

CEPE
Festo AX Controls

FESTO

Manual



8264959

8264959
2026-08a
[8264960]

Original instructions

CODESYS, Chrome, DisplayPort, Docker, EtherCAT®, FIREFOX, Linux, Microsoft, MODBUS, OPC UA, PHOENIX CONTACT, PLCNEXT COMMUNITY, PLCNEXT CONTROL, PLCNEXT STORE, PLCNEXT TECHNOLOGY, Python, Simulink, strongSwan are registered trademarks of the respective trademark owners in certain countries.

Table of contents

1	Home	7
1.1	Welcome to Festo AX Controls – The Open Automation Platform	7
1.1.1	Short introduction	7
1.1.2	Sources of information	8
1.1.3	Getting in touch with others	8
1.2	About this manual	8
1.3	Legal information	9
1.4	Safety notes	9
1.5	Version history	10
2	Licensing	11
2.1	Overview	11
2.2	Activate licenses with Festo Automation Suite	11
2.3	Activate licenses with WBM	14
3	Product range	20
3.1	Overview	20
3.2	Firmware releases	20
3.2.1	Release history	20
3.2.2	Firmware updates	21
3.3	Hardware documentation	21
4	Festo AX Controls features	22
5	Release notes	24
5.1	Overview	24
5.2	Festo AX OS Version 26.3.1.4	24
5.3	Festo AX OS Version 25.9.2.4	24
5.4	Festo AX OS Version 25.0.1.46	25
6	Operating System	26
6.1	Overview	26
6.2	Text editors	26
6.3	Overlay file system	26
6.4	Reset to default settings	26
6.5	System time	28
6.5.1	Default time zone	28
6.5.2	Changing the system time on a controller	28
6.6	Connecting to the controller	28
6.6.1	Web-based Management	28
6.6.2	Festo Automation Suite	28
6.6.3	For executing commands on the controller	28
6.6.4	For copying or editing files	29
6.6.5	Default System Use Notification	30
6.7	User rights	30

7	Security.....	31
7.1	Overview Industrial Cyber Security.....	31
7.2	Unused interfaces.....	31
7.3	Built-in features.....	31
7.4	Security settings via WBM.....	35
7.5	Password complexity rules.....	36
7.6	Authentication failure handling.....	37
7.7	Initial secure setup.....	38
7.7.1	Checking the CEPE.....	38
7.7.2	Get Familiar with the CEPE.....	39
7.7.3	Power supply.....	40
7.7.4	Software.....	40
7.7.5	Set BIOS Administrator Password.....	41
7.7.6	Connect.....	43
7.7.7	Setup Certificate.....	59
7.7.8	Configuring basic firewall settings.....	62
7.7.9	Security Logging.....	63
7.7.10	Further setup.....	64
7.7.11	User Data Protection.....	64
7.8	LDAP file-based configuration.....	67
7.8.1	Concept.....	67
7.8.2	Reference.....	67
7.9	Security context.....	71
7.10	Security Hardening.....	75
7.11	Configuring Central logging.....	76
7.12	Configuring Software Updates.....	77
7.13	Reset Procedures.....	83
7.14	Troubleshooting Guide.....	86
8	Web-based Management.....	87
8.1	Establishing a connection to WBM.....	87
8.2	Login to Web-based Management.....	87
8.3	Start page – areas and functions.....	88
8.4	Overview.....	89
8.5	Device.....	89
8.6	Diagnostics.....	89
8.6.1	Log Download.....	89
8.6.2	Notifications page.....	90
8.6.3	Notifications filter.....	90
8.6.4	Notifications table.....	91
8.6.5	Example Notifications Filter and Download.....	92
8.7	Configuration.....	92
8.7.1	Date & Time.....	92
8.7.2	Web services.....	96
8.7.3	Network.....	97
8.7.4	PLCnext Store.....	97
8.8	Security.....	98
8.8.1	Security Note.....	98
8.8.2	Certificate management.....	98

8.8.3	Firewall.....	101
8.8.4	User management.....	105
8.8.5	User policies.....	107
8.8.6	LDAP configuraton.....	109
8.8.7	Syslog.....	111
8.9	System.....	112
8.9.1	Device maintencance.....	112
8.9.2	License management.....	115
8.9.3	App management.....	116
8.9.4	Update.....	117
8.9.5	System services.....	118
8.9.6	Backup and Restore.....	120
8.10	Help.....	125

1 Home

1.1 Welcome to Festo AX Controls – The Open Automation Platform

With Festo AX Controls – The Open Automation Platform, and our portfolio for industrial electrical automation, we are offering you a complete system solution from a single source for the first time. With end-to-end software for end-to-end data utilisation that is real-time capable, flexible, expandable and secure
→ www.festo.com/ax-controls.

Festo AX OS is the firmware for Festo AX Controls controllers, which is based on PLCnext Technology. In the following, we will then speak of PLCnext.

If you're completely new to PLCnext Technology, you might find it helpful to get the gist and read about some use cases in the PLCnext Community first:

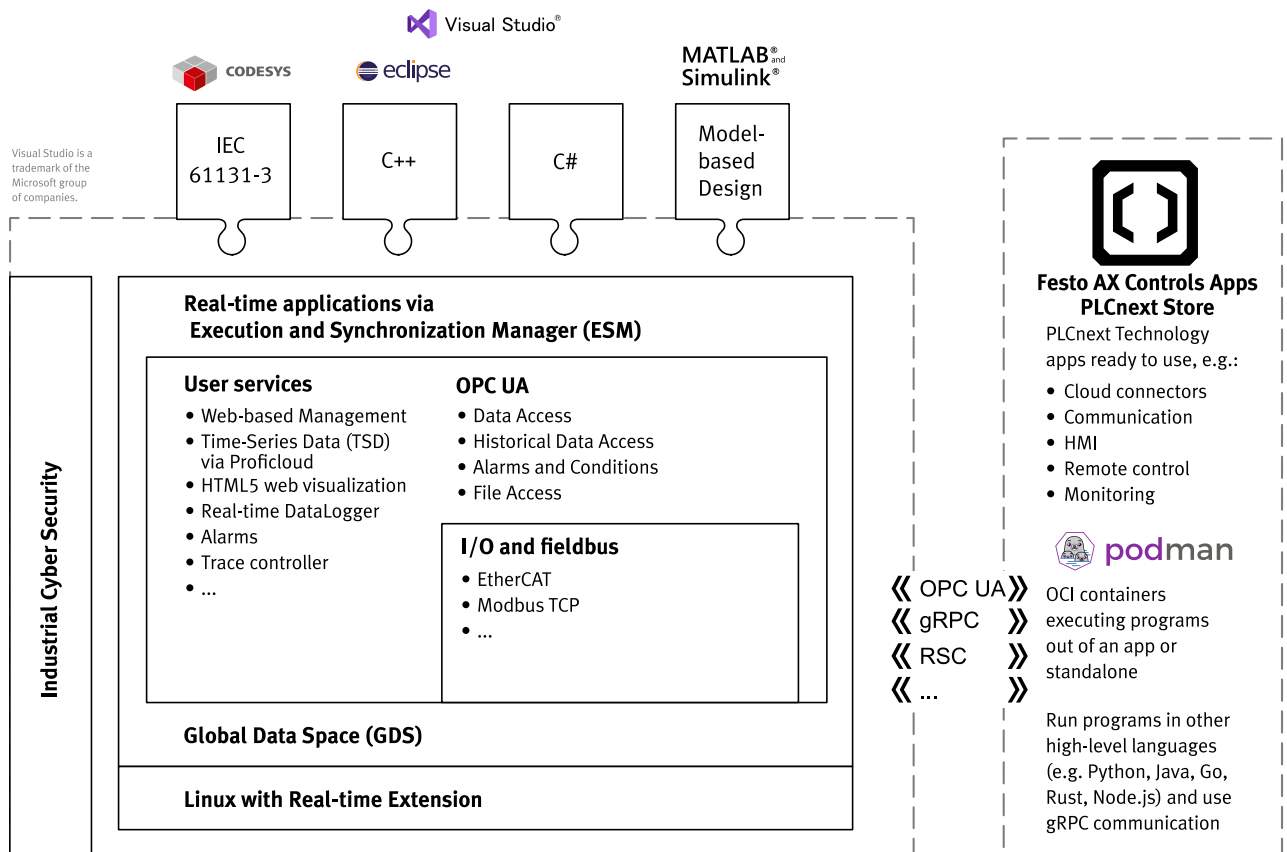
→ www.plcnext-community.net → About PLCnext Technology.

See also

- → 1.2 About this manual
- → 1.4 Safety notes
- → 3 Product range
- → 3.2 Firmware releases
- → 1.3 Legal information

1.1.1 Short introduction

Compared to the classic PLC you'll maybe know well already, the firmware of a Festo AX Controls device is different. The key feature is the openness of the whole system. To take you on board of this whole new world of opportunities, the following graphic gives an overview.



PLCnext Runtime System The PLCnext Runtime System is at the heart of the firmware. Its main parts are shown in the center. It is sitting on a PLCnext-specific, real-time capable Linux derivative which is the operating system on every PLCnext Control. From that base, you can choose the features and connection standards that suit your use case.

With Festo AX Controls, you can develop in the popular IEC 61131-3 languages, with Simulink models, and even in high-level languages. Code of all sources plugs into the PLCnext Runtime System to run synchronized by means of its core components, the ESM and the GDS.

1.1.2 Sources of information

There are various sources of information on the subject of PLCnext Technology, depending on your requirements and on which facet of PLCnext Technology you are looking for.

The following overview should help you to find the right source of information.

- Manual Festo AX Controls (this one!)
- Cyber security measures: → www.festo.com/sp → Search for CEPE → Downloads → Expert knowledge, Security Whitepaper for Festo controllers.
→ Security Whitepaper for Festo PLC
- Application notes, e.g. for programming in Python and USB3 Vision camera devices:
→ www.festo.com/sp, search for the device like "CEPE" → Downloads
→ Expert knowledge.
- Festo App Store → www.festo.com, search for the device like "CEPE".
PLCnext Store → www.plcnextstore.com/, filter for the devices from Festo.
- → CODESYS help
User documentation for the programming software CODESYS.
- PLCnext Technology C++ API programming reference
→ <https://api.plcnext.help/>.
User documentation for C++ programmers.
- PLCnext Technology on GitHub → <https://github.com/plcnext>
C++ / C# examples, scripts, and frameworks by PLCnext Technology.
- PLCnext Technology support forum → www.plcnext-community.net → Forum.
Swap ideas with other users and with PLCnext Technology's Technical Support.

1.1.3 Getting in touch with others

Getting in touch with others

Your questions, hints, and feedback are always welcome. Do not hesitate to connect with other PLCnext Technology users around the world, and our passionate PLCnext Technology team at PLCnext Technology.

- For development-related questions or hints, visit the PLCnext Community
→ www.plcnext-community.net → Forum.
- For further product information, application, and use cases, contact the regional Festo contact → www.festo.com/contact
- For feedback to this information platform, please send an email to axcontrols@festo.com.

1.2 About this manual

Application

This document describes the Festo AX Controls platform for industrial automation. It describes the Festo AX OS and its components, and it provides instructions on creating, using, and managing PLCnext Technology applications.

More information on PLCnext Technology is available in the PLCnext Community
 ➔ www.plcnext-community.net

Qualification of users

The use of products described in this user information is oriented exclusively to qualified application programmers and software engineers. The users must be familiar with the relevant safety concepts of automation technology as well as applicable standards and other regulations. Programming applications requires familiarity with IEC 61131-3 languages, C/C++, C#, and/or Simulink. In addition, users must always regard the general ➔ 1.4 Safety notes!

Notes



With this symbol, find additional information or detailed sources of information.

1.3 Legal information

General terms and conditions of use for technical documentation



See ➔ www.festo.com/sp, Link "Terms of use for electronic documentation".



All available documents for the product ➔ www.festo.com/sp.

Trademarks

Product names used in this website are trademarks of the respective owners. See front inside cover.

Licensing information on open source software

Controllers of the Festo AX Controls product family work with a Linux operating system. All license information can be found on the 'Licences' page of the Web-based Management (WBM) ➔ Licenses for all of the open source software used are shown.

How to contact us

- For technical issues, contact the regional Festo representative
 ➔ www.festo.com/contact.
- Accessories ➔ www.festo.com/catalogue.
- Cyber security information ➔ www.festo.com/psirt.

Your questions, hints, and feedback are always welcome. Do not hesitate to connect us via axcontrols@festo.com.

Make sure you always use the latest documentation that is available for your products. It can be downloaded at ➔ www.festo.com/sp, search for the product type.

1.4 Safety notes

Risk of unauthorized access to network

Accidental or improper execution of functions on the product can lead to failure or malfunction of the product and thus the entire connected system. In addition, unauthorised access to information stored on the product may be possible. The system operator must therefore take appropriate measures to prevent accidental or improper access to the product



Information on Cyber-security: ➔ www.festo.com/psirt ➔ Security Whitepaper for Festo controllers.

Risk of unauthorized access to devices

Devices with PLCnext Technology do not feature mechanical access protection and are therefore at risk of manipulation. Unauthorized access can occur via device interfaces, for example:

- USB ports
- Device HMI (touch panel as well as buttons, switches, etc.)
- Ethernet interfaces

To prevent damage, data corruption, loss of data, or misuse of data due to authorized access, make sure that only authorized access is possible.

- Protect the interfaces by installing the devices in a control cabinet.
- Secure the control cabinet with a lock.
- Make sure that only authorized persons have access to the control cabinet key.
- Run cables in such a way that they are protected against unauthorized access.

1.5 Version history

While the Festo AX Controls ecosystem evolves, we keep adding and elaborating this document. The following changes have been made since it is available. Note the reverse order - most recent changes are at the top!

Version	Changes
2026-07a	- Based on firmware release 26.3.1.4 ➔ 5.2 Festo AX OS Version 26.3.1.4. - Notes for firmware release 25.9.2.4 ➔ 5.3 Festo AX OS Version 25.9.2.4. - Updated licensing with WBM ➔ 8.9.2 License management and ➔ 2 Licensing. - Updated information on Security ➔ 7 Security. - Added information on ➔ 7.7.3 Power supply. - Reset via USB ➔ 6.4 Reset to default settings. - Updated information on WBM ➔ 8 Web-based Management. - Added information on Backup and Restore ➔ 8.9.6 Backup and Restore.
2025-07	- Published initially. - Based on firmware release 25.0.1.46 ➔ 5.4 Festo AX OS Version 25.0.1.46.

