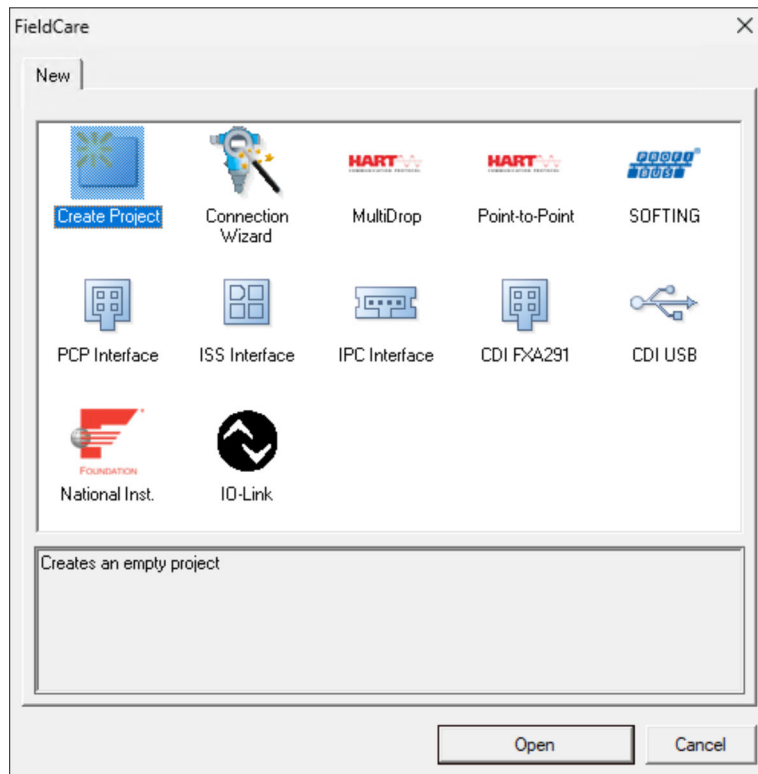


Special Documentation

Security Manual

FieldCare SFE500

Universal field device configuration tool for HART, PROFIBUS, FOUNDATION Fieldbus, Modbus, IO-Link, EtherNet/IP, PROFINET and PROFINET APL





A0023555

Table of contents

1	Reporting security gaps and advisories	4	5	Operation	19
			5.1	Target group	19
			5.2	Requirements of the personnel	19
2	About this document	5	5.3	Tasks during operation	19
2.1	Document function	5	5.3.1	General recommendations	19
2.2	Symbols used	5	5.3.2	Exporting and printing data	19
2.2.1	Safety symbols	5	5.3.3	Exporting and importing projects	19
2.2.2	Symbols for certain types of information and graphics	5	5.3.4	Performing regular backups	19
2.3	Documentation	6	5.4	Security factors during operation	20
2.3.1	Further applicable documents	6	5.5	Update management	21
2.3.2	Purpose and content of the document types	6	5.6	Repeating the risk analysis	21
3	System design	7	6	Decommissioning	22
3.1	Target group	7	6.1	Target group	22
3.2	System overview	7	6.2	Requirements of the personnel	22
3.2.1	General information	7	6.3	Decommissioning the product	22
3.2.2	System design and system boundaries	7	7	Appendix	23
3.3	Defining the security level	8	7.1	Security checklist for the product life cycle ...	23
3.4	Typical operating environment of the product	8	7.2	Version history	23
3.5	Measures required if necessary operating environment cannot be provided	9			
3.6	Carrying out risk analysis and risk assessment	9			
3.7	Recommended risk minimization measures ..	10			
3.7.1	Taking the entire system into account	10			
3.7.2	Training the users	11			
3.7.3	Optimizing access management	11			
3.7.4	Monitoring device data and device status	11			
3.7.5	Updating product software	11			
3.7.6	Protecting apps/applications	12			
4	Commissioning (installation and configuration)	13			
4.1	Target group	13			
4.2	Requirements of the personnel	13			
4.3	Installation	13			
4.4	Configuration	13			
4.4.1	Required security steps during commissioning	13			
4.4.2	Configuring the firewall	14			
4.4.3	Hardening the product	15			
4.4.4	Configuring user data	17			
4.4.5	Security-related product settings	17			
4.4.6	User management and impact on security	18			

