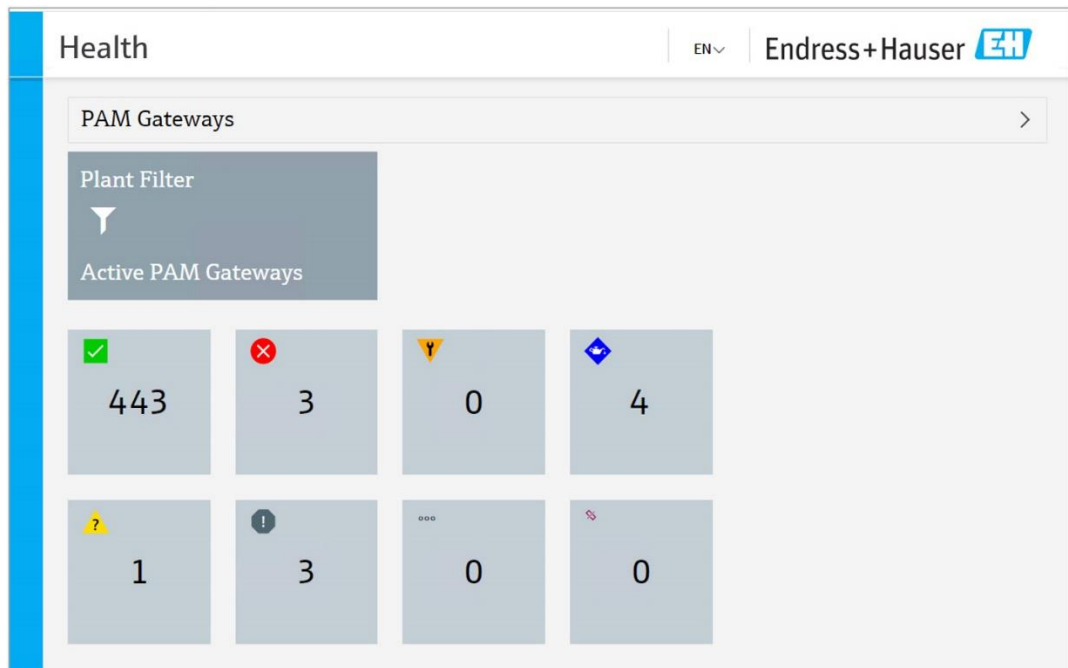


Special Documentation

Security Manual

Asset Health Monitoring Solution SAH70

Asset Health Monitoring Software



All rights reserved. Passing on and copying of this document, use and communication of its contents is not permitted without written authorization from Endress+Hauser Process Solutions AG.

Classification: PUBLIC

All rights reserved. Passing on and copying of this document, use and communication of its contents is not permitted without written authorization from Endress+Hauser Process Solutions AG.

Comments: / /		Project: 12230013 Asset Health Monitoring Solution SAH70	
Status: Released	Date: 21.07.2023	Author: Andreas Ernst	
Version: 1.00	Document number: D055-1	File name: AHM Solution SAH70 - Security_Handbuch D055_EN.docx	Page: 1 of 22
Template: D055_Security Manual_Template.docx, E+H Group Version, 01.00, Valid from 06.07.2022			

Security Manual**Asset Health Monitoring Solution SAH70**

Security Guideline

Table of contents

1	Notification of security vulnerabilities and advisories	4
2	About this document	5
2.1	Document function	5
2.2	Symbols used	5
2.2.1	Safety symbols	5
2.2.2	Symbols for certain types of information and graphics	6
2.3	Documentation	6
2.3.1	Further applicable documents	6
2.3.2	Purpose and contents of the documentation 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	8
3.3	Specifying the security level	9
3.4	Typical operating environment of the product	10
3.5	Measures if the required operating environment cannot be provided	10
3.6	Carrying out a threat analysis and risk assessment	10
3.7	Recommendation for measures that minimize risk	11
3.7.1	Analyzing the whole system	11
3.7.2	Training users	11
3.7.3	Optimizing access management	11
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	Start-up (installation and configuration)	14
4.1	Target group	14
4.2	Requirements for personnel	14
4.3	Installation	14
4.4	Configuration	14
4.4.1	Place the product in operation and configure	14
4.4.2	Required security steps during start-up	15
4.4.3	Configuring the firewall	16
4.4.4	Hardening the product	16
4.4.5	Configuring user data	17
4.4.6	Security-relevant configuration of the product	17
4.4.7	User management and effects on security	17
5	Operations	18
5.1	Target group	18
5.2	Requirements for personnel	18
5.3	Tasks during operation	18
5.4	Security aspects during operation	18
5.5	Update management	18
5.6	Repeating the threat analysis	19
5.7	Repair and disposal	19
6	Shutdown	20
6.1	Target group	20