Tab. 1: Version history

2 Licensing

2.1 Overview

There are 2 ways to activate your licenses:

- Online activation with Festo Automation Suite ➔ 2.2 Activate licenses with Festo Automation Suite.

Preferred way, as more comfortable.

Prerequisites:

- MyFesto account. Purchased licenses with the corresponding customer number. Account must be linked to customer number.
- PC with Festo Automation Suite and connection to internet and connection to CEPE.
- Offline activation in the WBM via Licence Portal (LP), see ➔ 2.3 Activate licenses with WBM.

Offline means: CEPE, WBM and engineering PC can be Offline (without internet connection).

- Festo CODESYS licenses

License Portal must be used, as the CODESYS licenses are not available in WebDepot.

- Festo licenses.

2.2 Activate licenses with Festo Automation Suite

Activation with Ticket-ID – preferred way!

Prerequisite: Festo Automation Suite Version 2.12.0.436 or later.

1. Select the device in the 'Device Scan' section of the Festo Automation Suite.
2. Select 'Licenses' in the right panel.
3. Select 'Available Licenses'.
4. Click 'Enter a Ticket ID'.
5. The dialog 'License Activation' opens.

License Activation

1 > 2 > 3

Enter the license key (ticket) for a valid license for the selected device, then click "Next" to continue activation.

Device Name	Device Type	Address	Product Key
CEPE	CEPE	192.168.1.10	[REDACTED]

License Key (Ticket)

Next **Cancel**

6. Enter the License key.

License Activation

1

>

2

>

3

Enter the license key (ticket) for a valid license for the selected device, then click "Next" to continue activation.

Device Name	Device Type	Address	Product Key
CEPE	CEPE	192.168.1.10	

License Key (Ticket)

Next

Cancel

7. Log-in to the device.

Device Login

1

>

2

>

3

Please sign in to the device to transfer the license to the device. Enter your credentials for: CEPE (device type), CEPE (device name).



User name

admin

Password

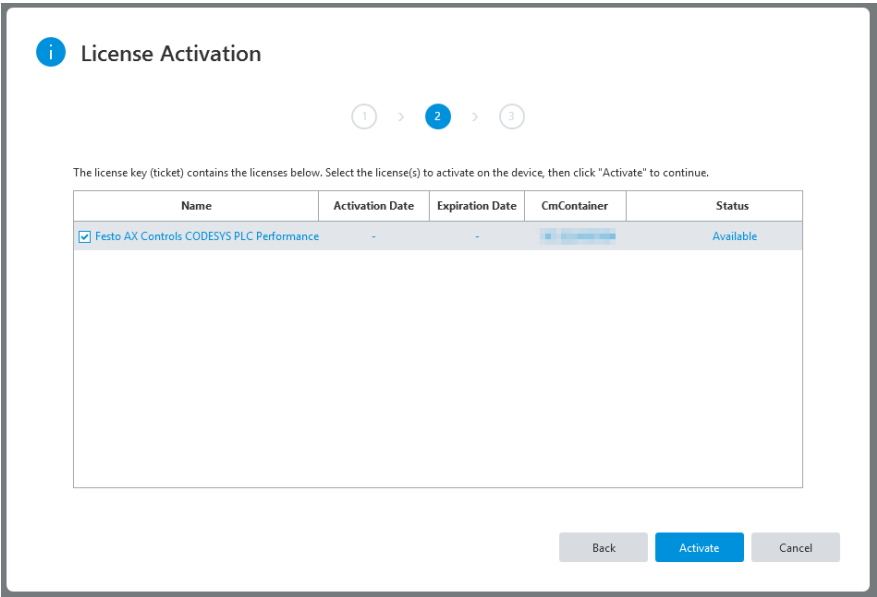
••••••••

Back

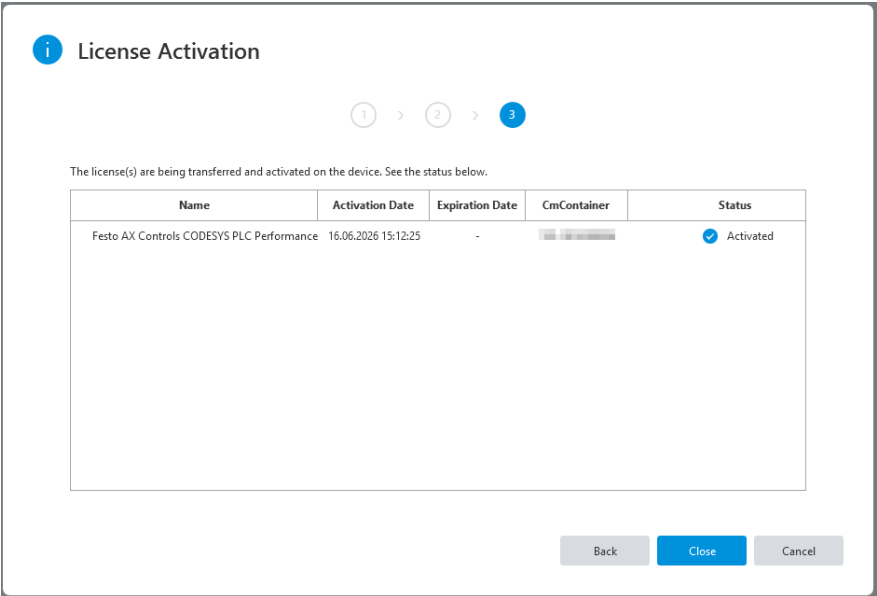
Login

Cancel

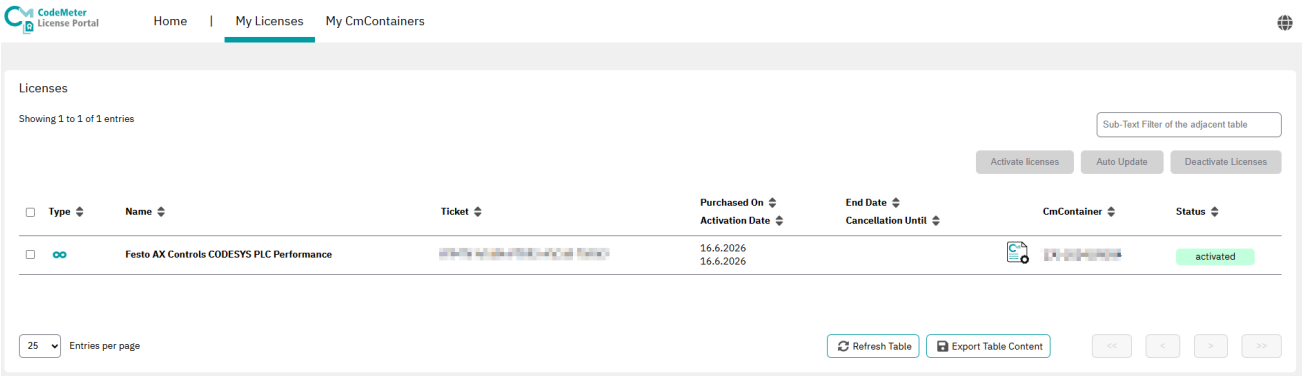
8. Select the license and click ‘Activate’.



9. Close the dialog.



10. Check the license in Codemeter.



Activation with MyFesto account

Prerequisites:

- MyFesto account. Purchased licenses with the corresponding customer number. Account must be linked to customer number
- PC with Festo Automation Suite with internet connection and connection to CEPE

1. Connect with 'Login' in the title bar to the MyFesto account.
2. Open device scan section.
3. Select device.
4. In the 'Actions' section select the 'Licenses' menu option.
Enter the password for the device. The factory default password for the user 'admin' is printed on the type plate.
⇒ Licenses available for the selected device are searched and displayed.
5. Select license.
⇒ Properties and information on the selected license are displayed.
6. Press the 'Activate' button.
⇒ The license is activated on the device.

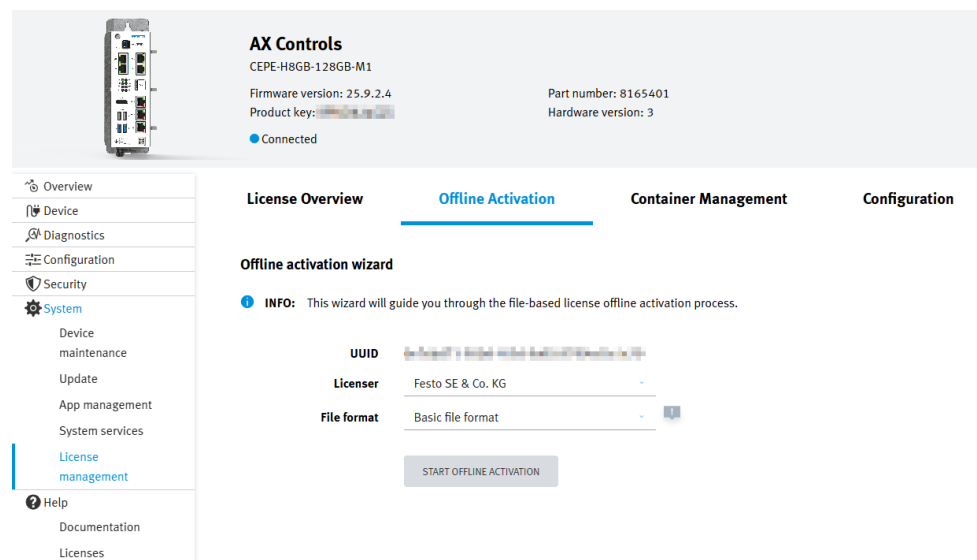
2.3 Activate licenses with WBM

1) WBM: Get License Request file

Log-in to WBM.

Open 'System' → 'License Management' page.

Click 'Start Offline Activation' button and get License Request file.

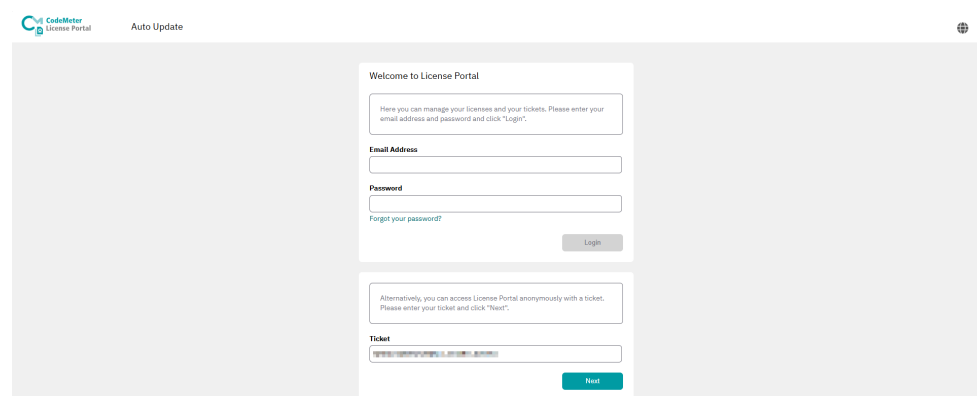


2) License Portal: Enter Ticket ID

Open License Portal in Browser.

LP (Prod) Adresse: ➔ <https://lc.codemeter.com/83810-prod/portal/>.

Enter Ticket-ID.



3) License Portal: Select license

Select the license by clicking the checkbox.

Click 'Activate licenses' button.

CodeMeter
License Portal

Home | My Licenses | My CmContainers

Licenses

Showing 1 to 1 of 1 entries

Sub-Text Filter of the adjacent table

Activate Licenses | Auto Update | Deactivate Licenses

☒	Type	Name	Ticket	Purchased On Activation Date	End Date Cancellation Until	CmContainer	Status
☒	∞	Festo AX Controls Python Trial		26.1.2026	1.7.2026		available active

25 Entries per page

Refresh Table | Export Table Content | << < > >>

4) License Portal: Target location another device

Select the target location: choose ‘Another Computer / Device’.
Important: The license needs to be activated on the device **not** on the (local) computer. Therefore **do not** choose ‘This Computer’!

CodeMeter
License Portal

Home | My Licenses | My CmContainers

Step 1 - Select Target Location

1. Location | 2. Container | 3. Summary | 4. Activation

This Computer

Choose this option, if you want to activate the license(s) at this Computer, either locally bound to this computer, or to a CmContainer, which is currently connected to this computer.

Another Computer / Device

Choose this option, if you want to activate the license(s) at another Computer, or an Embedded Device.

Expert Mode

Choose this option, if you are familiar with the activation workflow and you want to choose manually between all available CmContainers.

5) License Portal: Context File from a CmContainer

Select the target location: choose ‘I have a Context File from a CmContainer’.

CodeMeter
License Portal

Home | My Licenses | My CmContainers

Step 1 - Select Target Location - Another Computer / Device

1. Location | 2. Container | 3. Summary | 4. Activation

I have a Context File from a CmContainer

Choose this option, if you already have a Context File from the target CmContainer, where you want to activate the license(s)

I need help to create a Context-File

Choose this option, if you need help how to create a Context File of the target CmContainer at another Computer, or Embedded Device

I want to use a known CmContainer

Choose this option, if you want to activate the license(s) at a CmContainer which was already used, is known in this system and is linked to the used ticket, or account

123

I want to enter the serial number

Choose this option, if you want to enter the serial number of the target CmContainer manually. This requires that the CmContainer was already used and is known in the system

Select and upload the RaC file (from step 1).

CodeMeter
License Portal

Home | My Licenses | My CmContainers

Step 1 - Select Target Location - Another Computer / Device - I have a Context File from a CmContainer

1. Location | 2. Container | 3. Summary | 4. Activation

Datens auswählen

WilbuCmRaC

Upload

Select the given CmContainer and click ‘Continue’.