1 Reporting security gaps and advisories

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

The page contains the following information, for example:

- Up-to-date security warnings (security alerts) that affect Endress+Hauser products
- Contact e-mail address to report security gaps in Endress+Hauser products. PGP encryption enables confidential communication. You can download the public key from the web page.
- 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 used

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



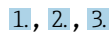
Reference to documentation



Reference to graphic



Notice or individual step to be observed



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 FieldCare SFE500

- Technical Information TI00028S
- Operating Instructions BA00065S

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

FieldCare is a tool for universal device configuration that supports various protocols and the Endress+Hauser service protocols.

The field devices can be connected directly via a suitable interface, such as a modem (point-to-point), a bus system (point-to-bus) or a network (LAN). FieldCare is quick, easy and intuitive to use.

You can install over 2700 device and communication drivers in the FieldCare device library. They can be used to operate all Endress+Hauser field devices and almost all HART and FOUNDATION Fieldbus devices (FieldComm Group libraries).

Further device drivers (DTMs) can be installed additionally. The generic HART DTM and PROFIBUS profile DTMs also enable operation of all the important basic functionalities of the relevant field devices.

3.2.2 System design and system boundaries

Supported field devices

- All Endress+Hauser field devices
- Almost all third-party field devices

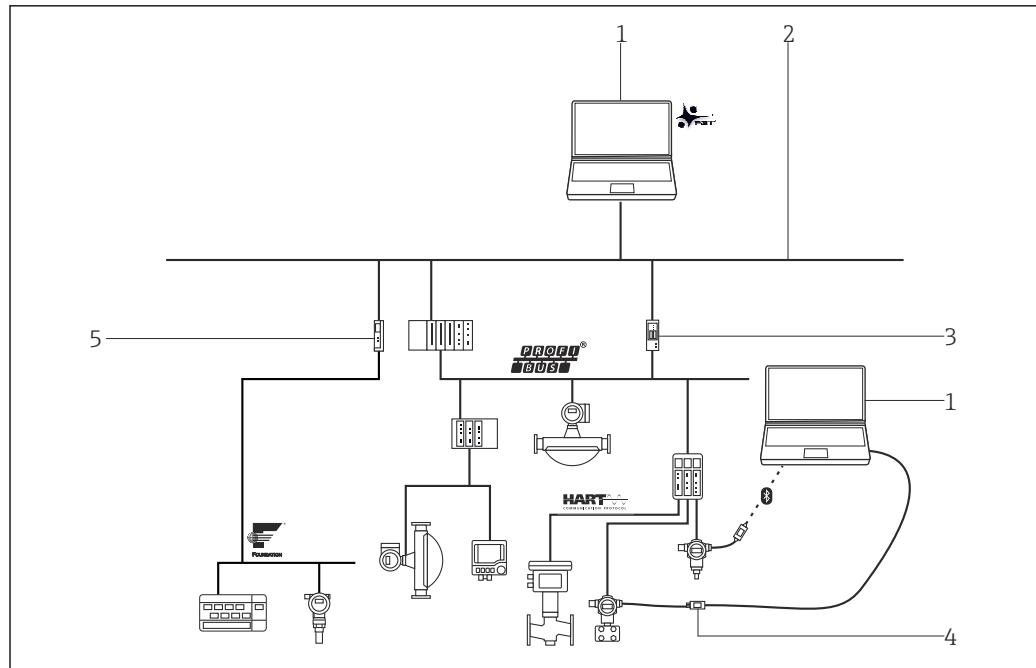
Supported protocols

- HART
- PROFIBUS DP/PA
- FOUNDATION Fieldbus
- Modbus
- IO-Link
- PROFINET
- EtherNet/IP

Endress+Hauser service protocols

- CDI
- ISS
- IPC
- PCP

Additionally, you can install further FDT DTMs and extend the list of supported field devices and protocols.