Security Manual
Asset Health Monitoring Solution SAH70

Security Guideline

6.2	Requirements for personnel	20
6.3	Shutting down the product	21
7	Appendix	22
7.1	Security checklist for the product life cycle	22
7.2	Version history	22

All rights reserved. Passing on and copying of this document, use and communication of its contents is not permitted without written authorization from Endress+Hauser Process Solutions AG.

Classification:
PUBLIC

All rights reserved. Passing on and copying of this document, use and communication of its contents is not permitted without written authorization from Endress+Hauser Process Solutions AG.

1 Notification of security vulnerabilities and advisories

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

This web page contains 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 to email service for new advisories for Endress+Hauser products
- Endress+Hauser contact: PSIRT@endress.com

Version: 1.00	Document number: D055-1	File name: AHM Solution SAH70 - Security_Handbuch D055_EN.docx	Page: 4 of 22
-------------------------	-----------------------------------	--	-------------------------

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



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



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



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



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

Version: 1.00	Document number: D055-1	File name: AHM Solution SAH70 - Security_Handbuch D055_EN.docx	Page: 5 of 22
------------------	----------------------------	---	------------------

2.2.2 Symbols for certain types of information and graphics



Tip

Indicates additional information



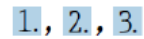
Reference to documentation



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:

- *W@M Device Viewer* (www.endress.com/deviceviewer): Enter the serial number from the name-plate
- The download area of the Endress+Hauser web site (www.endress.com/download)

Further applicable documents for AHM Solution

- Technical Information TI01544S
- Operating Instructions BA01682S
- Installation instructions
- FieldCare SFE500 Operating Instructions BA00065S

2.3.2 Purpose and contents of the documentation 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.

Version: 1.00	Document number: D055-1	File name: AHM Solution SAH70 - Security_Handbuch D055_EN.docx	Page: 6 of 22
-------------------------	-----------------------------------	--	-------------------------

Security Manual**Asset Health Monitoring Solution SAH70**

Security Guideline

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.

Version:	Document number:	File name:	Page:
1.00	D055-1	AHM Solution SAH70 - Security_Handbuch D055_EN.docx	7 of 22

3 System design

3.1 Target group

This section is directed to planners and system integrators

3.2 System overview

3.2.1 General information


The AHM Solution start-up is implemented by the Endress+Hauser service department.

The product runs on a Microsoft Windows operating system and the system therefore has a user interface, input options and user management.

In addition the AHM Solution uses the following interfaces:

- HTTP (recommended HTTPS)
- WCF
- EtherNet/IP
- HART

3.2.2 System design and system boundaries

 This security manual covers the AHM Solution, comprising the AHM server, PAM gateways, PAM clients and their connection to gateways and field devices. Other components, such as operating tools, are not included in this security manual. The system boundaries are marked in color in the following figure.