The screenshot shows the 'Step 2 - Select CmContainer' page in the CodeMeter License Portal. The page has a navigation bar with 'Home', 'My Licenses', and 'My CmContainers'. Below the navigation bar, there are four steps: 1. Location, 2. Container (active), 3. Summary, and 4. Activation. A 'Continue' button is visible. The main content area shows a table with columns: Connected, Type, CmContainer, Local Name of CmContainer, Portal Name of CmContainer, Hostname, and Owner. The table contains one entry for 'License Request File'. At the bottom, there is a '25 Entries per page' dropdown and an 'Export Table Content' button.

6) License Portal: Click 'Transfer Licenses'.

The screenshot shows the 'Step 3 - Summary' page in the CodeMeter License Portal. The page has a navigation bar with 'Home', 'My Licenses', and 'My CmContainers'. Below the navigation bar, there are four steps: 1. Location, 2. Container, 3. Summary (active), and 4. Activation. A 'Transfer Licenses' button is visible. The main content area shows a table with columns: Action, Ticket, Name, Amount, End Date, Activation Date, Target CmContainer, and Current CmContainer. The table contains one entry for 'Festo AX Controls Python Trial 1'. At the bottom, there is a '25 Entries per page' dropdown and an 'Export Table Content' button.

A WibuCmRaU File is downloaded automatically.

If not the download can be triggered again by clicking 'Download licensese update again'".

Keep the dialog open and switch to the WBM for uploading the WibuCmRaU file.

The screenshot shows the 'Step 3 - Summary' page in the CodeMeter License Portal. A 'Synchronize CmContainer' dialog box is open in the center. The dialog box has a 'Download license update again' button and a 'Pick license receipt file (*.WibuCmRaC) *' section. The 'Pick license receipt file' section shows a file selection interface with a 'Datei auswählen' button and a 'Keine Datei ausgewählt' status. The dialog box also has 'Cancel' and 'OK' buttons. In the background, the 'Step 3 - Summary' page is visible, showing the same table as the previous screenshot. A file explorer window is also open in the top right corner, showing the contents of the 'WibuCmRaU' folder.

Upload the WibuCmRaU in WBM

Offline license activation

1

2

3

License context

License upload

License receipt

Upload license update file

First select the WibuCmRaU file:

Select File

No file selected.

Cancel

Back

Next

Click 'Next'.

Offline license activation

1

2

3

License context

License upload

License receipt

Upload license update file

Status

The license update file has been successfully uploaded.

Cancel

Back

Next

Download the WibuCmRaR file.

Offline license activation

1

2

3

License context

License upload

License receipt

Create a license receipt file

First download the WibuCmRaR file to your PC:

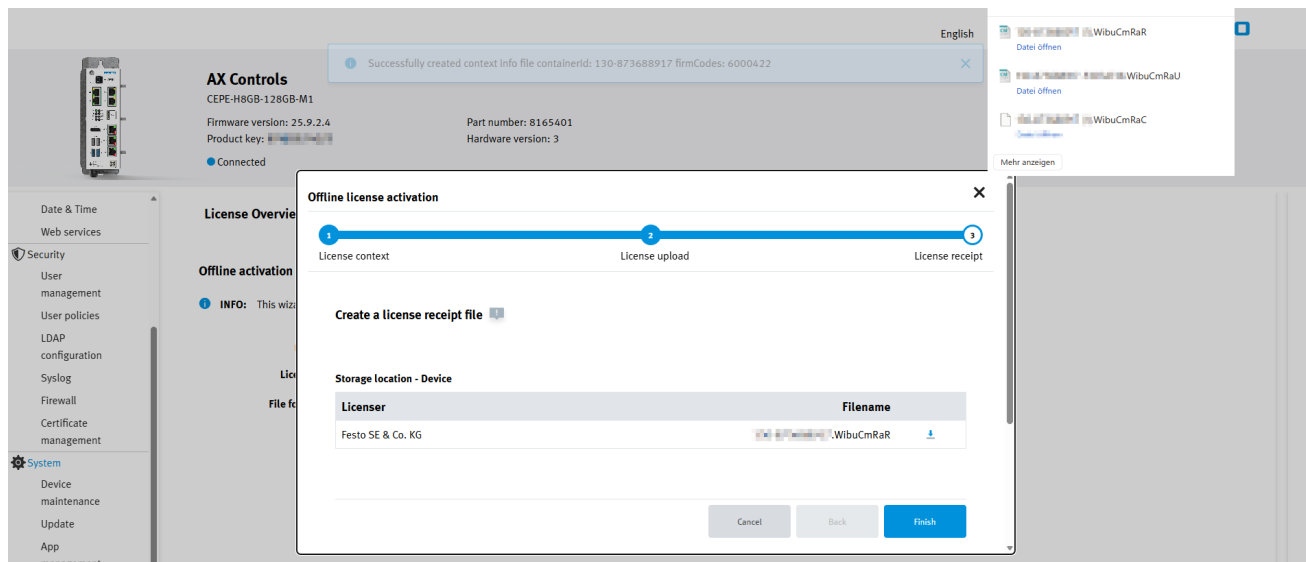
Storage location - Device

Licensor	Filename
Festo SE & Co. KG	.WibuCmRaR

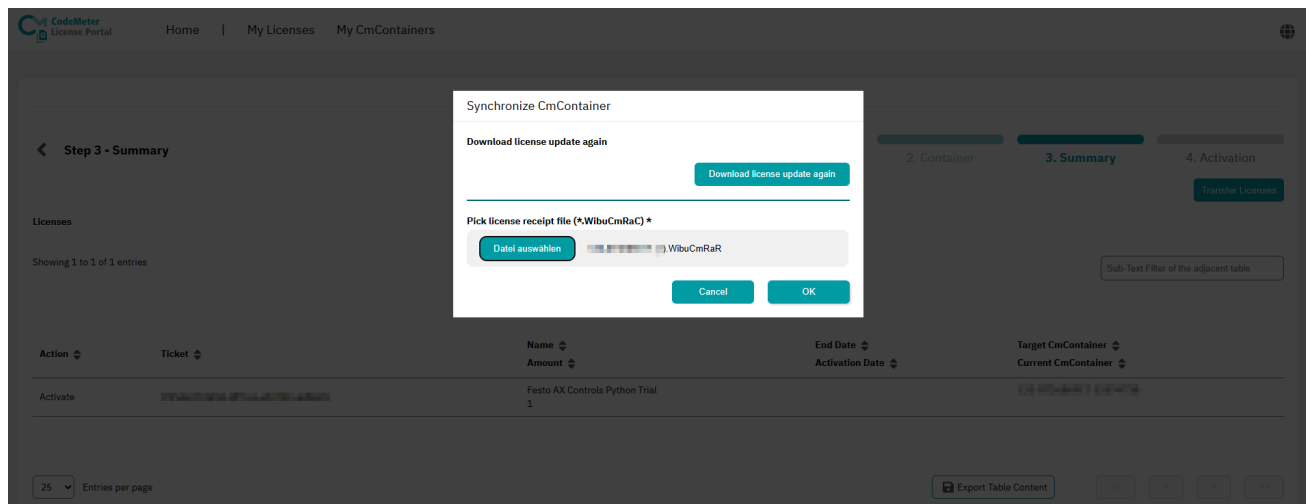
Cancel

Back

Finish



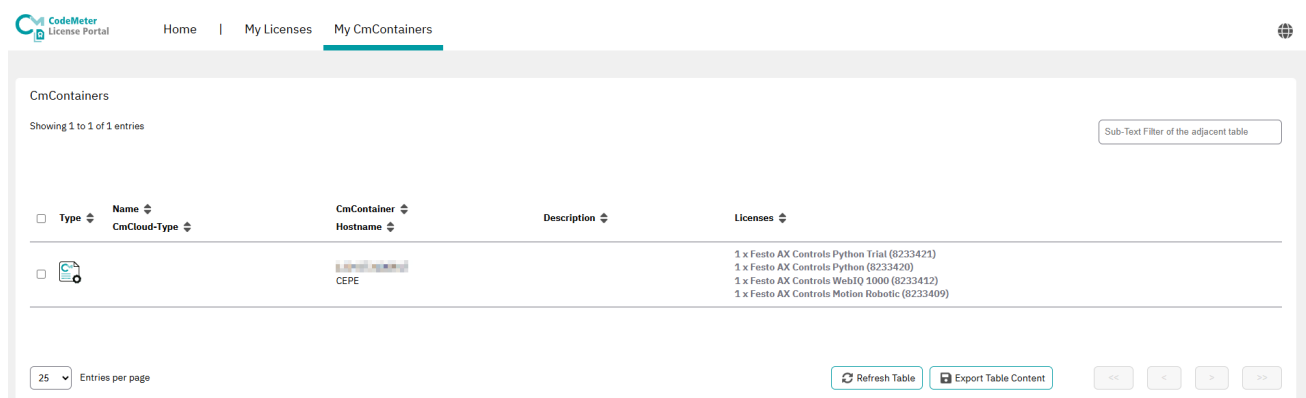
Switch back to the WIBU LP.
Upload the WibuCmRaR file.



Click 'OK'.
Finished!

7) License Portal and WBM: Check the activation status

In WIBU License Portal:



In WBM:

Englishadmin Logout in 19:33FESTO



AX Controls

CEPE-H8GB-128GB-M1

Firmware version: 25.9.2.4

Product key: 

● Connected

Part number: 8165401

Hardware version: 3

License OverviewOffline ActivationContainer ManagementConfiguration

CODESYS GmbH

License container: 

Product codeProduct textFeature map

8233409Festo AX Controls Motion Robotic0...

8233412Festo AX Controls WebIQ 10000...

8233420Festo AX Controls Python0...

8233421Festo AX Controls Python Trial0...

Refresh

REVERT PAGESAVE PAGE & RESTART

Date & Time

Web services

Security

User management

User policies

LDAP configuration

Syslog

Firewall

Certificate management

System

Device maintenance

Update

App management

System services

License management

Help

Documentation

Licenses

Festo — CEPE — 2026-08a

19

3 Product range

3.1 Overview

The information in this Info Center is about the PLCnext Runtime System, which is the firmware on Festo AX Controls devices. In addition, use cases with related hardware and software are described if useful in the course of a documented feature.

Each Festo AX Controls device comes with its own hardware documentation, which can be a data sheet containing the commissioning of the controller, or a user manual. For more details, see Hardware documentation → 3.3 Hardware documentation.

The engineering tools for Festo AX Controls devices, Festo Automation Suite and CODESYS, come with their own documentation in the form of an embedded help.

Covered Festo AX OS releases

This platform adds to the product information of these devices:

Type	Product	Firmware
CEPE-H8GB-128GB-C1	Control unit	25.0.1.46 or newer
CEPE-H8GB-128GB-M1	Control unit	25.0.1.46 or newer

Tab. 2



Note: For commissioning or disposing the hardware, see the respective user manual or data sheet → 3.3 Hardware documentation.

Related products

This platform adds to the product information for the following parts of the PLCnext Technology ecosystem:

Product	Product Type	Compatible to devices' firmware version
Festo Automation Suite	Engineering Software	25.0.1.46 or newer
CODESYS PLC 3.5 SP20	Engineering Software	25.0.1.46 or newer
WebIQ	App	25.0.1.46 or newer
Python	App	25.0.1.46 or newer
Node-RED	App	25.0.1.46 or newer
Motion Package Robotic (Single Axis, FTL)	App	25.0.1.46 or newer

Tab. 3



- For installing and using CODESYS, see → CODESYS help.
- For commissioning or disposing the hardware, see the respective user manual or data sheet → 3.3 Hardware documentation.

3.2 Firmware releases

3.2.1 Release history

The PLCnext Technology adventure at Festo began 2025 with the new CEPE controllers.

PLCnext Technology was originally developed in 2016 by PHOENIX CONTACT GmbH & Co. KG.

Firmware releases

This document spans the following firmware releases:

Release	Release date
26.3.1.4	September 2026
25.9.2.4	Januar 2026
25.0.1.46	July 2025

Tab. 4

Firmware releases on controllers

Festo AX Control	Release		
	25.0.1.46	25.9.2.4	26.3.1.4
CEPE-H8GB-128GB-C1	✓	✓	✓
CEPE-H8GB-128GB-M1	✓	✓	✓

Tab. 5

3.2.2 Firmware updates

You can download all available firmware releases for free in the Downloads section of your device's product page on ➔ www.festo.com/sp.



Before upgrading, check the Change notes for breaking changes! Find links to the regarding product pages linked in the Hardware documentation ➔ 3.3 Hardware documentation overview, or the pdf file in the already downloaded firmware zip package.

When updating the firmware, the licenses and also all modifications by the user are retained.
Licenses are not in the overlay file system but in a separate partition that remains during firmware update or factory reset ➔ 6.3 Overlay file system.

3.3 Hardware documentation

Festo AX Controls Hardware documentation

For each Festo AX Controls device or extension, there is a user manual or a data sheet available on the ➔ www.festo.com/sp website. For your convenience, we're making those PDF documents available for download here, too.
Where there's additional documentation mentioned, please refer to the respective product page on the PHOENIX CONTACT website.



See Festo AX Controls features or Extensions for the different purposes and restrictions of the following devices.

Festo AX Controls devices

Device	Product page facet	Additional sources
CEPE-H8GB-128GB-C1 CEPE-H8GB-128GB-M1	Downloads Operating instructions and Manuals ➔ www.festo.com/sp ➔ Search for CEPE ➔ Downloads ➔ User documentation	Information on Cyber-security: ➔ www.festo.com/sp ➔ Search for CEPE ➔ Downloads ➔ Expert knowledge, Security Whitepaper for Festo controllers.
	Downloads Application notes ➔ www.festo.com/sp ➔ Search for CEPE ➔ Downloads ➔ Expert knowledge, Application notes	

Tab. 6

4 Festo AX Controls features

In this topic you see the current features and the firmware release with which they have been implemented. For a sneak peek into our further development and current activities on key parts of the Festo AX Controls ecosystem, see the Development roadmap.