1 Example: System architecture with FieldCare

- 1 FieldCare
- 2 Ethernet
- 3 Ethernet/PROFIBUS gateway e.g. Fieldgate SFG500
- 4 Commubox FXA195
- 5 Ethernet/FOUNDATION Fieldbus gateway

FieldCare SFE500 is operated on Microsoft Windows. Microsoft Windows is referred to in this manual as the host system and can be installed either natively on a PC, laptop or in a virtual environment.

The following options are available for connecting the field devices:

- Via modem
- Via gateway between the TCP/IP network and corresponding fieldbus
- Via gateway between different fieldbuses, such as HART-over-PROFIBUS
- Via wireless transmission, e.g. WirelessHART

In addition to FieldCare SFE500, a control system is running in the process plant, which controls the plant and must access the process values of the field devices for this purpose.

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

We recommend that you define the typical operating environment of the product in order to draw up the security-related properties.

The requirements of the environment should be determined by assessing the operating environment. For example, you can factor in a denial-of-service attack.

The following considerations may apply for a typical operating environment for example:

- The product is a system component.
- The product is equipped with at least one interface. See the system overview section for information on interfaces.
- The product is operated in an industrial environment.
- Access to the system is regulated. Only authorized staff have access to the system.
- The personnel are trained and instructed on the use of the product and on the security risks.
- 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.
- The product has at least one data connection that leaves the production area.
- The security of the network components 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 installed in an environment that is protected in accordance with the defense in depth principle.
- Passwords for the product are only known by authorized personnel.
- Only authorized personnel can access the product via the associated Human Machine Interface (HMI).


The product can only defend against attacks to a limited extent because the processing power of the product in question is limited.

3.5 Measures required if necessary operating environment cannot be provided

If the specified requirements for the operating environment cannot be met, alternative measures may have to be arranged. 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 host system on which FieldCare SFE500 is installed should not leave the factory.

Carry out the following if there is any suspicion of unauthorized access:

- Check the signatures of the FieldCare SFE500 installation and the signatures of installed DTMs. →  13
- Compare the checksum with a reference installation.
- Restore FieldCare SFE500 or FieldCare projects from a backup. →  19
- Restart the DTD database from a trusted source.

FieldCare SFE500 uses the DTDs (Device Type Descriptions) from the database to determine the field device status. If an attacker has manipulated these DTDs, the wrong field device status is displayed. You may no longer use this field device status as the basis for decisions.

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 Taking the entire system into account

FieldCare SFE500 is an application that is used in a production system.


A production system can quickly become a unit of different end devices. 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 tool under consideration in this manual is Endress+Hauser's FieldCare SFE500. Additional analyses are required for the entire system.

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.

An attacker can gain complete access to components of the control system, such as field devices, since the communication server communicates via the Communication Service without encryption in FieldCare SFE500. The communication server interface (Communication Service) is disabled by default. →  17

DTMs

DTMs are used for configuring field devices via FieldCare SFE500. The DTMs must originate from trusted sources only and the origin must be validated via digital signatures before installation.

 Hardening the product: →  15

Update management: →  21

FDI Packages

FDI Packages are used for the configuration of field devices via FieldCare SFE500. The FDI Packages may only come from trusted sources. The person installing the FDI Packages must validate the origin via digital signatures prior to 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

User management is implemented in FieldCare SFE500. This meets the requirement for security level SL1 in the area of access management.

It must be noted that any user that can access the host system can potentially use the full range of functions of FieldCare SFE500.

Host and client system

We recommend that you apply the same identity and access management rules for access to the host system as for other areas of the company. For example:

- Only grant access rights to employees who require access to carry out their tasks
- Only allocate user accounts (Accounts) with strong passwords
- Generate, back up and manage passwords with a password manager
- Use different passwords for different services
- Automatic lock when system is no longer used

We recommend the following points for the host system:

- Only use the host system for FieldCare SFE500
- Do not install any other applications on the host system
- Only authorized and trained users may work on the host system

3.7.4 Monitoring device data and device status

The occurrence of multiple attacks on a product in a system causes anomalies in network traffic. If a product suddenly starts producing unrealistic values, this may indicate the occurrence of an attack.