Version: 1.00	Document number: D055-1	File name: AHM Solution SAH70 - Security_Handbuch D055_EN.docx	Page: 8 of 22
-------------------------	-----------------------------------	--	-------------------------

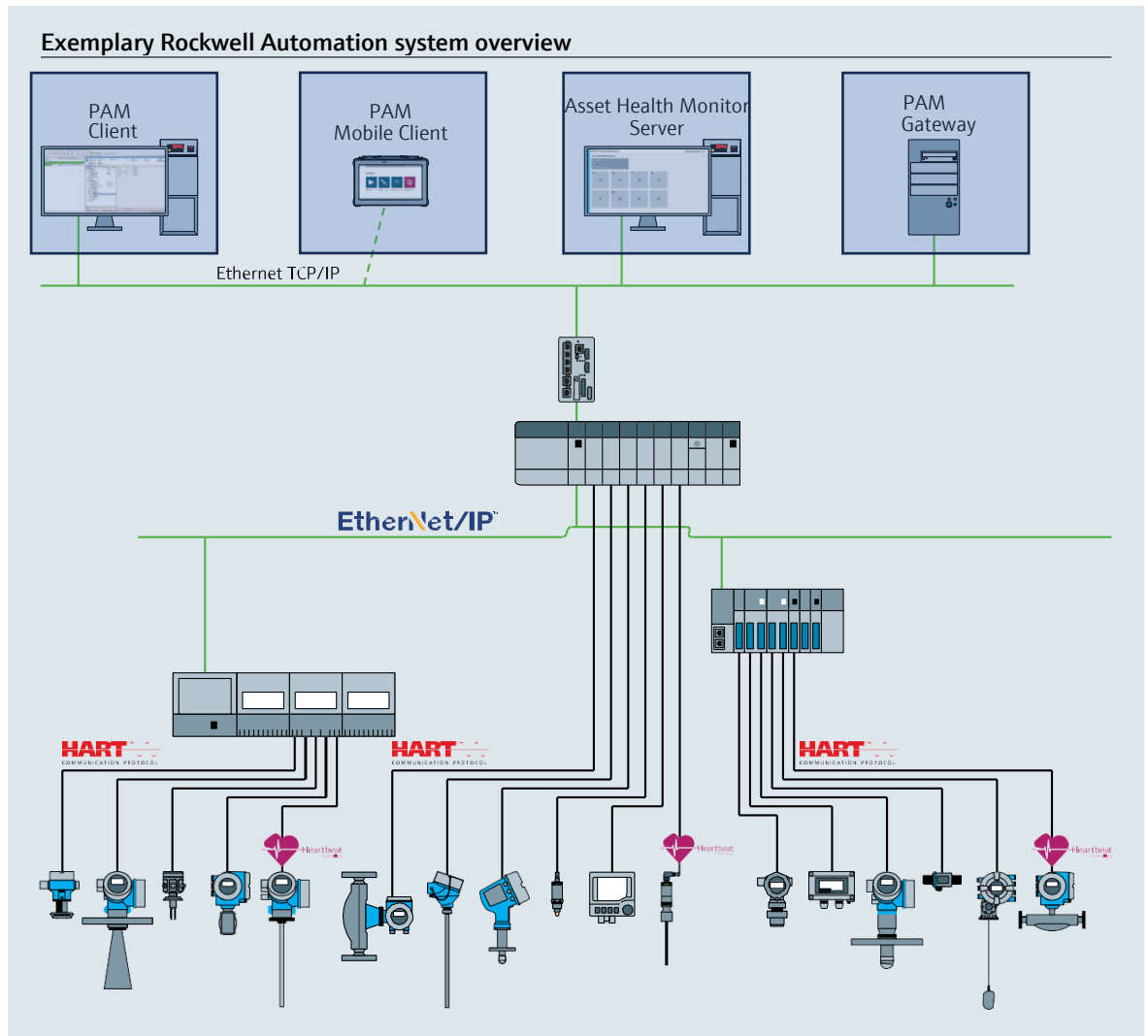




Figure 1 Exemplary system design

 The AHM Solution is described in the general texts of this document as the product, depending on the context.

 In the following, no differentiation is made between PAM Client and PAM Mobile Client; they are both referred to as PAM Client.

The AHM server and the PAM gateway are run on Microsoft Windows, which is described in the following as the host system. This can be installed natively on a PC or in a virtual environment.