Festo AX Operating system

Festo AX OS version	25.0.1.46	25.9.2.4	26.3.1.4
based on the PLCnext Linux Operating System version	2025.0	2025.9	2026.0
Linux kernel	6.1 LTS	6.1 LTS	6.1 LTS
OSADL real-time Linux services, based on the PREEMPT_RT patches of the Linux kernel	✓	✓	✓
Performance enhancement – optimized kernel setting	✓	✓	✓
Docker ready	✓	✓	✓

Tab. 7

PLCnext Store interface

Festo AX OS version	25.0.1.46	25.9.2.4	26.3.x.x
based on the PLCnext Linux Operating System version	2025.0	2025.9	2026.0
License mechanism for apps (copy protection)	✓	✓	✓
PLCnext App offline installation	✓	✓	✓

Tab. 8

Industrial Cyber Security

Firmware version	25.0.1.46	25.9.2.4	26.3.1.4
Remote SSL connection	✓	✓	✓
User Management - predefined roles	✓	✓	✓
Firewall (nftables)	✓	✓	✓
VPN	✓	✓	✓
IPsec (strongSwan)	✓	✓	✓
Trust & Identity Store	✓	✓	✓
TLS Sockets	✓	✓	✓
LDAPS user authentication	✓	✓	✓

Tab. 9

Web-based Management (WBM) on PLC

Festo AX OS version	25.0.1.46	25.9.2.4	26.3.1.4
based on the PLCnext Linux Operating System version	2025.0	2025.9	2026.0
Login authentication	✓	✓	✓
User management	✓	✓	✓
LDAPS configuration	✓	✓	✓
Firewall configuration	✓	✓	✓
Certificate management (Trust and Identity Store)	✓	✓	✓
Firmware update	✓	✓	✓
PLCnext App installations overview	✓	✓	✓
PLCnext App status	✓	✓	✓
PLCnext App offline installation	✓	✓	✓
View and download system notifications	✓	✓	✓
Status information regarding Ethernet interfaces	✓	✓	✓
Configure an HTTPS certificate for nginx web server	✓	✓	✓
Configure IP settings	✓	✓	✓
Enable/disable System Services	✓	✓	✓

Festo AX OS version	25.0.1.46	25.9.2.4	26.3.1.4
based on the PLCnext Linux Operating System version	2025.0	2025.9	2026.0
Configure Syslog	✓	✓	✓
Overview	✓	✓	✓
Backup and restore page	–	–	✓

Tab. 10

Real-time C++ programming

Festo AX OS version	25.0.1.46	25.9.2.4	26.3.1.4
based on the PLCnext Linux Operating System version	2025.0	2025.9	2026.0
Real-time C++ programs	✓	✓	✓
Call of RSC services	✓	✓	✓
Threads	✓	✓	✓
Retain memory access	✓	✓	✓
TLS Sockets	✓	✓	✓
License management RSC services	✓	✓	✓
Support for component ports	✓	✓	✓
IDcpService, RSC service for scanning the network of a specific interface and for editing device parameters	–	✓	✓
IAcyclicCommunicationService, RSC service for implicit reading	–	✓	✓

Tab. 11

Web server

Festo AX OS version	25.0.1.46	25.9.2.4	26.3.1.4
based on the PLCnext Linux Operating System version	2025.0	2025.9	2026.0
Web-based Management in Festo AX Controls devices	✓	✓	✓
HTML5	✓	✓	✓
HTTPS	✓	✓	✓
REST data interface – access global and external variables	✓	✓	✓

Tab. 12

Notification Manager and Logger

Festo AX OS version	25.0.1.46	25.9.2.4	26.3.1.4
based on the PLCnext Linux Operating System version	2025.0	2025.9	2026.0
System notifications (diagnostic)	✓	✓	✓
View and download notifications via WBM	✓	✓	✓
Register, send, and receive notifications (C++)	✓	✓	✓
Log notifications (SQLite database)	✓	✓	✓
Security notifications – dedicated security log	✓	✓	✓

Tab. 13

5 Release notes

5.1 Overview

This section covers issues of the firmware releases from 25.0.1.46.



For security issues and possible vulnerabilities, see the security advisories of the Product Security Incident Response Team (PSIRT) → www.festo.com/psirt.

5.2 Festo AX OS Version 26.3.1.4

New Features

- Backup & Restore
 - Creation and deployment of encrypted backups
 - Downloading and uploading of encrypted backups
- Ability to install signed and unsigned apps after administrator configuration in the WBM

Changes

- Visual adjustments in the WBM

Security Hardening

- Issues with OpenSSL resolved
- Allowing installation of signed apps set as the default (already installed apps do not need to be signed)

Fixed Bugs

- Device IP range 192.168.2.10/24 available for use
- Configured network gateway is correctly displayed and applied during device scan
- OPC UA device information corrected
- "Bad Request" error on WBM login fixed
- Improved error handling when entering invalid TCP/IP configurations in the WBM
- MT LED now behaves correctly (as described in the manual)

Known Limitations

- Backup & Restore: Download of backup using Chrome or Edge Browser gets stuck after a few percent.
 - **Workaround:** use FIREFOX Browser instead or download via SSH/SCP. The following steps are necessary to download (or upload) a backup via SSH/SCP:
 1. Login with ssh and admin user
 2. Change directory: `cd /opt/plcnext/data/Services/BackupAndRestore`
 3. List existing (backup)files: `ls`
 download file:


```
scp admin@<device-ip>/opt/plcnext/data/Services/BackupAndRestore/<chosen-backup>.backup /local-dir/
```

 upload file: `scp /local-dir/<chosen-backup>.backup admin@<device-ip>/opt/plcnext/data/Services/BackupAndRestore/<chosen-backup>.backup`

5.3 Festo AX OS Version 25.9.2.4

New Features

- Web-Based Management (WBM):
 - Possibility to set the systemtime manually
 - Possibility to configure and sync the systemtime with an NTP server
 - Log/report download
 - Enable mounting of USB drives
 - Enabled usage of PHOENIX CONTACT licenses

- Show temperature gauge on overview page
- Redirection from HTTP to HTTPs by browser possible
- Support for USB3Vision

Changes

- Service configuration in WBM extended
- Performance improvements
- License offline activation in WBM shows correct default format
- New firmware archive provided
- Improved fan control
- Improved device SSH access in case of system failure

Security Hardening

- PLCnext Store service default off
- Enabled stricter user management ruleset
- Disabled possibility to deactivate user authentication

Fixed Bugs

- Show correct app license texts in WBM
- Help/Licenses page also available in German
- Fixed WBM help page
- Redirect to CODESYS WebVisu via <device-ip>/webvisu fixed
- "Reset to default" via hardware button bound to boot time
- Fixed behavior of power supply LED under certain scenarios
- Console login for 'Admin' via DisplayPort fixed
- Fixed retain data loss on certain scenarios
- Improved system shutdown at certain power fail scenarios

Known Issues

- Watchdog exception calling CODESYS Modbus FB
 - Usage of some licenses (e.g. Modbus) have a big performance spike at the initial license check and result in a long task execution time, resulting in a watchdog timer violation if watchdog is used
- Same error exists on Control Win V3 and therefore is a general CODESYS SP20 error
 - It is affecting CODESYS SL licenses as well as Festo CODESYS licenses
 - Workaround
 - Do not use watchdog for this tasks
- WBM: invalid/timeout session prints message but does not redirect to login page

5.4 Festo AX OS Version 25.0.1.46

Features

- Initial version of Festo AX OS (based on PLCnext Technology).
- Web-based Management as the user interface on every Festo AX Controls device, allowing access to static and dynamic controller information as well as modification of certain controller settings.
- Firmware update of the device.
- App and license management.
- User Management.
- Firewall with settings for input and output rules.
- System service management to enable and disable system services, e.g. like SSH.

Known Issues

- Web-Based Management (WBM):
 - Attempting to update a running (OCI container) app fails silently - no error message is shown, and the app is removed from the system.

Workaround: Stop app before updating it.

- App installation could fail on a clean device (first boot or after factory reset). Subsequent installs also fail until another factory reset is done.

Workaround: Perform a factory reset.

- CodeMeter causes CPU spikes, that could potentially violate task execution time.
- The system is expected to indicate its power state with a green LED; however, after power-on, the power supply LED initially shows green but then turns off unexpectedly.
- User login via local shell (DisplayPort and serial) is currently not possible.

6 Operating System

6.1 Overview

The PLCnext Technology control platform is based on a Linux operating system with the OSADL real-time patch → <https://www.osadl.org/OSADL-QA-Farm-Real-time.linux-real-time.0.html>. Linux is a highly reliable, open source operating system suitable for applications that require a high stability.

The operating system features the following components and services:

- Firewall (can be configured via the Web-based Management → 8.8.3 Firewall)
- SSH/SFTP
- NTP (Network Time Protocol)
- DNS

6.2 Text editors

Nano and Vim are installed on the controller as text editors. When you are connected to the controller via the SSH console, you can call the desired editor via the command line. To open a file with the desired editor, enter nano <file name> or vim <file name>.

Nano

The Nano text editor is easy to use and is therefore recommended for less experienced users. Find an introduction and documentation of features at the GNU nano website → www.nano.org.

Vim

The Vim text editor has an extended range of functions and is a popular editor in the Linux environment. Find an introduction and documentation of features at the Vim website → www.vim.org.

6.3 Overlay file system

The overlay filesystem stores the user modifications of the device (Configuration, project data, apps and app data) and is kept during firmware update but removed at factory reset.

6.4 Reset to default settings

Reset types

Two types of reset perform the following actions on the controller partitions:

- Reset to default settings Type 1
- Reset to default settings Type 2

Reset to default settings Type 1

This process deletes the overlay partition with the user data (such as apps, configuration, etc.) to reset the device to its default settings without altering the underlying base partition with the installed operating system.

**Note:**

- The last installed operating system remains active. It will not be reset to the factory settings.
- Installed licences will remain on the device
- The IP address will be reset to the default: 192.168.1.10/24

Reset to default settings type 1 with the WBM:

- Run the 'Reset the device ...' function in the 'Device Maintenance' → 'Device Control' section.

Reset to default settings type 1 with the reset button:

1. Press and hold the reset button.
2. Switch on the device.
 - ⇒ After approximately 5 seconds, the housing LED starts flashing, indicating the start of the factory reset sequence.
3. Release the reset button.
 - ⇒ Factory reset type 1 starts.
 - ⇒ Factory reset type 1 is being completed.
 - ⇒ The housing LED stops flashing.
4. The device restarts automatically at the end of the sequence.

Reset to default settings Type 2

This process deletes the overlay partition with the user data (such as apps, configuration, etc.) to reset the device to its default settings. Exactly the same as the Type 1 reset to the default settings.

The user also has the option of selecting an image file to select the version of the operating system for installation.

Reset to default settings type 2 with the reset button:

1. Press and hold the reset button.
2. Switch on the device.
 - ⇒ After approximately 5 seconds, the housing LED starts flashing, indicating the start of the factory reset sequence.
3. Continue to press and hold the reset button.
 - ⇒ After approximately 5 seconds, the housing LED starts flashing at double frequency, indicating the factory reset type 2 sequence.
4. Release the reset button.
 - ⇒ Factory reset type 2 starts.
 - ⇒ Factory reset type 2 is being completed.
 - ⇒ The housing LED stops flashing.
5. The device automatically restarts into the recovery system at the end of the sequence.

Reset via USB

How to perform a reset via USB:

1. Format USB stick in FAT32 (other file systems may work, but only FAT32 is guaranteed).
2. Create (at least) one partition.
3. Put a file into the partition: `_reset1.axc` or `_reset2.axc`, depending on the type of reset that should be executed.
4. Mount USB stick to supported port of the device.
5. Reboot or power cycle the device.
6. After a while, the reset should be successful.

6.5 System time

6.5.1 Default time zone

All Festo AX Controls devices are set by default to `UTC0` which is `UTC±00:00` of the Coordinated universal time (UTC → www.bipm.org).

6.5.2 Changing the system time on a controller

Setting via WBM

The preferred method to change the time is the WBM where manual time changes and NTP is possible → 8.7.1 Date & Time.

Using the NTP client

It is possible to connect to Network Time Protocol (NTP) servers or to start your own server.

Setting via WBM → 8.7.1 Date & Time.

Additional information

- Find a general overview to the Network Time Protocol daemon (ntpd) in the developer's introduction → www.eecis.udel.edu/~mills/ntp/html/ntpd.html
- Find a detailed description of the configuration options in the developer's documentation → www.eecis.udel.edu/~mills/ntp/html/confopt.html
- The PLCnext Runtime System already contains the NTP utilities (e.g. `ntpq` and `ntpd`) for diagnostic and monitoring purposes.

6.6 Connecting to the controller

6.6.1 Web-based Management

See → 7.7.6.1 Connecting to Web-based Management.

6.6.2 Festo Automation Suite

Example for the functions of Festo Automation Suite:

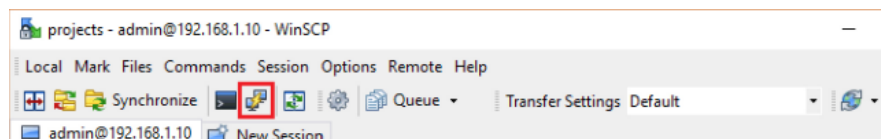
- Scan for devices
- Access the WBM of the controller by means of the device specific plug-in
- Change IP address or other network settings
- Update firmware
- Manage licences

Information on this functions or how to proceed see help of the Festo Automation Suite.

6.6.3 For executing commands on the controller

Using a Windows computer

1. If already connected to the controller using WinSCP, open the console by clicking the 'Open in PuTTY' button:
(You may also start PuTTY directly.)