Since real-time monitoring is not an option for most users, this process needs to be automated. We recommend using monitoring software that oversees specific parameters and the condition of the product and network and reports any deviations.

FieldCare SFE500 is software in the production system. Detection of anomalies is a task of the higher-level system.

Monitoring the fieldbuses

FieldCare SFE500 is connected to the control system via various protocols. Communication with the field devices is not encrypted. The physical protection, as well as detection and correction of anomalies is then 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 that you regularly check if new updates are available and install them. Missed updates are a serious security risk as potential attackers could also be aware of the vulnerabilities to be fixed.

If there is an existing Internet connection, FieldCare SFE500 automatically checks for updates and sends notifications.

If there is no Internet connection, you can download updates at the following address:

<https://software-products.endress.com/>

 Hardening the product: →  15

Update management: →  21

3.7.6 Protecting apps/applications

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 FieldCare SFE500. This includes regular installation of operating system updates and application updates as well as the use of a virus scanner.

Protection of the access data of 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 following sections.


1. Encrypt the hard disk. →  13
2. Check installation files. →  13
3. Restrict access to host system. →  14
4. Follow the rules listed for the database. →  14

Encrypting the hard drives

Since FieldCare SFE500 stores device and system data unencrypted on hard drives, we recommend you encrypt the hard disks of the host system.

Checking the installation files

Before running the FieldCare SFE500 setup, the user who is installing FieldCare must perform an integrity and authenticity check of the installation files. The installation files are digitally signed for this purpose.

-  Perform the following check for each installation file (*.exe). If you are installing FieldCare SFE500 via the "Installation Manager" of the FieldCare packages, check the signature of the "InstallationManager.exe" file beforehand.

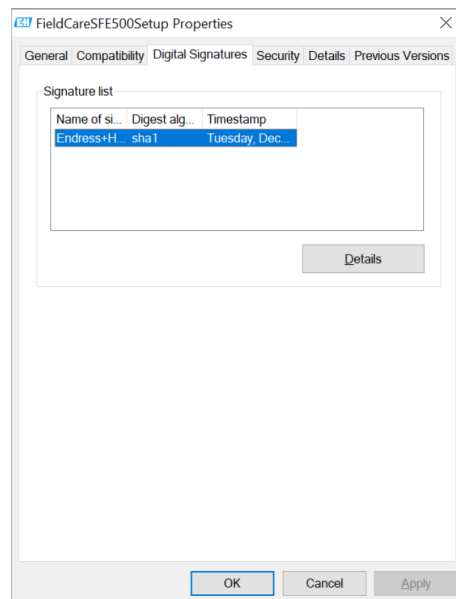
NOTICE**Incorrect installation files**

Installation of malware

- ▶ Only run installation files that contain the entry **Endress+Hauser Process Solutions AG** in **Name of signer**.

Check installation files (*.exe)

1. Select the installation file with the mouse.
2. Using the context menu, open the properties for the file.



3. Select the **Digital Signatures** tab.
4. Check whether **Name of signer** contains the entry **Endress+Hauser Process Solutions AG**. If the **Digital Signatures** tab does not exist or if the entry for **Name of signer** is different, you must **not** run the installation file. The installation file is not from Endress+Hauser in this case and could contain malware.

Restricting access to host system

FieldCare SFE500 stores the data in the local Microsoft SQL Server installation by default. The data includes project information, static and dynamic device data such as manufacturer information, tags and configuration data as well as information about the plant structure, historical device status and user credentials.

These data are not encrypted when saved. Any user who has access to the host system can view and modify these data.

Following the rules for the database

Given that the database is only available locally after a new installation of FieldCare SFE500 and Microsoft SQL Server, only the local user can access the data on the host system.

We do not recommend that you make the database available in the network via TCP/UDP. If the database is available in the network via TCP/UDP, an attacker can access FieldCare SFE500 data and modify them.

4.4.2 Configuring the firewall

Windows has a 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 Windows Firewall increases the attack surface in Windows.

Every infected PC 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

FieldCare SFE500 does not require any entries in the Windows Firewall during normal operation.