3.3 Specifying the security level

Depending on the required security level, the system and the products installed on it must meet various requirements. Initially, you must specify the required **security level** SL1 to SL4 for the system. Depending on the security level, you can then determine the requirements for the system in accordance with DIN IEC 62443-3-3, and the requirements for the products in accordance with DIN EN 62443-4-2.

Version: 1.00	Document number: D055-1	File name: AHM Solution SAH70 - Security_Handbuch D055_EN.docx	Page: 9 of 22
-------------------------	-----------------------------------	--	-------------------------

3.4 Typical operating environment of the product

We recommend that you define the typical operating environment to specify the security-relevant properties of the product.

Analysis of the operating environment should provide information on the requirements posed by the environment. For example, you may observe a denial-of-service attack.

The following points, for example, could apply to a typical operating environment:

- The product is a system component.
- The product is operated in an industrial environment.
- Access to the host system, on which the product is installed, is regulated. Only authorized persons have access to the host system.
- Personnel have been trained in how to use the product and the related security risks.
- The product is operated in an Ethernet network that is only intended for industrial purposes. The network is either completely isolated from the remaining company network or is protected by fire-walls.
- The product is optionally equipped with a HTTPS-protected data connection that leaves the production area. Authentication for access is ensured by the operator.
- Perimeter protection is used to protect the automation network against external attacks such as, for example, a denial-of-service attack.
- The product is installed in an environment that is secured according to the defense-in-depth concept.
- Passwords for the product are only known to authorized persons.
- Only authorized persons can access the product via the corresponding Human Machine Interface (HMI).
- As the processing power of the host system is limited, certain attacks can only be defended against to a limited extent.

3.5 Measures if the required operating environment cannot be provided

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

3.6 Carrying out a threat analysis and risk assessment

When planning a facility, a risk assessment must be carried out for the entire facility using an integrated approach. Risk assessments for facilities can be carried out in reference to VDI 2182.

As part of the risk assessment, a risk analysis/threat analysis should be completed.

When carrying out a risk analysis, the following aspects should be taken into consideration:

- Interfaces of the product via which communication with the product is possible or which can be used to access the product.
- Data flows of the product within the facility
 - Incoming data to the product

Version: 1.00	Document number: D055-1	File name: AHM Solution SAH70 - Security_Handbuch D055_EN.docx	Page: 10 of 22
-------------------------	-----------------------------------	--	--------------------------

- Outgoing data from the product
- Data flows of the product that leave the area of the facility and potentially overcome firewalls

You can use the risk analysis to draw up measures that will reduce risk.

In addition to carrying out the risk assessment, the planning process should also be used to specify how the product should be configured during start-up. This might include, for example, deactivation of interfaces and/or services that are not required, changing standard passwords, etc. These measures are outlined in the following sections.

3.7 Recommendation for measures that minimize risk

3.7.1 Analyzing the whole system

The AHM Solution is an application that is integrated in a production system.

A production system can quickly develop into a patchwork of different end devices. Every deviating product represents a new potential hazard with such heterogeneous integrated solutions, resulting in breaches in the interfaces and insecure transmission paths.

This manual deals with the AHM Solution of Endress+Hauser. For the overall system, additional analyses are required.

Network

Special attention should be given to the network components used (e.g. router and switches). The integrity of the components and access to the network must be secured and/or restricted by the operator. The current version of the AHM Solution, the PAM client, the AHM server and the PAM gateway are not encrypted in their communication with each other, which means that an attacker would otherwise have complete access to components of the control system (e.g. field devices).

DTMs

DTMs are used in the AHM Solution for the configuration of field devices. These must only come from trustworthy sources and their origin must be validated by digital signatures before installation.

3.7.2 Training users

Depending on the application scenario, users who are not familiar with the field may also come into contact with the system. We recommend that these users be trained to ensure safe and secure use of the corresponding end devices and / or interfaces and to familiarize them with pertinent security issues (see section 5.3).

3.7.3 Optimizing access management

In the current version of the AHM Solution, there is no access management in the web application and for configuration by means of PAM client. This means that any person who has the possibility of communicating with the product via the network can access all interfaces and data provided by the product. We therefore recommend that the measures outlined in sections 4.4.3 and 4.4.4 are carried out.