2. At the prompt, enter the 'admin' user password for confirmation.
⇒ You're ready to issue Linux commands on the controller via the console:



Using a Linux computer

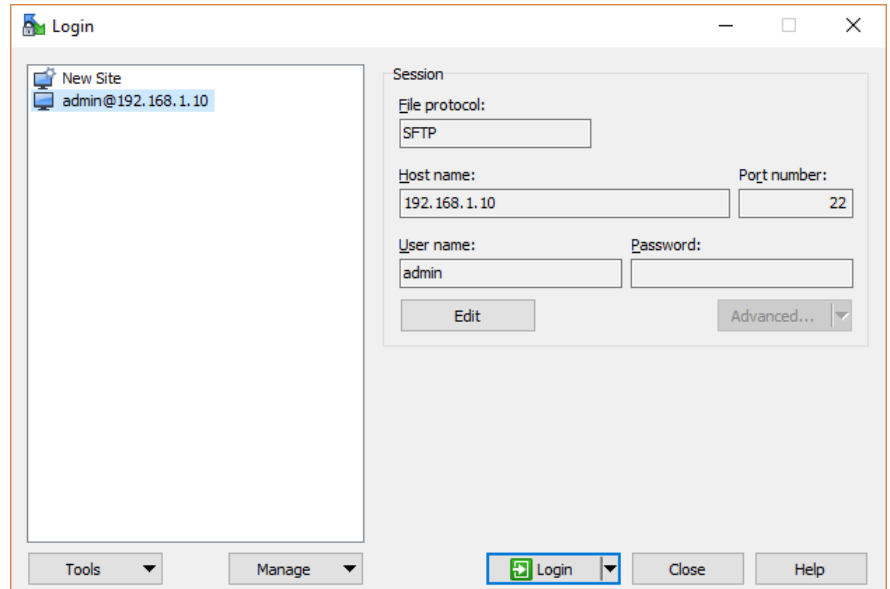
1. In a console, execute this command:
`ssh admin@<controller_IP_address>`

2. At the prompt, enter the 'admin' user password for confirmation.
⇒ You're ready to issue Linux commands on the controller via the console.

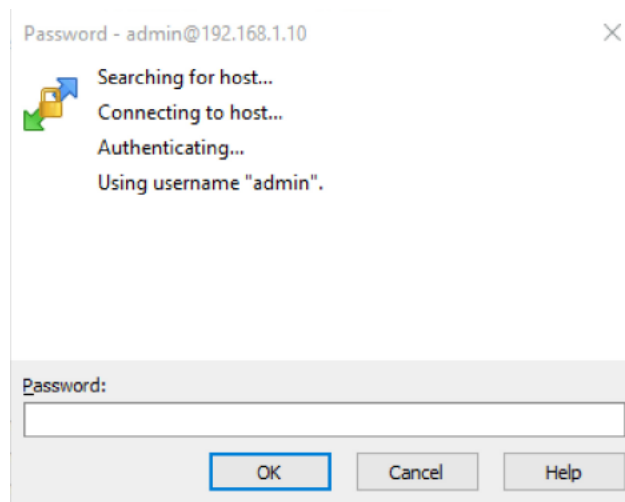
6.6.4 For copying or editing files

Using a Windows computer

1. To configure a new connection setting in WinSCP, click on 'New Site' in the upper right section:



2. Enter the IP address of the controller and 'admin' as the user name.
3. Click 'Login'.
4. In the dialog box that opens, enter the password for the 'admin' user and confirm with 'OK'.
⇒ WinSCP shows the file system on the controller and on your computer in a split view.



5. Navigate through the host computer directories and firmware directories and perform your task.

Using a Linux computer

Under Linux, SCP is available via console, e.g. for copying files:

1. To copy a file from the host computer to a directory on the controller; e.g. copying to /opt/plcnnext/:

```
scp <file> admin@<controller_IP_address>:/opt/plcnnext/
```

2. At the prompt, enter the password for the 'admin' user for confirmation.
⇒ The file is copied from the host computer to the controller.
3. To copy a file from a directory on the controller (e.g. /opt/plcnext/) to the current host computer directory:
`scp admin@<controller_IP_address>:/opt/plcnext/<file>`
4. At the prompt, enter the password for the 'admin' user for confirmation.
⇒ The file is copied from the controller to the host computer.

6.6.5 Default System Use Notification

If you connect to the controller via SSH or SFTP (e.g. using WinSCP), you will receive the following system use notification for your attention:

System use notification

Hinweis:

Dieses Geraet darf nur von autorisierten Benutzern fuer autorisierte Zwecke verwendet werden. Ihre Anmeldeinformationen und alle Benutzeraktionen auf diesem Geraet koennen ueberwacht, aufgezeichnet, kopiert und auditiert werden. Durch die weitere Verwendung dieses Geraets erklaeren Sie sich mit diesen Bedingungen einverstanden.

Notice:

This device may only be used by authorized users for authorized purposes. Your credentials and all user actions on this device can be monitored, recorded, copied and audited. By continuing to use this device, you agree to these terms.

The displayed text is stored in a txt file on the controller by default and can be changed or replaced if necessary. The file can be found in the file system on the controller under /opt/plcnext/config/System/Um/UmSystemUseNotification.txt. To change the file, you must be logged in as the Linux 'admin' user. You can edit the System Use Notification → 8.8.5 System Use Notification via the WBM of the controller.

See also

- Operating system → 6 Operating System
- System time → 6.5.1 System time
- Authentication failure handling → 7.6 Authentication failure handling
- User rights → 6.7 User rights

6.7 User rights

Festo AX Controls devices are supplied with a preset 'admin' user and a default password that is printed on the controller's housing.



Security note: Use the default 'admin' password only for initial access and change it as soon as possible!
See → 8.8.4 User management.

‘admin’ user

When a user logs onto a controller with the ‘admin’ user, the user is also recognized with the same name and password by the Linux system. The user is therefore assigned to the `plcnnext` group of the Linux system. Files that this user may read, write to and/or execute are assigned to the `plcnnext` group file system.

Override with sudo

Executing Linux commands that require higher rights is made possible for the users via `sudo`. Which Linux commands the users are allowed to execute via `sudo` is being configured in the Linux system.

7 Security

7.1 Overview Industrial Cyber Security

Cyber security in the industrial automation gains more attention in the upcoming years, so Festo AX OS is going to develop faster in this regard. Come back to this section for more features and basic information.



Security Note: For security issues and possible vulnerabilities, please contact the Product Security Incident Response Team (PSIRT) of Festo via its website → www.festo.com/psirt.

7.2 Unused interfaces

The following interfaces are not used:

Device	Firmware		
	25.0.1.46	25.9.2.4	26.3.1.4
CEPE-H8GB-128GB-C1	AP, XF20, XF10, XF1, XF2 and CARD		
CEPE-H8GB-128GB-M1			

Tab. 14

7.3 Built-in features

The Festo AX OS platform is developed in compliance with the IEC 62443-4-1 process. The implemented cybersecurity functions are aligned to IEC 62443-4-2.

FR1 – Identification and authentication control (IAC)

No.	Description	SL	Fulfillment – AX OS	Reference
CR 1.1	Human user identification and authentication	SL1	Festo AX OS provides that each user can be identified and authenticated by the User Manager in the WBM.	→ 7.7.6.5 User Management
CR 1.1 RE1	Unique identification and authentication	SL2	Festo AX OS provides that each user can be uniquely identified and authenticated by the User Manager in the WBM.	→ 7.7.6.5 User Management
CR 1.2	Software process and device identification and authentication	SL2	Festo AX OS provides that each non-human user access can be identified and authenticated by the User Manager in the WBM.	→ 8.8.2 Certificate management
CR 1.2 RE1	Unique identification and authentication	SL3	Festo AX OS provides that each non-human user access can be uniquely identified and authenticated by the User Manager in the WBM. Via the Trust Store, unique identification and authentication can be configured.	→ 8.8.2 Certificate management
CR 1.3	Account management	SL1	Festo AX OS provides that users can be managed via the User Manager in the WBM or via LDAP.	→ 7.7.6.5 User Management → 8.8.6 LDAP configuration

No.	Description	SL	Fulfillment – AX OS	Reference
CR 1.4	Identifier management	SL1	Festo AX OS provides that users can be managed via the User Manager in the WBM, via LDAP, or via the Linux configuration files.	➔ 7.7.6.5 User Management ➔ 8.8.6 LDAP configuration
CR 1.5	Authenticator management	SL1	Festo AX OS provides that the initial authenticator content is defined by the User Manager in the WBM. Password complexity rulesets and session handling are configurable.	➔ 7.7.6.5 User Management ➔ 8.8.6 LDAP configuration ➔ 7.5 Password complexity rules order ➔ 7.7.6.11 Password Policies
CR 1.7	Strength of password-based authentication	SL1	Festo AX OS provides that each user is assigned to configurable password complexity rulesets. The rulesets can be configured according to password guidelines.	➔ 7.5 Password complexity rules order ➔ 7.7.6.11 Password Policies
CR 1.7 RE1	Password generation and lifetime restrictions for human users	SL3	Festo AX OS provides that each user is assigned to configurable password complexity rulesets. The rulesets can be configured according to password guidelines including expiration rules.	➔ 7.5 Password complexity rules order ➔ 7.7.6.11 Password Policies
CR 1.8	Public key infrastructure certificates	SL2	Festo AX OS provides an Identity Store and a Trust Store in the WBM.	➔ 8.8.2 Certificate management
CR 1.9	Strength of public key authentication	SL2	Festo AX OS provides an Identity Store and a Trust Store in the WBM for managing certificate-based authentication.	➔ 8.8.2 Certificate management
CR 1.10	Authenticator feedback	SL1	Each component of the Festo AX OS with authentication function provides the possibility to hide the feedback of authenticator information during the authentication process.	➔ 7.7.6.5 User Management
CR 1.11	Unsuccessful login attempts	SL1	Festo AX OS defines rules how to handle authentication errors including unsuccessful login attempts.	➔ 7.7.6.5 User Management
CR 1.12	System use notification	SL1	Festo AX OS provides that a system usage message is displayed before authentication. The message is configurable by authorized personnel in the user authentication settings.	➔ 7.7.6.5 User Management
CR 1.14	Strength of symmetric key authentication	SL2	Symmetric keys are used only internally for TLS and OPC UAsecure communication.	➔ 8.8.2 Certificate management

Tab. 15

FR2 – Use control (UC)

No.	Description	SL	Fulfillment – AX OS	Manual Reference
CR 2.1	Authorization enforcement	SL1	Festo AX OS provides that users can be managed via the User Manager in the WBM, via LDAP, or via the Linux configuration files.	➔ 8.8.4 User management ➔ 7.7.6.5 User Management ➔ 8.8.6 LDAP configuration
CR 2.1 RE1	Authorization enforcement for all users (humans, software processes and devices)	SL2	Festo AX OS provides that users can be managed via the User Manager in the WBM, via LDAP, or via the Linux configuration files. Users are assigned to roles which have a predefined set of permissions.	➔ 8.8.4 User management ➔ 7.7.6.5 User Management ➔ 8.8.6 LDAP configuration
CR 2.1 RE2	Permission mapping to roles	SL2	Festo AX OS provides that users are assigned to roles which have a predefined set of permissions. The User Manager assigns roles and permissions to the session representing the user.	➔ 8.8.4 User management ➔ 7.7.6.5 User Management
CR 2.5	Session lock	SL1	Festo AX OS provides that there is an implemented time limit of 20 minutes for inactive sessions.	➔ 7.7.6.5 User Management

No.	Description	SL	Fulfillment – AX OS	Manual Reference
CR 2.6	Remote session termination	SL2	Festo AX OS provides that there is an implemented default timeout of 20 minutes. The duration can be set in the WBM.	➔ 7.7.6.5 User Management
CR 2.8	Auditable events	SL1	Festo AX OS provides a security logging to log all auditable events.	➔ 7.11 Configuring Central logging
CR 2.9	Audit storage capacity	SL1	Festo AX OS provides a security logging ensuring the audit storage capacity.	➔ 7.11 Configuring Central logging
CR 2.10	Response to audit processing failures	SL1	Festo AX OS provides that there is an external logging system for checking and reporting local errors.	➔ 7.11 Configuring Central logging
CR 2.11	Timestamps	SL1	Festo AX OS provides that timestamps are available and can be set via the WBM.	➔ 7.11 Configuring Central logging ➔ 8.7.1 Date & Time
CR 2.11 RE1	Time synchronization	SL2	Festo AX OS provides that the system time can be synchronized using NTP.	➔ 8.7.1 Date & Time
CR 2.12	Non-repudiation	SL1	Festo AX OS provides a security logging to log all auditable actions and events. Central logging via syslog-ng ensures non-repudiation.	➔ 7.11 Configuring Central logging

Tab. 16

FR3 – System integrity (SI)

No.	Description	SL	Fulfillment – AX OS	Manual Reference
CR 3.1	Communication integrity	SL1	Festo AX OS uses TLS for the communication channels (HTTPS, OPC UA). TLS ensures the integrity and authenticity of the communication.	➔ 8.8.2 Certificate management
CR 3.1 RE1	Communication authentication	SL2	Festo AX OS uses TLS for the communication channels (HTTPS, OPC UA). TLS ensures the integrity and authenticity of the communication.	➔ 8.8.2 Certificate management
CR 3.3	Security functionality verification	SL1	Festo AX OS provides various security measures and different verification interfaces that can be used to check the security settings by the system integrator or asset owner during production.	➔ 7.9 Security context
CR 3.4	Software and information integrity	SL1	Festo AX OS provides integrity of data in transition by using TLS. The User Management controls the access permission to data at rest. Physical access to the controller must be protected by a lockable cabinet.	➔ 7.7.6.5 User Management ➔ 7.9 Security context
CR 3.4 RE1	Authenticity of software and information	SL2	Festo AX OS provides a User Management which grants authenticity for data access. Only users with valid credentials and permissions can access the device and change data. User actions are logged.	➔ 7.7.6.5 User Management ➔ 7.11 Configuring Central logging
CR 3.5	Input validation	SL1	Festo AX OS provides input validation on all interfaces.	➔ 7.9 Security context
CR 3.6	Deterministic output	SL1	Deterministic outputs are configured via the application runtime, which defines the default value for each output in case of failure.	➔ 7.9 Security context
CR 3.7	Error handling	SL1	Festo AX OS does not provide any information that could be exploited by adversaries to attack the device. Special permissions are required to read error messages. Unauthenticated users do not receive critical information.	➔ 7.7.6.5 User Management ➔ 7.11 Configuring Central logging
CR 3.8	Session integrity	SL2	Festo AX OS authorization is performed by the User Manager, which creates secure sessions protected by TLS.	➔ 7.7.6.5 User Management
CR 3.9	Protection of audit information	SL2	Only the Festo AX OS roles 'SecurityAdmin' and 'SecurityAuditor' have the permission to read security loggings.	➔ 7.11 Configuring Central logging