However, for the operation of certain DTMs, it may be that you are prompted by the FieldCare SFE500 software to release ports in Windows Firewall.

4.4.3 Hardening the product

In the field of security, the term "hardening" means that the only services enabled are those that are required for the correct operation of the product in the application in question.


DTMs

We recommend the following measures for DTMs:

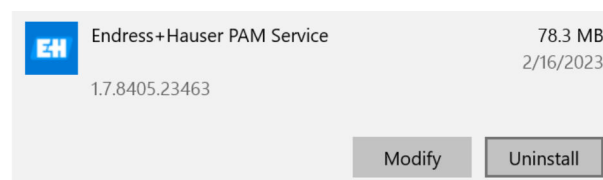
- Only install DTMs from trusted sources. Check the digital signature before installation.
→  13
- Uninstall unused DTMs to reduce the potential attack surface.

In FieldCare SFE500, the PAM Service is installed, which is executed with admin rights. In certain circumstances, this loads service DTMs and executes them with increased rights.

You can uninstall the PAM service if the following apply:

- You regularly check for product updates manually and install these updates manually
→  21
- The Device Agent of FieldCare SFE500 is **not** used as Configuration Client for the Asset Health Monitoring Solution SAH70.

- ▶ Uninstall the **PAM Service** in Windows settings.

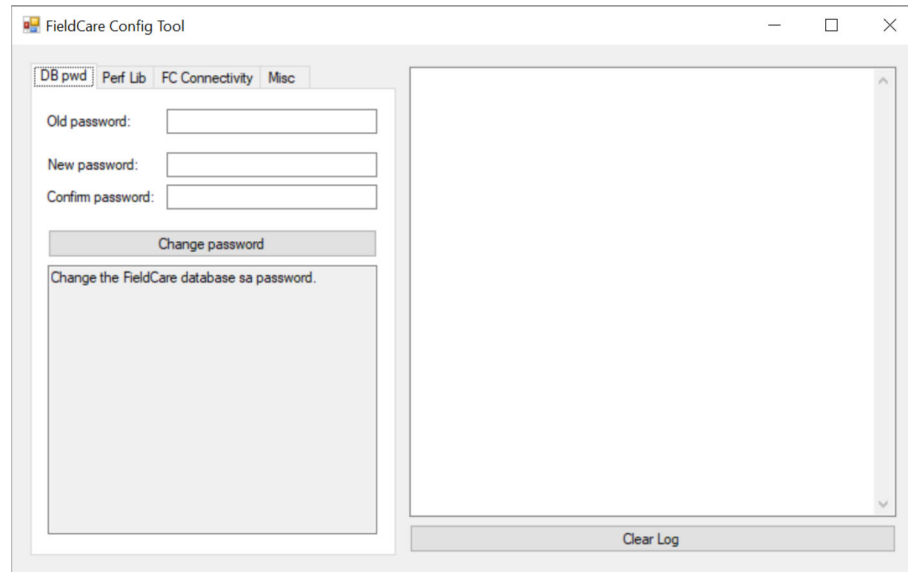



 2 Uninstalling the PAM service


Preconfigured default passwords

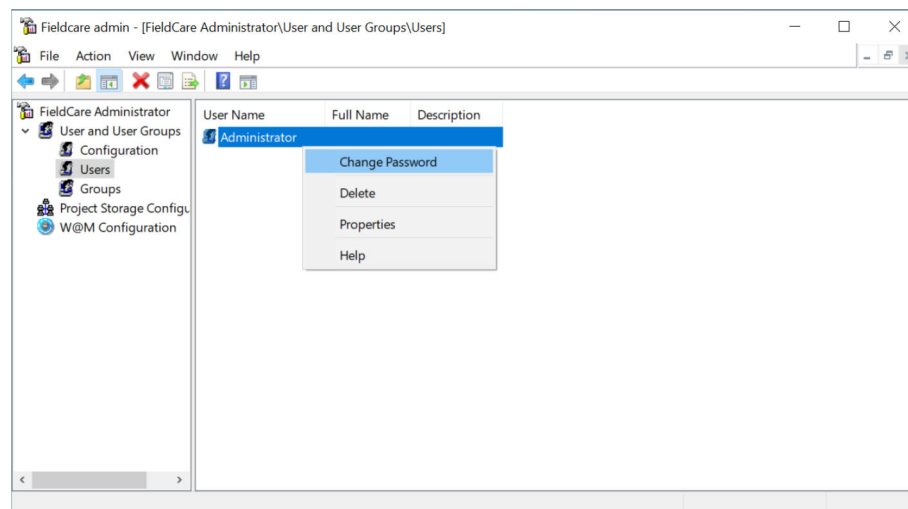
After a new installation, default passwords are configured for the database and "FieldCare Administration".