Host and client systems

We recommend that the same rules be applied for identity and access management for access to the host system as for other company areas.

- Employees should only be given access authorization that is required for the employee to carry out their work.

Version:	Document number:	File name:	Page:
1.00	D055-1	AHM Solution SAH70 - Security_Handbuch D055_EN.docx	11 of 22

Security Manual**Asset Health Monitoring Solution SAH70**

Security Guideline

- User accounts should only be issued with strong passwords
- Generate, save and administer passwords using a password manager
- Use different passwords for different services
- Automatic blocking when the system is no longer used

We recommend that the host system (AHM server and PAM gateway) be used exclusively for the product and that no further applications be installed there. Also, no other users should be allowed to work on the host system, as this would enable them to have access to the configuration or the data of the product.

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 the use of monitoring software which monitors certain parameters and the status of the product and of the network and reports any deviations that occur.

The AHM Solution is software in the production system and the detection of anomalies is a task of the higher-level system.

Monitoring via EtherNet/IP or HART

The AHM Solution is connected to a control system via EtherNet/IP and HART. Communication with the devices is mostly unencrypted. Physical protection and the detection and remedying of anomalies is the responsibility of the operator of the control system.

Version: 1.00	Document number: D055-1	File name: AHM Solution SAH70 - Security_Handbuch D055_EN.docx	Page: 12 of 22
-------------------------	-----------------------------------	--	--------------------------

3.7.5 Updating product software

Due to the dynamics in IT, increasing requirements in connective networking, and the use of software libraries, updates are required.

We recommend that you check regularly to see if updates are available and to install any updates. Missed updates represent an acute security risk as attackers could have information on the vulnerabilities that are being rectified.

3.7.6 Protecting applications and apps

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

To secure applications, mobile and stationary end devices should also be protected that have access to the AHM Solution. This includes the regular installation of operating system and application updates as well as the use of a virus scanner.

To protect the customer system and customer data, the protection of access data of the end devices should also be ensured. Access data and certificates should be securely stored.

Version: 1.00	Document number: D055-1	File name: AHM Solution SAH70 - Security_Handbuch D055_EN.docx	Page: 13 of 22
-------------------------	-----------------------------------	--	--------------------------

4 Start-up (installation and configuration)

4.1 Target group

This section is directed to the operating personnel.

4.2 Requirements for personnel

The personnel must fulfill the following requirements:

- Has a professional qualification corresponding to this function and task.
- Authorized by the facility operator.
- Conversant with national regulations.
- Has read and understood information in the manual and additional documentation as well as certificates (depending on the application) before commencing work.
- Follows instructions and complies with general policies.

4.3 Installation

Install the product in accordance with the corresponding Brief Operating Instructions / Operating Instructions and connect electrically.

4.4 Configuration

4.4.1 Place the product in operation and configure

Place the product in operation and configure in accordance with the corresponding Brief Operating Instructions / Operating Instructions. Follow the instructions in this section and additional sections for the area of "security".

The AHM Solution start-up is implemented by the Endress+Hauser service department.

An integrity and authenticity check of the installation data must be carried out by the person who installs the product. The installation files are digitally signed for this purpose.

Right-click on the installation files for this and select the properties of the file.

Version: 1.00	Document number: D055-1	File name: AHM Solution SAH70 - Security_Handbuch D055_EN.docx	Page: 14 of 22
-------------------------	-----------------------------------	--	--------------------------