Tab. 17

FR4 – Data confidentiality (DC)

No.	Description	SL	Fulfillment – AX OS	Manual Reference
CR 4.1	Information confidentiality	SL1	Festo AX OS provides confidentiality of data in transition by using TLS. The User Management controls the access permission to data at rest. Physical access to the controller must be protected by a lockable cabinet.	➔ 8.8.2 Certificate management ➔ 7.7.6.5 User Management
CR 4.2	Information persistence	SL2	Reset procedures set back the device to factory defaults securely, ensuring no residual sensitive data remains.	➔ 7.13 Reset Procedures
CR 4.3	Use of cryptography	SL1	Festo AX OS provides TLS for the communication channels (HTTPS, OPC UA). The cryptography is based on OpenSSL and offers state-of-the-art security mechanisms.	➔ 8.8.2 Certificate management

Tab. 18

FR5 – Restricted data flow (RDF)

No.	Description	SL	Fulfillment – AX OS	Manual Reference
CR 5.1	Network segmentation	SL1	Festo AX OS provides separate Ethernet interfaces. The controller supports network segmentation configuration via the WBM firewall.	➔ 8.8.3.1 Example Extended Firewall settings

Tab. 19

FR6 – Timely response to events (TRE)

No.	Description	SL	Fulfillment – AX OS	Manual Reference
CR 6.1	Audit log accessibility	SL1	Festo AX OS provides a security logging to log all auditable actions and events.	➔ 7.11 Configuring Central logging
CR 6.1 RE1	Programmatic access to audit logs	SL3	Festo AX OS provides a security logging to log all auditable actions and events and provides them to a central logging server via syslog-ng.	➔ 7.11 Configuring Central logging
CR 6.2	Continuous monitoring	SL2	Festo AX OS provides a security logging to log all auditable actions and events and provides them to a central logging server via syslog-ng for continuous monitoring.	➔ 7.11 Configuring Central logging

Tab. 20

FR7 – Resource availability (RA)

No.	Description	SL	Fulfillment – AX OS	Manual Reference
CR 7.1	Denial of service protection	SL1	Festo AX OS provides netload limiter and firewall (nftables) to control the communication load.	➔ 8.8.3.1 Example Extended Firewall settings
CR 7.1 RE1	Manage communication load from component	SL2	Festo AX OS provides netload limiter and firewall (nftables) to control the communication load. The task management is designed to manage and recover from high communication load.	➔ 8.8.3.1 Example Extended Firewall settings
CR 7.2	Resource management	SL1	Festo AX OS provides netload limiter and firewall (nftables) to control the communication load and resource management. In addition, the task management controls execution and resource load.	➔ 8.8.3.1 Example Extended Firewall settings
CR 7.3	Control system backup	SL1	Festo AX OS provides an app to start a backup during normal operations. It generates a backup file which is managed by the Device and Update Management.	➔ 8.9.6 Backup and Restore
CR 7.3 RE1	Backup integrity verification	SL2	Festo AX OS backup data is integrity protected. Before starting a restore, the data integrity is validated.	➔ 8.9.6 Backup and Restore
CR 7.4	Control system recovery and reconstitution	SL1	Festo AX OS provides recovery after a disruption or failure. To recover a device based on the backup data, it must be set to delivery status by reset, configured according to the system configuration, and the restore data is managed by the Device and Update Management.	➔ 8.9.6 Backup and Restore ➔ 7.13 Reset Procedures

No.	Description	SL	Fulfillment – AX OS	Manual Reference
CR 7.6	Network and security configuration settings	SL1	Festo AX OS provides that the network and security configuration can be set via the WBM.	➔ 7.7.6.3 Network settings ➔ 7.9 Security context
CR 7.7	Least functionality	SL1	Festo AX OS provides that the secure-by-default configuration follows the principle of least functionality: only components that have been considered in the threat analysis are active. The firewall is enabled by default with minimal open ports.	➔ 7.9 Security context ➔ 8.8.3.1 Example Extended Firewall settings

Tab. 21

Embedded device requirements (EDR)

No.	Description	SL	Fulfillment – AX OS	Manual Reference
EDR 2.13	Use of physical diagnostic and test interfaces	SL2	Festo AX OS protects access to physical test and diagnostic interfaces through the housing. Interfaces cannot be accessed through the housing with testbed adapters. The device must be protected in a lockable cabinet. The device must be shipped in a secure manner.	➔ 7.9 Security context
EDR 3.2	Protection from malicious code	SL1	Festo AX OS provides protection from malicious code by using TLS for data in transition. The User Management controls the access permission to the data at rest.	➔ 8.8.2 Certificate management ➔ 7.7.6.5 User Management
EDR 3.10	Support for updates	SL1	Festo AX OS provides a WBM page to install updates. OPC UA Software Update is supported to integrate Festo AX OS into the Device and Update Management Service.	➔ 7.12 Configuring Software Updates
EDR 3.10 RE1	Update authenticity and integrity	SL2	Festo AX OS provides RAUC update containers signed with an X509.3 certificate from a product vendor. Before installation, the authenticity and integrity of the update is verified. All update files provided via the download center are verifiable with a SHA 512.	➔ 7.12 Configuring Software Updates
EDR 3.11	Physical tamper resistance and detection	SL2	Festo AX OS provides that the cabinet must be locked; the application must supervise cabinet accesses.	➔ 7.9 Security context
EDR 3.13	Provisioning asset owner roots of trust	SL2	Festo AX OS provides the Certificate Authentication web page to install Asset Owner Roots of Trust via the Trust Store mechanism. Devices containing installed Asset Owner Roots of Trust must be specially protected in the field by locked cabinets.	➔ 8.8.2 Certificate management
EDR 3.14	Integrity of the boot process	SL1	Festo AX OS provides a partial boot integrity check for the OS and FW prior to starting the PLC function. The result is shown in the WBM and a notification in the security logging is generated.	➔ 7.7.6.4 Check the integrity state
EDR 3.14 RE1	Authenticity of the boot process	SL2	Festo AX OS provides a partial boot integrity check for the OS and FW based on the root of trust of the device.	➔ 7.7.6.4 Check the integrity state

Tab. 22



For developing secure-by-design, IEC 62443-2 compliant applications with PLCnext Technology, get a good grasp of the concepts used in the Security context.

7.4 Security settings via WBM

For the time being, most of the security-related settings in PLCnext Technology are configured in the ‘Security’ area of the Web-based Management (WBM) that resides on every Festo AX Controls . For basic handling of the WBM, see ➔ 8 Web-based Management.

To help you find your way through the many settings and parameters for each security feature, the information to the security-related topics in this section are sorted according to the pages in the ‘Security’ area of the WBM:

- Firewall , see → 8.8.3 Firewall
- User management , see → 8.8.4 User management
- User policies , see → 8.8.5 User policies
- LDAP configuration, see → 7.8.1 LDAP file-based configuration
- Syslog , see → 8.8.7 Syslog
- Certificate management , see → 8.8.2 Certificate management

In addition, you might be interested in these security-related topics:

- LDAPS connection → 7.8.1 LDAP file-based configuration
- Additional filters via nftables

7.5 Password complexity rules

User authentication usually requires a set of restrictions as to how long and complex a password needs to be and which characters a user can choose. With the security demand of periodical changes, the expiration of passwords need to be defined.

- See the User Authentication → 8.8.4 User management WBM topic for the general handling of users rights and roles.
- See the Authentication failure handling → 7.6 Authentication failure handling topic for more background on general restrictions that can cause problems.

Two sets of password complexity rules are predefined and depend on the user roles. You may need to adjust the rulesets to meet the needs of your application. We advise that the user roles ‘Admin’, ‘SecurityEngineer’, ‘SecurityAuditor’, ‘CertificateManager’, ‘UserManager’, and ‘Engineer’ have the ‘Admin ruleset’ by default. All other user roles may have the ‘Default ruleset’ by default.

- Adapt the ruleset to the conditions of your application.
- Apply a ruleset to each user role.

Password complexity rules

Setting	Explanation	Admin ruleset	Default ruleset
Minimum characters count	Number of characters a new password must at least contain in general.	10	8
Minimum ASCII characters count	Number of ASCII letters a new password must at least contain.	2	2
Minimum mixed letters count	Number of letters that must be specified as lowercase letters and as uppercase letters respectively (concerns a-z respectively A-Z of the basic ASCII table).	1	1
Minimum numbers count	Number count a new password must at least contain.	1	1
Minimum special characters count	Number of special characters a new password must at least contain.	1	0
Allowed special characters	ASCII special characters that are allowed for the special character count rule.	{ } [] # , ; : . ^ ? ! _ ' ~ @ \$ % / \ = + - * &	{ } [] # , ; : . ^ ? ! _ ' ~ @ \$ % / \ = + - * &
Block username	A new password must not contain the username.	enabled	enabled
Block reused passwords	A repeated password will be blocked on next set attempt.	enabled	enabled

Setting	Explanation	Admin ruleset	Default ruleset
Password reuse	Defines how many previously used passwords are checked, in order to prevent their reuse.	5	5
Check block list	A new password must not contain a phrase from the blocklist.	disabled	disabled

Tab. 23

Password interval rules

Setting	Explanation	Admin ruleset	Default ruleset
Password interval rules	Number of allowed password changes per interval.	disabled	disabled
Password changes per interval	Number of allowed password changes per interval.	0	3
Password change interval	Limitation of password changes within this time interval.	0 Days	1 Day(s)

Tab. 24

Password expiration rules

Setting	Explanation	Admin ruleset	Default ruleset
Password expiration rules	The password expiration rules are applied in the system.	disabled	disabled
User lock is active	The password expiration rules are applied in the system.	disabled	disabled
Days until expiration	Number of days that may pass before the current password expires.	120	240
Days until warning	Number of days before the password expires on which a warning is displayed to the user to change the current password.	30	30

Tab. 25

7.6 Authentication failure handling

If a Festo AX Controls device denies access because of invalid credentials for a specific user name, it usually is no big deal - just try again with the valid credentials. But a failing user authentication (➔ 8.8.4 User management) always starts a cascade of events.

Access to a Festo AX Controls device is handled by the User Manager for all types of connections. When the user authentication fails, the username is entered into a penalty list which keeps also track of the current number of failed login attempts. Retrying with invalid credentials will cause that this user is blocked for a specific penalty delay (for security reasons, we do not publish any details on the specifics here). Every unsuccessful retry will extend that delay so brute-force attacks cannot cause a security issue.

Of course, that's what is expected from a secure system. With extensive use of interfaces and services logging in to the Festo AX Controls device, this authentication failure handling can cause unexpected side effects:

- Even valid credentials do not grant access:
During the penalty delay, the affected user is not allowed to log in again even with the valid credentials until the delay has expired. In this case, logging in via WBM or any other service or interface is denied, too, even if valid credentials are presented.
- Not all types of connections seem to be affected:
The blocking concerns only another login attempt, so if e.g. the OPC UA client has already logged in successfully before a WBM login fails, the running OPC UA session remains unaffected.
- Service clients in auto-retry mode are increasing the delay:
If invalid credentials are set in the login routine of e.g. a OPC UA client that is set to retry the login frequently until succeeding, it can deadlock that user in a never-ending penalty delay.
- Maximum Festo AX Controls session count:
Activation is rejected in case the maximum Festo AX Controls session count is reached.
The maximum count can be set by ‘admin’ user so it might be exceeded earlier or later.

Remedy

The service logs are reporting why the access is denied and are showing the penalty delay in milliseconds. The ‘admin’ user could access the PLC and search the diagnostic log files for the cause and the duration of the delay.

- If the penalty delay is still reasonable (e.g. 5 min) then just wait until it expires and try again with valid credentials.
- If the penalty delay is far beyond reasonable then restart the PLC. The penalty list is erased and the user is back in good standing.

Preventive measures

- It is highly recommended to make sophisticated use of the different user roles for access in different use cases, such as accessing the Festo AX Controls device for programming, OPC UA access, ... That's what the fine-tuned user roles → 8.8.4 User management are for.
- In general, avoid accessing devices with the ‘admin’ user as much as possible. Having the above described cascade in mind, it's an especially bad idea to access a device as the ‘admin’ user via a client or interface in auto-retry mode: You're prone to locking yourself out of the device for good by making a simple typo in the credentials.

See also

- Industrial Cyber Security → 7 Security
- Security - User management → 8.8.4 User management
- LDAP connection configuration → 7.8.1 LDAP file-based configuration

7.7 Initial secure setup

7.7.1 Checking the CEPE

Shipping packaging

Stickers are attached to the packaging to prevent tampering with the device during shipping (e.g. by installing a different firmware) and to detect unauthorized opening of the packaging.

- Make sure that the packaging has not yet been opened. To do this, check that the sticker on the box of the CEPE Controller is intact.
- If the sticker on the box is damaged, you must not use the device!
- If you notice any damage to the packaging, contact Festo immediately.

Measures for shipment

- If a CEPE is delivered from the system integrator to the asset owner, the following measures must be taken into account:
- There must be no customer-specific data on the CEPE.
 - Send the initial/ recovery password separately from the CEPE Controller.
 - Preferably, CEPE Controller and password should be shipped individually in sealed packaging with security seals.

