the router and switches for example.

The integrity of the components and access to the network must be guaranteed or limited by the operator.

Drivers

Device drivers such as DTMs are used to configure field devices via the Field Xpert software. The device drivers must originate from trusted sources only and the origin must be validated via digital signatures before installation.

3.7.2 Training the users

Depending on the application scenario, users who are not specialized in this area may come in contact with the IIoT ecosystem. We recommend that these users be trained in the safe use of the relevant terminals and/or interfaces and be made aware of security issues.

3.7.3 Optimizing access management

No explicit user management is implemented in the Field Xpert software. Access to Netilion and Endress+Hauser's software license management are password-protected.

Please note that any user who can log in to Field Xpert via the Windows login can potentially use the full range of functionality of the Field Xpert software.

We recommend that you apply the same identity and access management rules for access to the operating system (Windows) as for other areas of the company. For example:
- Grant employees only the access rights they need to perform their tasks
- Only allocate user accounts with strong passwords
- Use a password manager to generate, store, and manage passwords
- Use different passwords for different services
- Automatic lock when system is no longer used

We recommend using the tablet PC only for the Field Xpert software and associated utility programs.

Only authorized and trained users should work with the tablet PC. With the tablet PC, users have access to the configuration settings and data of the tablet PC, as well as to the field devices.

3.7.4 Monitoring device data and device status

Multiple attacks on a product in a system create anomalies in the network traffic. If a product suddenly delivers unrealistic values, this can be an indication of an attack.

As real-time monitoring is not a realistic possibility for most users, this process has to be automated. We recommend using monitoring software that monitors specific parameters and the status of the product and of the network and reports any deviations.

The Field Xpert tablet PC is a device with software in a production system. Detection of anomalies is a task for the higher-level system.

Monitoring the fieldbuses

The Field Xpert tablet PC can be connected to a control system via various protocols. Communication with the field devices is not encrypted nowadays. Physical protection, as well as the detection and resolution of anomalies, is the responsibility of the control system operator.

3.7.5 Updating product software

Given the dynamic nature of IT and increasing requirements in networking and the use of software libraries, updates are always required.

We recommend checking regularly to see if new updates are available and to install any updates. Missed updates pose a serious security risk, as attackers could have information on the vulnerabilities they are meant to rectify.

If there is an existing Internet connection, the Field Xpert software automatically checks for updates and sends notifications.

If there is no Internet connection, you can download the updates via the Endress+Hauser software portal: https://software-products.endress.com/

Update management: → 18

Drivers

If you start the Field Xpert software and the tablet PC is connected to the Internet, the software automatically searches for new DTMs. New DTMs are downloaded to the tablet PC and installed automatically.

You must download FDI Packages manually and install them on the tablet PC using the FDI Package Manager.

You must download IODDs manually and install them on the tablet PC using the IODD DTM Configurator.

You can download all the device drivers and communication drivers via the Endress+Hauser software portal: https://software-products.endress.com/

Operating system

A Microsoft Windows operating system runs on the Field Xpert tablet PC. It is the responsibility of the operator to update the operating system.

For detailed information, see the Technical Information for SMTxx → 6

3.7.6 Protecting applications and apps

Software and, in particular, a heterogeneous software landscape represent a further security risk, such as the use of Android apps on a tablet and Windows solutions on a PC.

In order to secure the applications, protection should also be provided for the mobile and stationary terminals that have access to the Field Xpert tablet PC. This includes regular installation of operating system updates and application updates as well as the use of a virus scanner.

Protection of the login details for the terminals should also be ensured in order to protect the customer system and customer data. Access data and certificates must be kept in a safe place.

4 Commissioning (Installation and configuration)

4.1 Target group

This section is aimed at operating personnel.

4.2 Requirements of the personnel

Personnel must fulfill the following requirements:
- Must have a relevant qualification for this specific function and task.
- Authorized by the rig owner/operator.
- Be familiar with federal/national regulations.
- Before starting work: personnel must read and understand the instructions in the manual and supplementary documentation as well as the certificates (depending on the application).
- Personnel must follow instructions and comply with general policies.

4.3 Installation

Install the product according to the associated Brief Operating Instructions/Operating Instructions.

4.4 Configuration

4.4.1 Required security steps during commissioning

Commission and configure the product in accordance with the associated Brief Operating Instructions/Operating Instructions. With regard to security, please also refer to this section and the additional sections.

For detailed information, see the SMTxx documentation: → 6

With regard to security, pay attention to the following during commissioning:
- Integrate the product in the operating environment in accordance with the specified requirements → 10.
- Ensure the operating system is up-to-date.
- Disable booting from an external physical medium.
- Secure the BIOS settings with a password.
- Disable any USB ports that are not required for operation.
- Disable Bluetooth and WLAN if not required for operation.
- Disable optional WWAN if not required for operation.
- After commissioning, change the admin password.
- Encrypt the internal hard disk using Microsoft's BitLocker encryption feature. Newer versions of the Field Xpert software are already encrypted on delivery.

4.4.2 Configuring the firewall

The Field Xpert tablet PC has a Windows firewall.