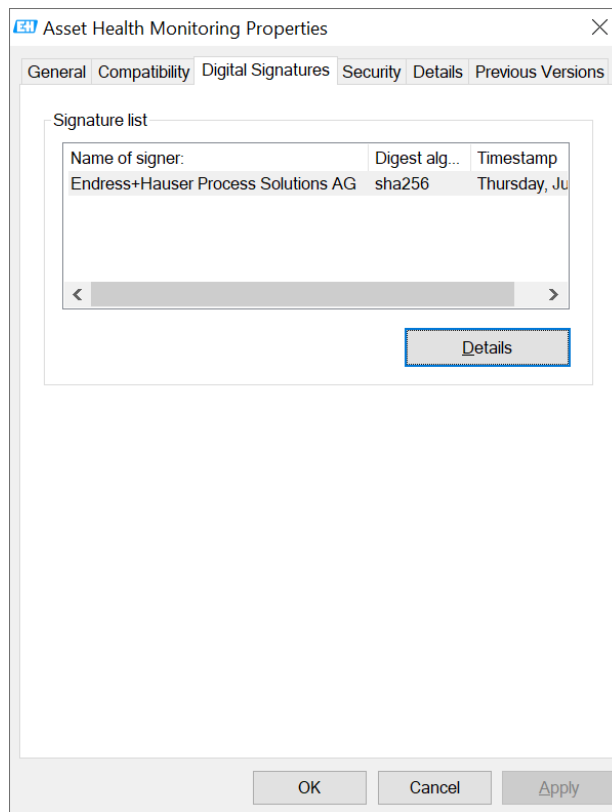


Figure 2 Checking the digital signature

Switch to the tab "Digital Signatures" and verify the "Name of Signer" contains "Endress+Hauser Process Solutions AG". If the tab "Digital Signatures" is missing or the "Name of Signer" is different, the file should not be run under any circumstances. The file is not from Endress+Hauser and may contain malware.

It is recommended that the AHM server and PAM gateway be operated on a single host and are not installed on separate hosts. Communication between these does not take place over an encrypted channel in the current version of the solution. If, for technical reasons, it is not possible to install these on a single host, we recommend that particular attention be given to the measures described in section 3.7.1.

 System overview AHM Solution: → 3.2

4.4.2 Required security steps during start-up

Activating HTTPS for the web application

To ensure the web application communications are encrypted and the user can verify the authenticity of the application, HTTPS must be activated. In addition we recommend the use of a certificate specially generated for the server.

Deactivating the PAM service on the PAM gateway

The PAM service is a background service that offers services that are not used in the AHM Solution. It is therefore recommended that the PAM service and the PAM agent be deinstalled on the PAM gateway. Open Windows settings for this and deinstall the two applications as shown in Figure 3 Deinstallation of software that is not required.

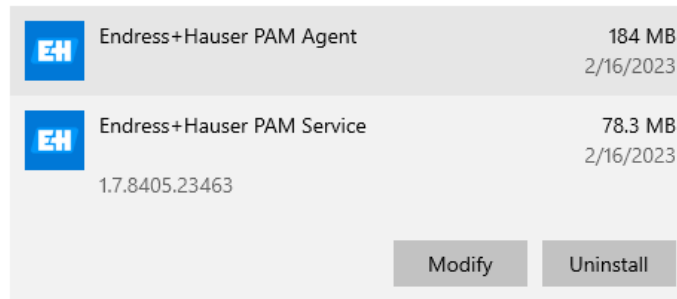


Figure 3 Deinstallation of software that is not required

4.4.3 Configuring the firewall

Only the following ports may be enabled in the Windows firewall for operating the AHM Solution:

- TCP 443 (HTTPS for access to the web application)
There is no authorization on the interface in the current version of the AHM Solution. We therefore recommend where possible to restrict the scope, whereby only connections from specific IP addresses are accepted (IP whitelisting).