1. Open the following programme:
%ProgramData%\Endress+Hauser\FieldCare SFE500\Configuration\FC_ConfTool.exe.



 3 FieldCare Config Tool: Change password

2. Enter the old and new password.
3. Click **Change password**.
4. Open **FieldCare Administration**.
5. Log in as described in the Operating Instructions →  6.
 - ↳ The "FieldCare admin" window is opened.
6. Select **Users** in the left column.
7. Select **Administrator**.
8. Change the password via the **Change Password** context menu.



 4 FieldCare Administration: Change password

FieldCare's access to the Microsoft SQL database only works **without** a password.

We recommend the following measures since access to the database is not password-protected:

- Do not make the database available in the network.
- Protect the host system from unauthorized access.

4.4.4 Configuring user data

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



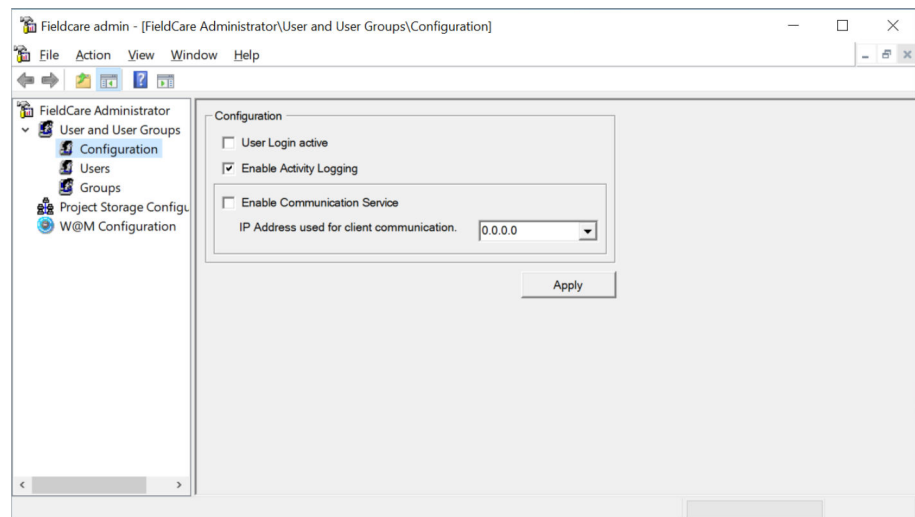
For detailed information on user administration, see Operating Instructions BA00065S

4.4.5 Security-related product settings

Communication Service

The Communication Service is disabled in FieldCare Administration by default. For security reasons, we recommend that you leave this service disabled.

The Communication Service must only be enabled for client-server communication (e.g. Asset Health Monitoring Solution SAH70). The service enables communication with the field devices configured in FieldCare SFE500 without user authentication and without encryption. Every user can thus access the field devices in the same network as the host system.



5 FieldCare Administration: Communication Service disabled

4.4.6 User management and impact on security

FieldCare SFE500 has its own user administration that is disabled initially after FieldCare SFE500 is installed.

Activation of user administration in FieldCare SFE500 can be another safety layer in the defense-in-depth concept.



For detailed information on user administration, see Operating Instructions BA00065S

FieldCare SFE500 stores the user password obfuscated and thus not entirely secure.

We advise you not to use the same passwords for user administration of FieldCare SFE500 and for Windows.

In addition, we recommend locking Windows automatically on inactivity.

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 this section and the following sections.