The Windows firewall can significantly help to build a "First Line of Defense" or to function as "Defense in Depth" in the LAN.

Disabling the Windows firewall increases the vulnerability of the Field Xpert software installed on the tablet PC.

Every infected PC or mobile device with access to the company intranet can establish a connection to an unprotected server and jeopardize the server by using a weak spot in a Windows service or in a third-party application.

In addition, the Windows firewall can defend against denial-of-service attacks. In a denial-of-service attack, a Windows PC is bombarded with network traffic, either causing it to crash or making it inaccessible to the rest of the network.

We recommend you switch on Windows Firewall by defining the configuration for private networks and public networks as follows:
- Windows Firewall status: On
- Incoming connections: Block
- Outgoing connections: Allow

The Field Xpert software does not require any entries in the Windows firewall during normal operation.

However, for the operation of certain device drivers, it may be that you are prompted by the Field Xpert software to release ports in the Windows firewall.

4.4.3 Hardening the product

In the field of security, “hardening” means that only those services and functions are enabled and connections activated that are necessary for the proper operation of the product for the specific application.

Drivers

We recommend un-installing unused drivers to reduce the potential attack surface.

4.4.4 Configuring user data

User data include, for example, login data, users, device tags (TAG), passwords, IDs, etc.

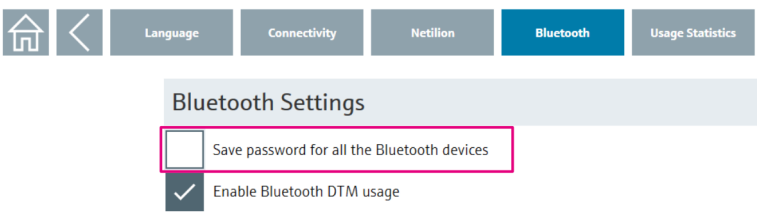
Create, change and delete user accounts in accordance with Windows documentation.

4.4.5 Security-related product settings

Bluetooth settings

You can save passwords for Bluetooth field devices on the tablet PC so that they are used automatically the next time you establish a connection. If you do **not** want this function, you must disable the **Save Password for all the Bluetooth devices** option.

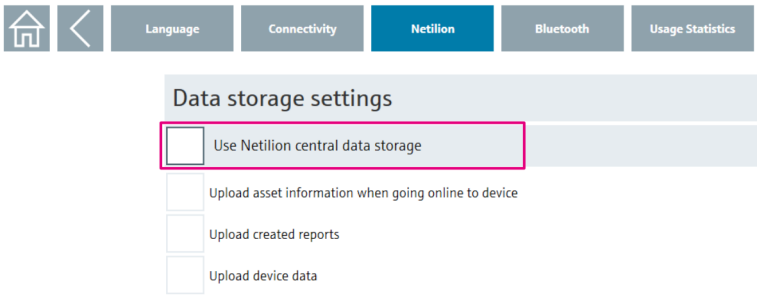
1. Tap the ☰ icon in the header on the start screen.
   ↳ The "DTM Catalog" page is displayed.
2. Tap the **Settings** tab.
   ↳ The "Language" page is displayed.
3. Tap the **Bluetooth** tab.
   ↳ The Bluetooth settings are displayed.



Netilion settings

You can save device data and device reports on the tablet PC and upload them to the Netilion cloud platform at a later stage.If you do **not** want this function, you must disable the **Use Netilion central data storage** option.

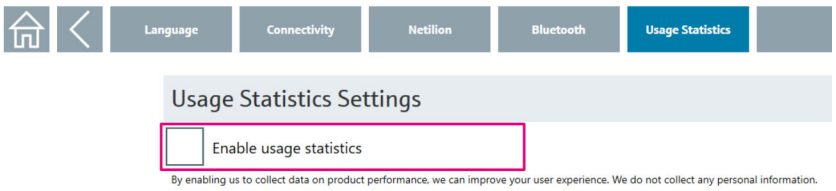
1. Tap the ☰ icon in the header on the start screen.
   ↳ The "DTM Catalog" page is displayed.
2. Tap the **Settings** tab.
   ↳ The "Language" page is displayed.
3. Tap the **Netilion** tab.
   ↳ The settings for the data storage are displayed.



Usage statistics settings

Data about usage is collected by default for product improvement. If you do not want to have data collected, disable the **Enable usage statistics** option.

1. Tap the ☰ icon in the header on the start screen.
   ↳ The "DTM Catalog" page is displayed.
2. Tap the **Settings** tab.
   ↳ The "Language" page is displayed.
3. Tap the **Usage Statistics** tab.
   ↳ The usage statistics settings are displayed.



5 Operation

5.1 Target group

This section is aimed at operating personnel.

5.2 Requirements of the personnel

Personnel must fulfill the following requirements:
- Must have a relevant qualification for this specific function and task.
- Authorized by the rig owner/operator.
- Be familiar with federal/national regulations.
- Before starting work: personnel must read and understand the instructions in the manual and supplementary documentation as well as the certificates (depending on the application).
- Personnel must follow instructions and comply with general policies.