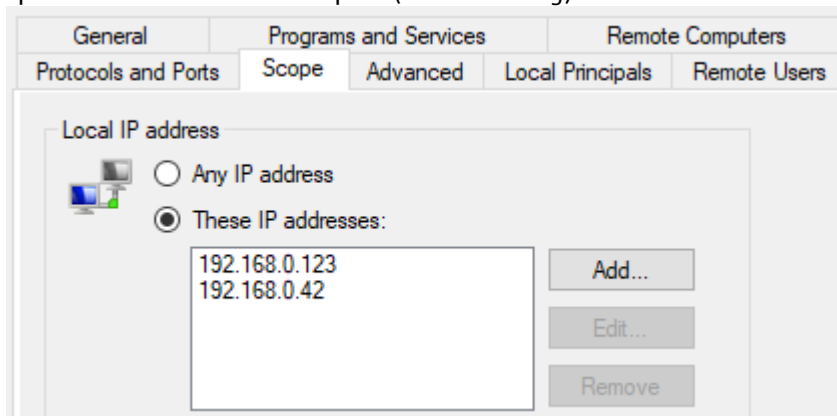


Figure 4 Specifying scopes in a firewall rule

- TCP 8302 (port for connecting PAM clients)
Non-secured connection which should only be permitted if configuration via PAM clients is used.
We recommend when setting up firewall authorizations to also configure the scope, and to only permit connection from IP addresses which are authorized PAM clients.
- TCP 1433, UDP 1434 (port for communication between AHM server and PAM gateway)
Only on the PAM gateway, if the AHM server is operated on another host.
We also recommend in this instance when setting up firewall authorizations to configure the scope, and to only permit connection of the AHM server.

4.4.4 Hardening the product

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

Web Reporter

Web Reporter is a module of FieldCare 2 that is supplied with the AHM Solution. Web Reporter is no longer maintained and we therefore recommend that it be deactivated.

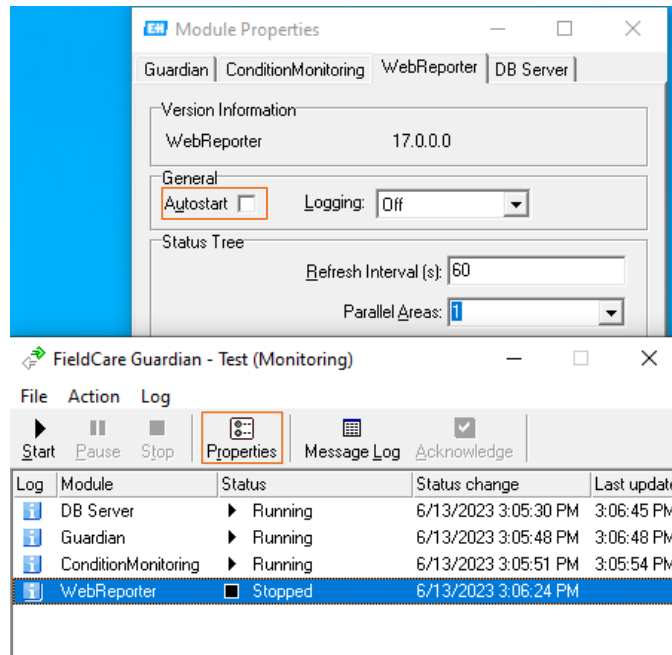


Figure 5 Deactivating Web Reporter

Communication Service

If configuration via PAM clients is not used, the Communication Server should be deactivated in the FieldCare Administration on the PAM gateway. For the corresponding configuration, see installation instructions 2.3.5

If configuration via PAM clients is used, the measures described in section 3.7.1 must be followed.

If possible, we recommend that the Communication Service only be activated temporarily.

4.4.5 Configuring user data

User data includes, for example login data, user, tag name, passwords, IDs etc.

see FieldCare Operating Instructions section 3.1.2

4.4.6 Security-relevant configuration of the product

Log level

The product is installed with a secure log level. Lower log levels, such as trace or debug, can contain information about field devices, and should only be temporarily configured for diagnosing problems. Log files must always be handled confidentially.

4.4.7 User management and effects on security

see FieldCare Operating Instructions: → 2.3.1

5 Operations

5.1 Target group

This section is directed to the operating personnel.

5.2 Requirements for personnel

The personnel must fulfill the following requirements:

- Has a professional qualification corresponding to this function and task.
- Authorized by the facility operator.
- Conversant with national regulations.
- Has read and understood information in the manual and additional documentation as well as certificates (depending on the application) before commencing work.
- Follows instructions and complies with general policies.

5.3 Tasks during operation

Operate the product according to the corresponding Operating Instructions. Follow the instructions in this section and following sections for the area of "security".