7.7.2 Get Familiar with the CEPE

Connecting elements

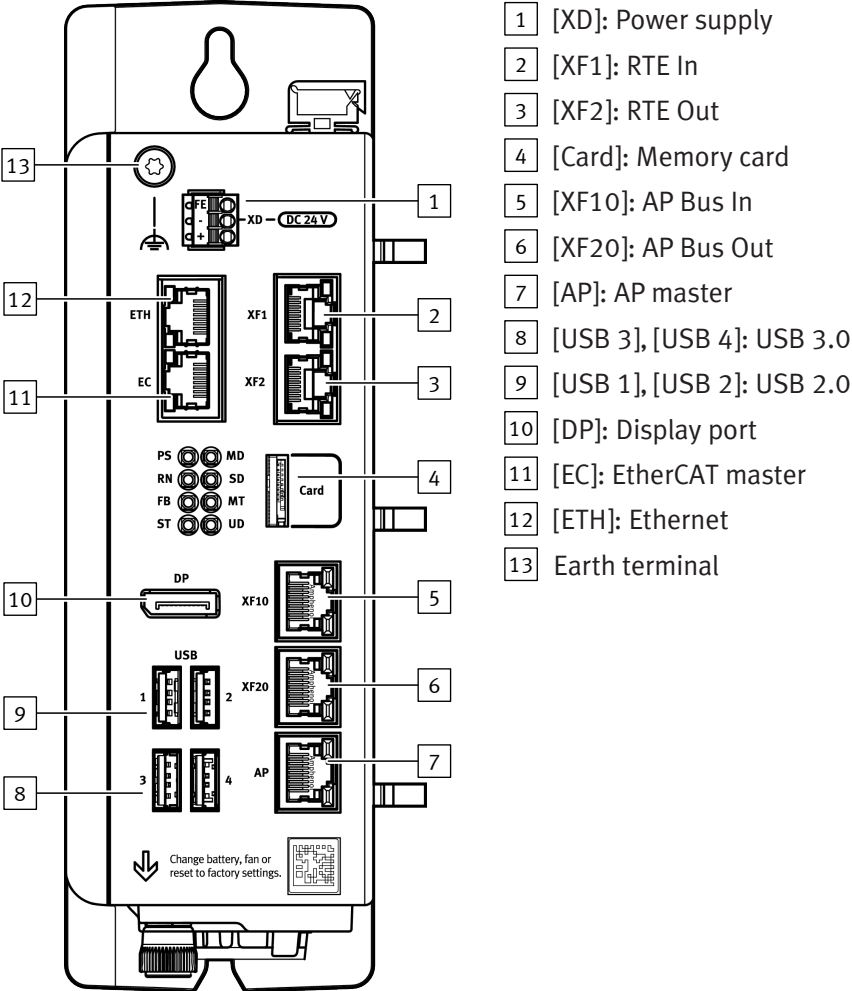


Fig. 1: CEPE front view

Fan module with battery

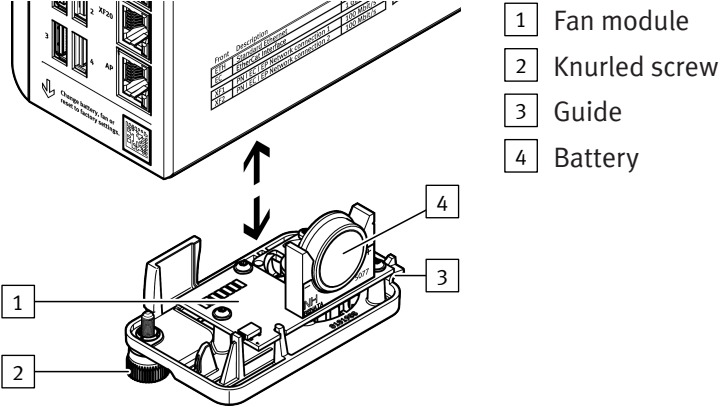


Fig. 2: Fan module

Labels

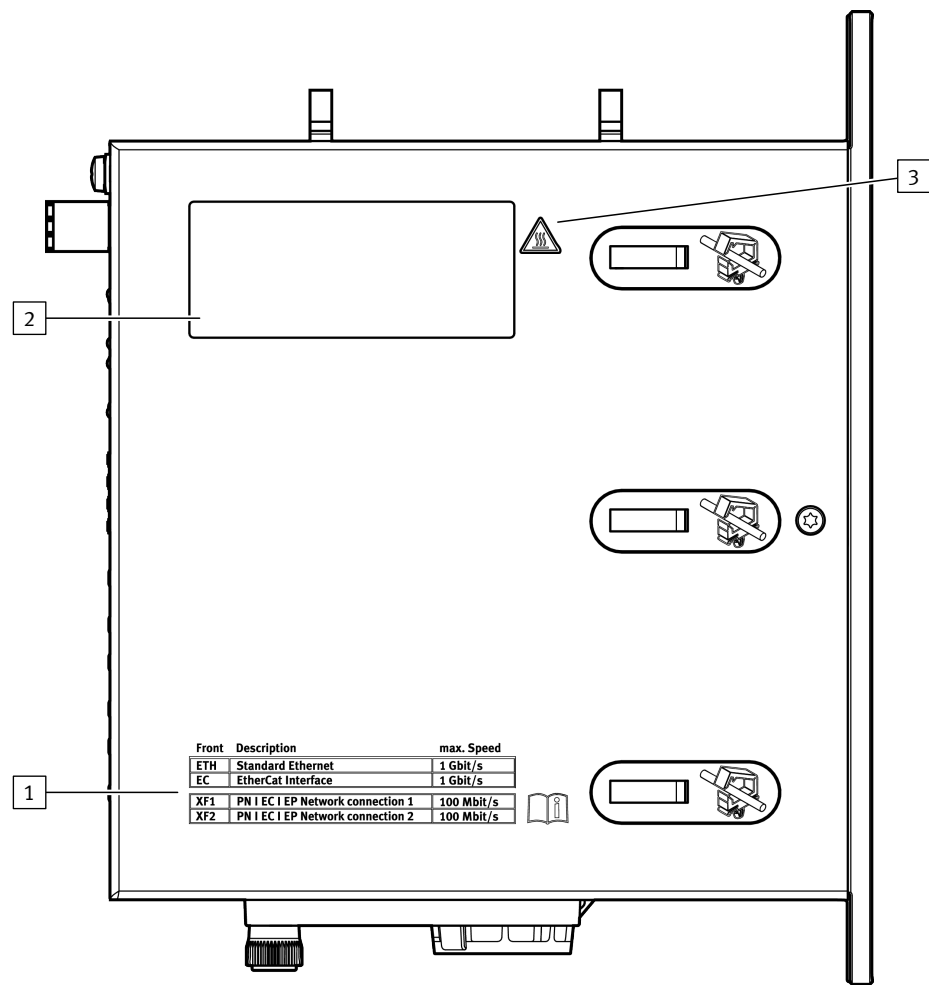


Fig. 3: Labels on the right side of the housing

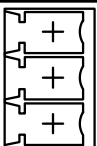
1 Information on the EtherNet inter-
faces

2 Product labelling (type plate)

3 "Hot surface" warning symbol

7.7.3 Power supply

Connect the power supply according to the following pin allocation. Use an external fuse with a maximum rating of 4 A for line protection.

Power supply [XD]			
Port	Pin		Function
	3	FE	Functional earth
	2	–	0 V
	1	+	24 V DC power supply

Tab. 26: Pin allocation

Now the CEPE will start up, which can be physically observed via LEDs lighting up (see operating Instructions) and the Fan spinning.

7.7.4 Software

Each Festo-related software provided for download from the Festo website provides an SHA512 value. It can be used to check the integrity of the software after download before installation on the PC or on the CEPE.

Inbetriebnahme Festo Automation Suite Parametrierung, Programmierung und Wartung elektronischer Geräte von Festo Systemvoraussetzungen: - Windows 10 Version 1607 oder höher - Windows 11 32 oder 64 Bit Mehr						
	Version 2.11.0.657 Mehr	2.11.0.657	SHA-512	Deutsch [de] ▾	489 MB	↓
	Version 2.10.1.1 Mehr	2.10.1.1	04990fd085e623ee43da768d08d5c339ef3efbdd05f81b5929a6d1415ae774e821fabbcd0b4701bbe8a631544719d3406145826c403053fd1b7900776d9b4565	Deutsch [de] ▾	486 MB	↓
	Version 2.10.0.557 Mehr	2.10.0.557		Deutsch [de] ▾	486 MB	↓
	Version 2.9.1.1 Mehr	2.9.1.1		Deutsch [de] ▾	477 MB	↓

Verification tools:

- **Linux:** sha512sum <filename>
- **Windows (PowerShell):** Get-FileHash <filename> -Algorithm SHA512
- **Windows (7-Zip):** Right-click the file → CRC SHA → SHA-512

Festo Automation Suite

Parameterisation, programming and maintenance of electronic devices by Festo.
 Festo Automation Suite: → www.festo.com, search for 'Festo Automation Suite', tab 'Downloads', section 'Software'

CODESYS app

CODESYS PLC (x86): → www.festo.com, search for 'CODESYS PLC (x86)', tab 'Downloads', section 'Software'

Other apps

Other apps: → www.festo.com, search for 'CEPE', tab 'Downloads', section 'Software'

Preinstalled apps

Preinstalled Apps: → www.festo.com, search for 'CEPE', select type 'CEPE-H8GB-128GB-M1' or 'CEPE-H8GB-128GB-C1', tab 'Downloads', section 'Software'

Produktvergleich
☒ Unterschiedlich

☐ Identisch

[Download](#)
[Alles löschen und schließen](#)

 Steuereinheit CEPE-H8GB-128GB-M1 8165401	 Steuereinheit CEPE-H8GB-128GB-C1 8165400
---	---

Technische Daten

Zusätzliche Funktionen	IO-Link OPC-UA, MQTT WebIQ 1000 tags + 2500 alarms Enthaltene Lizenzen: Festo AX Controls CODESYS PLC Basic Festo AX Controls CODESYS PLC Standard Festo AX Controls CODESYS PLC Advanced Festo AX Controls CODESYS SoftMotion 4 Festo AX Controls CODESYS SoftMotion 8 Festo AX Controls WebIQ 1000 Festo AX Controls Motion Robotic	IO-Link OPC-UA, MQTT Enthaltene Lizenzen: Festo AX Controls CODESYS PLC Basic
-------------------------------	---	--

7.7.5 Set BIOS Administrator Password**7.7.5.1 Overview BIOS Administrator Password**

To configure the BIOS/UEFI Administrator Password on the CEPE (PLC) during initial setup, you need:

- The CEPE (PLC) powered off.
- A monitor with Display Port is available.
- A USB keyboard is available.
- Access to the current BIOS/UEFI Administrator Password (initially set to 'Festo').

7.7.5.2 Entering the UEFI Setup

1. Connect monitor and keyboard.
 - Connect the monitor to the CEPE.
 - Connect a USB keyboard directly to the CEPE.
2. Power on the CEPE.
3. Open the UEFI setup menu.

Immediately after powering on, repeatedly press the 'Esc' key.

Continue pressing the 'Esc' key until a password prompt appears.

If the operating system starts to boot instead of showing the password prompt, power off and retry, pressing 'Esc' earlier and more frequently.
4. At the password prompt, type: 'Festo'
5. Confirm with 'Enter'.
6. If the password is correct, the BIOS setup menu will open.

7.7.5.3 Changing the Administrator Password

1. Navigate to the 'Security' area.

Use the arrow keys to move through the UEFI menu.

Look for a tab or section named: 'Security'.

Press 'Enter' to open the relevant menu.
2. Select 'Administrator Password'.

In the 'Security' section, locate: 'Administrator Password'

Highlight this entry and press 'Enter'.



3. Enter the new password 2 times.



By default, the password requirements are set to a minimum of three characters, but passwords should follow this password policy:

- Minimum characters: 10
- Minimum ASCII letters: 2
- Minimum mixed letters (lower and upper case): 1
- Minimum numbers: 1
- Minimum special characters: 1
- Avoid simple or easily guessable passwords.

NOTICE

Document the new password only in approved secure credential storage according to your internal IT/security policies. Loss of the BIOS/UEFI password can block authorized service access.

7.7.5.4 Saving and Exiting

1. To save changes in the UEFI menu, navigate to the 'Exit' or 'Save & Exit' tab.
2. Select: 'Save Changes and Exit'.
⇒ The CEPE will reboot.

7.7.6 Connect

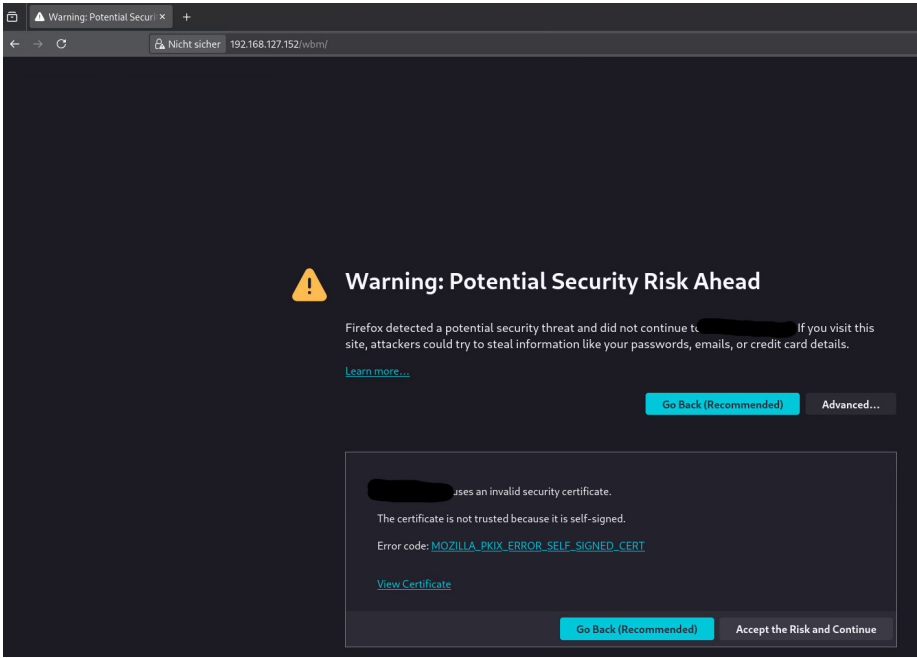
7.7.6.1 Connecting to Web-based Management

The CEPE has web-based management (WBM). WBM can be accessed via an Ethernet cable. For secure communication, the web server of the device uses a self-signed TLS certificate automatically generated by the device. When you first access the WBM, the TLS certificate is not known to your web browser. Therefore, a security warning opens in the web browser, even though it is a secure connection.

Establish the first connection as follows:

1. Ensure the PC can reach the subnet 192.168.1.x.
2. Open `https://192.168.1.10` in a browser.

3. Accept the initial browser warning for the self-signed certificate.



4. Log in with user name ‘admin’ and the default **admin password (Pwd)**.
The default ‘admin’ password (Pwd) is printed on the product labelling (rating plate) ➔ 7.7.2 Get Familiar with the CEPE.