5.3 Tasks during operation

Operate the product in accordance with the associated Operating Instructions. With regard to security, please also refer to the sections below.

5.3.1 General recommendations

- Only enter passwords when unobserved.
- If a password is no longer trustworthy, disable the associated user account immediately and change the password.
- When the tablet PC is not in use, disable it and lock it away or use a security cable to protect it from theft to prevent unauthorized access to the product.

5.3.2 Exporting and printing data

You can export and print the configuration settings of field devices using the Field Xpert software.

Since these data are not encrypted and protected by the Field Xpert software, it is the responsibility of the operating staff to protect these data and treat the data as confidential.

5.3.3 Exporting and loading device data

The Field Xpert software provides the following file formats for exporting and importing files: *.dcdtm, *.deh, *.curves, *.crv or *.csv.

The Field Xpert software exports the data without protection. Since the exported files can be modified, it is the responsibility of the operating staff to protect the files against modification.

The Field Xpert software does not carry out any validation when importing files. The operating staff is responsible for ensuring that only files from trusted sources are imported.

5.4 Security aspects during operation

Perform the following tasks regularly during operation:
- Windows updates
- Updates for the Field Xpert software
- Updates for device drivers such as FDT/DTM and FDI Packages

5.5 Update management

5.5.1 Operating system

The operating system on the Field Xpert tablet PC is automatically updated by Microsoft update routines. Updating the operating system is the responsibility of the operator, e.g. the updates must be approved and the tablet PC must be regularly connected to the Internet.

5.5.2 Field Xpert software

Update management for the Field Xpert software includes the following options:
- Automated by Endress+Hauser
- Manually by the user

Updates are provided for:
- Security patches
- Troubleshooting
- New functionality

Automated update management by Endress+Hauser

Endress+Hauser provides the updates for the Field Xpert software on the Endress+Hauser S3 server. Afterwards, the updates are automatically loaded to the Field Xpert tablet PC in the background. Manual intervention is not required.

The time of the updates is defined by Endress+Hauser or the user.

Endress+Hauser guarantees the integrity and authenticity of the updates. The company using the tool does not need to check the integrity of the updates.

Manual update management by the user/operator

If an Internet connection is not available, you can also get the updates manually and install them → 13.

Updates are published in the Endress+Hauser software portal:
https://software-products.endress.com/

The user defines the time of the updates.

Endress+Hauser uses checksums and signatures in the software to guarantee the integrity and authenticity of the updates. The person who performs the update must carry out an integrity and authenticity check.

5.6 Repeating the risk analysis

External events can change the risk situation that systems are exposed to; unknown attack patterns can occur for example. According to Section 4.4 of the VDI/VDE 2182-1-2011 guidelines, risk analysis must be repeated and updated at regular intervals or in the event of changes to the system that could influence the risk analysis.

5.7 Repair and disposal

Repair or dispose of the product in accordance with the Operating Instructions.

6 Decommissioning

6.1 Target group

This section is aimed at operating personnel.

6.2 Requirements of the personnel

Personnel must fulfill the following requirements:
- Must have a relevant qualification for this specific function and task.
- Authorized by the rig owner/operator.
- Be familiar with federal/national regulations.
- Before starting work: personnel must read and understand the instructions in the manual and supplementary documentation as well as the certificates (depending on the application).
- Personnel must follow instructions and comply with general policies.

6.3 Decommissioning the product

There are various reasons why the product may need to be decommissioned. Depending on the reason for decommissioning, certain actions are required.

Reason for decommissioning	Actions required
The product is not being used for a prolonged period of time.	1. Close all programs on the tablet PC. 2. Shut down Windows.
The product has a fault that you are unable to rectify.	Contact Endress+Hauser Service.
The product is to be disposed of.	Before you dispose of, or scrap, the physical media, we recommend that you proceed in accordance with the following guideline: NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization Smart devices may contain credentials that allow the device to communicate within the production plant or access certain services. Credentials are access data (login data) such as name, passwords and security certificates. When disposing, ensure that the data carrier is completely and safely deleted to exclude the possibility of data recovery. Alternatively, destroy the data carrier physically.

7 Appendix

7.1 Security checklist for the product life cycle

Life cycle	Task	Checked
Planning	Typical operating environment of the product defined and taken into account for planning. → 🖹 10 If required, alternative measures taken into account. → 🖹 11	❑
	Engineering-phase planning work considered. Threat analysis and risk assessment carried out. → 🖹 11	❑
	Where possible, risk minimization measures have been taken into account. → 🖹 11	❑
Goods receipt/transport	When accepting the goods, check that the packaging is undamaged.	❑
Commissioning	Product hardened for specific application. → 🖹 15	❑
Operation	Operation requirements observed. → 🖹 17	❑
	Update management requirements observed. → 🖹 18	❑
	Planning for renewed threat analysis performed. → 🖹 18	❑
Decommissioning	Product taken out of service. → 🖹 19	❑

7.2 Version history

Document version	Software version	Changes
01.25	as of 1.08.10	First version

www.addresses.endress.com

Endress+Hauser

People for Process Automation