When entering passwords, care must be taken to ensure that no-one can observe the information that has been input. If a password is no longer trustworthy, the corresponding user account must be blocked or the password changed.

In the browser, the user must validate the secure connection to the AHM server during access to the AHM server, which is mostly indicated by means of a padlock next to the address line.

When exiting the workspace, the user must log out of their computer to prevent unauthorized access to the product.

5.4 Security aspects during operation

Windows updates

Windows updates must be regularly carried out for the host system on which the AHM Solution is installed.

HTTPS certificates

The certificates for the HTTPS connection have a limited service life and must be regularly updated.

5.5 Update management

Endress+Hauser provides updates for the AHM Solution. Updates are installed by the Endress+Hauser service department.

Endress+Hauser provides updates for the following cases:

- Security updates
- Bug fixes: troubleshooting of existing functions
- Functional upgrades of the product

Version: 1.00	Document number: D055-1	File name: AHM Solution SAH70 - Security_Handbuch D055_EN.docx	Page: 18 of 22
-------------------------	-----------------------------------	--	--------------------------

Security Manual**Asset Health Monitoring Solution SAH70**

Security Guideline

Endress+Hauser ensures the integrity and authenticity of the updates using checksums and signatures in the software. An integrity and authenticity check of the updates must be carried out by the person who installs the update. Information on how to check the signature is contained in section 4.4.1.

Updates are published in the Endress+Hauser software portal:

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

5.6 Repeating the threat analysis

The threat situation of facilities can change as a result of external events such as, for example, the occurrence of previously unknown attack patterns. In accordance with VDI/VDE 2182-1-2011, section 4.4, the threat analysis must be repeated and updated at regular intervals or in case of changes to the facility that may affect the threat analysis.

5.7 Repair and disposal

/

Version:	Document number:	File name:	Page:
1.00	D055-1	AHM Solution SAH70 - Security_Handbuch D055_EN.docx	19 of 22

6 Shutdown

6.1 Target group

This section is directed to the operating personnel.

6.2 Requirements for personnel

The personnel must fulfill the following requirements:

- Has a professional qualification corresponding to this function and task.
- Authorized by the facility operator.
- Conversant with national regulations.
- Has read and understood information in the manual and additional documentation as well as certificates (depending on the application) before commencing work.
- Follows instructions and complies with general policies.

Version: 1.00	Document number: D055-1	File name: AHM Solution SAH70 - Security_Handbuch D055_EN.docx	Page: 20 of 22
-------------------------	-----------------------------------	--	--------------------------

6.3 Shutting down the product

There are various reasons for shutting down the product. Depending on the reason for the shut-down, specific measures are required.

Reason for the shutdown	Required measures
The product is not used over a long period of time.	Switch off the hosts systems, or if not possible, at least end the processes
The product has a fault and you are unable to rectify the fault.	Contact Endress+Hauser
You want to dispose of the product.	We recommend that, before disposing of or scrapping physical media on which the product is installed, you follow the following guidelines: NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization

7 Appendix

7.1 Security checklist for the product life cycle

Life cycle	Task	Approved
Planning	Typical operating environment of the product defined and taken into account for planning. → 3.4 If required, alternative measures taken into account. → 3.5	<input type="checkbox"/>
	Planning work in the engineering phase considered. Threat analysis and risk assessment carried out. → 3.6	<input type="checkbox"/>
	Where possible, measures to reduce risks considered. → 3.7	<input type="checkbox"/>
Goods receipt / transport	Checks carried out to ensure that the supplied files identify Endress+Hauser as the manufacturer	<input type="checkbox"/>
Commissioning	Product hardened for the application case. → 4.4	<input type="checkbox"/>
Operations	Core instructions for operations followed. → 5.3, 5.4	<input type="checkbox"/>
	Core instructions for update management followed. → 5.5	<input type="checkbox"/>
	Planning of iterative threat analysis completed. → 5.6	<input type="checkbox"/>
Shutdown	Shut down the product. → 6	<input type="checkbox"/>

7.2 Version history

Document version	Software version	Changes
01.00	From 02.00.00	First version