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.
- Lock the PC when you leave the work station to prevent unauthorized access to the product.

5.3.2 Exporting and printing data

You can export and print data such as data on the project, plant topology and field devices via FieldCare SFE500.

Since these data are not encrypted and protected by FieldCare SFE500, it is the responsibility of the operating staff to protect the data and treat the data as confidential.

5.3.3 Exporting and importing projects

FieldCare SFE500 provides the following file formats: *.fcproj, *.fcp, *.fcdtm, *.csv or *.xml for the export and import of files.

FieldCare SFE500 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.

FieldCare SFE500 does not carry out any validation when importing files. The operating staff are responsible for ensuring that only files from trusted sources are imported.

5.3.4 Performing regular backups

We recommend you perform regular backups so that you can quickly restore FieldCare SFE500 with the associated projects after a failure or after a security problem.


The following options are available for backup:

- Backup of all hard drives including Windows and all files
- Backup of all FieldCare projects

Both backup options offer only limited measures to protect the content. It is the responsibility of the operating staff to protect and secure backed up data.

Backup of all hard drives including Windows and all files

We recommend that you save the entire hard disk regularly including Windows and all files due to the operating principle of FDT. This ensures that, once restored, all DTMs are also available again on the system.

 Please note that when the system is restored on new hardware, your FieldCare SFE500 license is invalid. Contact Endress+Hauser Service in this case. If possible, you should return the software license to the Endress+Hauser software portal before a backup (disable).

Backup of all FieldCare projects

If a complete backup of the hard disk is not possible, we recommend that you back up FieldCare SFE500 projects. You can restore the functionality with the installation files for FieldCare SFE500 and the required DTMs and FDI Packages.

Recovery can take several hours.

 You must restore the FieldCare SFE500 license if you choose this method of recovery. Contact Endress+Hauser Service in this case.

Save FieldCare project


1. Select the project in FieldCare SFE500.
2. Click **File** → **Import/Export** → **Export Project**.
 - ↳ The "Export Project" dialog box is displayed.
3. Select a storage location, enter a name and click **Save**.
 - ↳ You are prompted for a password.
4. Select **Password protected**.
5. Enter the password.
6. Click **OK**.

Restore FieldCare project

1. Click **File** → **Import/Export** → **Import Project**.
 - ↳ The **Import Project** dialog box is displayed.
2. Select project.
3. Click **Open**.
 - ↳ If the project was protected with a password during export, you are prompted to enter the password.
4. Enter the password.
5. Click **OK**.

5.4 Security factors during operation

Perform the following tasks regularly during operation:

- Windows updates
- Updates for FDT/DTM field device drivers and FDI Packages
- Updates for FieldCare →  11

5.5 Update management

Update management for FieldCare SFE500 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 FieldCare SFE500 on the Endress+Hauser S3 server. Afterwards, the updates are automatically loaded to the FieldCare SFE500 host 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. →  11

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. →  13

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.

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 longer period of time.	Switch off host systems. Stop all processes if it is not possible to switch off the host systems.
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 digital certificates. Credentials may be stored in the database in the case of FieldCare SFE500. 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 has been defined and taken into account in planning. → 8 Where necessary, alternative measures have been taken into account.	<input type="checkbox"/>
	Planning activities taken into account in engineering phase. Threat analysis and risk assessment completed. → 9	<input type="checkbox"/>
	Where possible, risk minimization measures have been taken into account. → 10	<input type="checkbox"/>
Incoming goods/ transportation	Checked that the signature of the supplied files identifies Endress+Hauser as the manufacturer. → 13	<input type="checkbox"/>
Commissioning	Product hardened for specific application. → 15	<input type="checkbox"/>
Operation	Operation requirements observed. → 19	<input type="checkbox"/>
	Update management requirements observed. → 21	<input type="checkbox"/>
	Recurring risk analysis planning completed. → 21	<input type="checkbox"/>
Decommissioning	Product taken out of service. → 22	<input type="checkbox"/>

7.2 Version history

Document version	Software version	Changes
01.00	As of 02.18	First version



71639422

www.addresses.endress.com