NOTICE

Security note: Use the default ‘admin’ password only for initial access and change it as soon as possible!

5. To not receive a security warning (in the browser) when accessing the WBM in the future, you must download the certificate to your PC and add it as a trusted certificate to the web browser.
- After login:
- Open ‘Device’ ➔ ‘General Data’
 - Check whether you are working on the correct device:
 - Compare Product key as printed on product labelling, see ➔ 7.7.2 Get Familiar with the CEPE.
 - Compare device type as printed on product label, e.g. CEPE-H8GB-128GB-M1.
 - Firmware version: Always use the latest certified version. It is available here ➔ www.festo.com/sp, search for CEPE, tab ‘Downloads’ ➔ ‘Software’.

WBM Sections

Section	Functions
Overview	Status and diagnostic displays, general system information
Device	General device information
Diagnostics	Diagnostic information, messages
Configuration	Network status, apps
Security	User authentication, certificate authentication, and firewall
System	Firmware update, licence and app management
Help	Links to additional information

Tab. 27

7.7.6.2 Check the device

1. Open the ‘General Data’ page (‘Device’ - ‘General Data’).

2. Check whether you are working on the correct device:
Serial No. as printed on the device.
3. Check for the newest Firmware release: ➔ www.festo.com, search for 'CEPE', select type 'CEPE-H8GB-128GB-M1' or 'CEPE-H8GB-128GB-C1', tab 'Downloads', section 'Software'
4. Make sure the correct time is set. The time can be set either manually or via an NTP server ➔ 6.5 System time.
5. If a newer version is available, click on 'Download' and go to 'System' - 'Update in the WBM'.

PLCnext Control
CEPE-H8GB-128GB-M1
Firmware version: 25.1.0.7
Product key: [REDACTED]
● Connected

Part number: 8165401
Hardware version: 0

General data

Vendor	Festo SE & Co. KG
Address	Ruiter Str. 82, 73734 Esslingen, Germany
Internet	https://www.festo.com
Device type	CEPE-H8GB-128GB-M1
Part number	8165401
Product key	[REDACTED]
Firmware version	25.1.0.7
Hardware version	0
Mainboard serial	Default string
Aux HW ID	6CBE0D00061D003A00AED770DCC9
Aux HW version	0
Aux BL version	0.1.2
Aux FW version	0.1.6
Aux FPGA version	0xecb06f80b545
Aux FPGA revision	01
Aux FPGA API	00
Aux FPK	
BIOS version	CTL6R926
CPU Module version	1.0.0
CPU Module serial	LOD120057
TPM revision	7.63
SSD model	TS128GMTS952T-I
SSD serial	G653150103
SSD revision	02J0TBDA

6. Select firmware to be updated

Status

Device health Check function

Update list

Name	Version	
Firmware	0.0.31	Update
Project:		Update

7. Select File and start update.

Update Firmware

Information

Status

PreparedForUpdate

Hardware revision

02

Current version

0.0.31

Backup version

0.0.31

Pending version

N/A

Installation

Start and resume automatically after installation

☒

Select File

No file selected.

START AND RESUME

START UPDATE

7.7.6.3 Network settings

Your specific security context determines the network structure and also the IP addresses. To assign the IP addresses that are suitable for you, you must derive them from your security context.

i

If you already changed the default network settings of the CEPE via the Festo Automation Suite, you can skip this section.

You should change the default Network settings regardless of your setup, as you can not use multiple CEPE in default factory state within in the same network with the same IP.

1. Log in to the WBM.

2. Go to ‘Configuration’ - ‘Network’

3. In the ‘TCP/IP’ section, assign the IP address, subnet mask, and gateway for the [ETH] interface according to your security context.

LAN Interfaces

TCP/IP (LAN 1)

Status

IP address

192.168.127.152

Subnet mask

255.255.0.0

Default gateway

192.168.128.1

DNS server addresses

8.8.8.8

8.8.4.4

-

MAC address

00:E0:4B:7B:E6:19

Configuration

192.168.127.152

255.255.0.0

192.168.128.1

8.8.8.8

8.8.4.4

DNS server address

4. Click on ‘Save Page & Restart’. Now the CEPE will be **rebooted**.

If you can not connect to the CEPE WBM due to a Network misconfiguration, you are still able to change the network settings via the Festo Automation Suite as it is relying on the Festo Multicast Protocol.

Deriving IP Addresses from the Security Context

Your specific security context determines the network structure and IP addresses. Derive addresses from your zone segmentation plan:

46

Festo — CEPE — 2026-08a

- define a network prefix reflected in the first bits of the IP addresses (e.g. 172.16.xx.0)
- assign distinct address spaces per zone to support network segmentation
- ensure each controller interface connects to the appropriate zone

The information under different TCP/IP sections refers to the respective Ethernet interfaces of the controller. Assign addresses for each interface according to the zone it connects to.

7.7.6.4 Check the integrity state

After boot, the integrity check result is displayed as a notification in the WBM:

1. Log in to the WBM.
2. Open 'Diagnostics' → 'Notifications' page.
3. Check the notification area for the integrity check result.

Successful firmware integrity check:

Notifications					
Severity	Time	Sender	Name	Notification	
1	2025-11-26 12:39:59	PLC Manager	Arp.Plc.Domain.Plc.StateChanged	Plc state changed: None --> Ready	
1	2025-11-26 12:39:59	User Manager	Security.Arpl.System.Um.UserAuthenticationInitiallyEnabled	User authentication is initially enabled	
1	2025-11-26 12:39:59	System Manager	Arp.System.Acl.SystemManager.StateChanged	SystemManager state changed: Ready, error=false, warning=false	
1	2025-11-26 12:39:59	BuiltInDeviceSelfTest	External.BuiltInDeviceSelfTest.INFO	Starting SBIST (Startup Built-In Self Test)	
1	2025-11-26 12:39:59	report-integrity-status	External.report-integrity-status.INFO	Firmware integrity checks were successful.	
1	2025-11-26 12:39:58	Firewall Manager	Security.Arpl.Services.Firewall.Startup	Firewall run status is Started, activation status is Activated, active tables: name=plcnext_filter, family=ip@name=plcnext_ip6_filter, family=ip6	
1	2025-11-26 12:39:58	Device Interface	Security.Arpl.Device.Interface.NtpConfigStatus	NTP servers config. Servers Hostnames:	
1	2025-11-26 12:39:58	Device Interface	Security.Arpl.Device.Interface.EthernetInterfaces	Configured IP Addresses: Interface number 1 Ip Address 192.168.126.210	
1	2025-11-26 12:39:58	Device Interface	Security.Arpl.Device.Interface.DeviceInfo	Device Info: article name CEPE-H8GB-128GB-M1, article number 8165401, serial number NLQKL9MTBWL, firmware version 25.9.2.3 (25.9...	
Firmware integrity checks were successful.					
Export CSV File					

Failed firmware integrity check:

Notifications					
Severity	Time	Sender	Name	Notification	
1	2025-11-26 12:43:27	BuiltInDeviceSelfTest	External.BuiltInDeviceSelfTest.INFO	System time OK	
1	2025-11-26 12:43:27	BuiltInDeviceSelfTest	External.BuiltInDeviceSelfTest.INFO	PCIE configuration OK	
1	2025-11-26 12:43:27	BuiltInDeviceSelfTest	External.BuiltInDeviceSelfTest.INFO	SMARTCTL SSD test OK	
1	2025-11-26 12:43:24	User Manager	Security.Arpl.System.Um.SessionCreated	Session created. User: admin, User roles: Admin, Security Token: 022BD701, Object name: Wbm, currently opened Sessions 2	
1	2025-11-26 12:43:11	BuiltInDeviceSelfTest	External.BuiltInDeviceSelfTest.INFO	Starting SBIST (Startup Built-In Self Test)	
2	2025-11-26 12:43:10	report-integrity-status	External.report-integrity-status.WARNING	Actual hash of file /media/rfs/rw/upperdir/opt/plcnext/Security/integrity_check_lipsum_test.txt differs from estimated value b97c8c122...	
2	2025-11-26 12:43:10	report-integrity-status	External.report-integrity-status.WARNING	Firmware integrity checks have failed.	
1	2025-11-26 12:43:09	System Manager	Arp.System.Acl.SystemManager.StateChanged	SystemManager state changed: Running, error=false, warning=false	
1	2025-11-26 12:43:09	Notification Manager	Arp.System.Nm.SubscribeToNotRegisteredNotification	A subscriber subscribed to not registered notification name: App	
Firmware integrity checks have failed.					
Export CSV File					

7.7.6.5 User Management

The CEPE supports local user administration in the WBM, page 'Security' → 'User Management'.

See also → 7.7.6.5 User Management.

Delivery state

- User authentication is enabled and can not be disabled
- Only the 'admin' user exists initially
- The unique default 'admin' password is printed on the controller type plate, see → 3.3 Hardware documentation

NOTICE

Unauthenticated access

More accesses are possible via the ‘admin’. This can disrupt production and reduce security.

•

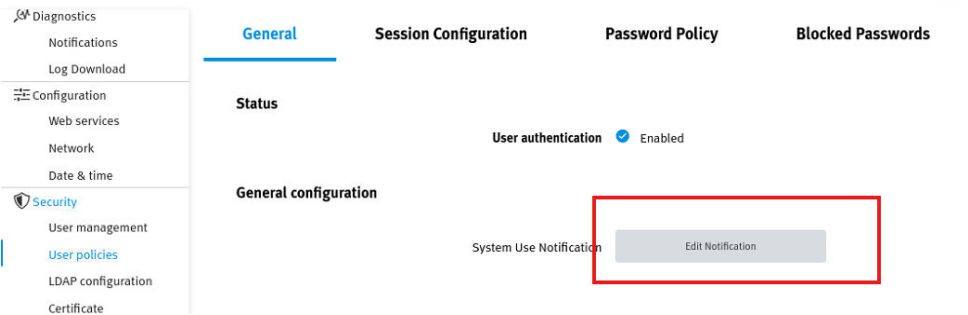
Do not start any plant with the ‘admin’ account active in production. The ‘admin’ account is for commissioning only.

User-Management Features

- Role assignment per user, see → 8.8.4 User management
- Password rulesets, see → 7.7.6.11 Password Policies
- Configurable session timeout and login penalties
- Configurable maximum concurrent sessions
- System use notification shown before login

Login Banner Configuration

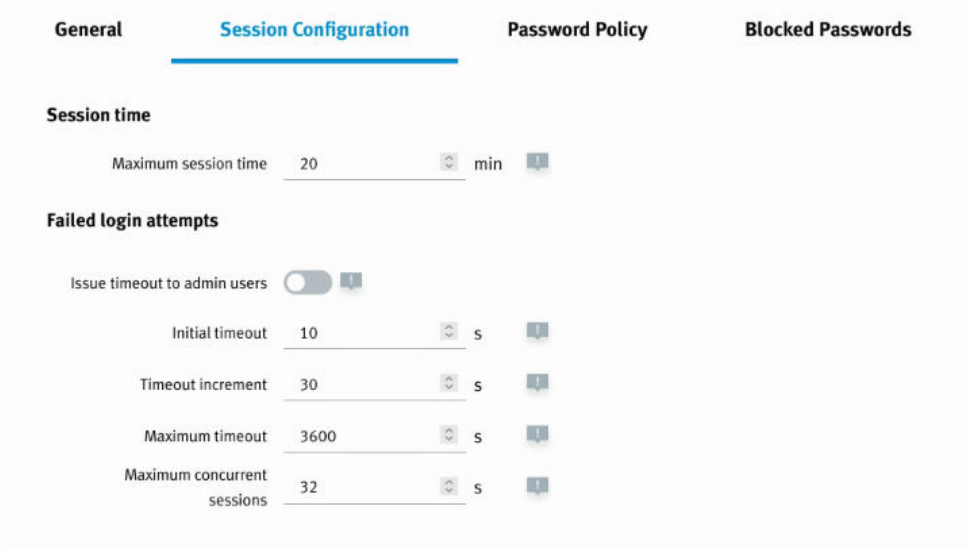
Configure the login banner (System Use Notification) in ‘Security’ → ‘User Policies’ on the ‘General’ tab, section ‘General configuration’, button ‘Edit Notification’:



This notification is displayed at every login attempt and must include all languages required by your organization.

Session Configuration

Configure session and logout parameters in ‘Security’ → ‘User Policies’ on the ‘Session Configuration’ tab:



Parameter	Default Value	Description
Maximum session time	20 min	After this period of inactivity the session is automatically closed. Do not set this to 0 – this locks out everyone from the WBM.
Exclude ‘Admin’ users from timeout	false	When set to true, excludes ‘Admin’ users from timeout penalties on repeated login failures.

Parameter	Default Value	Description
Initial timeout	10 s	Penalty time after three failed password attempts
Timeout increment	30 s	Additional penalty time after each further failed attempt
Maximum timeout	3600 s	Maximum penalty time between login attempts
Maximum concurrent sessions	32	Number of simultaneous communication channels permitted. Minimum value: 2.

Tab. 28



For security reasons, the 'Maximum concurrent sessions' value should be as low as possible. Each communication to the controller needs its own session, including WBM access. To determine the minimum viable value: count concurrent sessions required by your project (WBM, OPC UA, remoting, etc.) and add 2 to prevent locking yourself out. All changes made in the 'Session Configuration' tab are saved only by pressing the 'Apply and reboot' button. The controller only reboots if all settings can be applied error-free.

7.7.6.6 Managing Users via WBM

Navigate to 'Security' → 'User Management' to:

- view all local users and their assigned roles
- add, modify, or delete user accounts
- assign password rulesets
- assign or revoke roles

By default, on a PLCnext Control only a single user is configured and assigned to the 'Admin' user role. We recommend to assign other users and user roles, once the controller is put into production, which is done by means of the 'User management' WBM page, see → 8.8.4 User management.

NOTICE

Only Security responsables should have access to the 'Admin', 'Security Engineer' and 'CertificateManager' roles as these can modify the previously established security settings.

Users roles with access to 'System' → 'Device Maintenance' via WBM can:

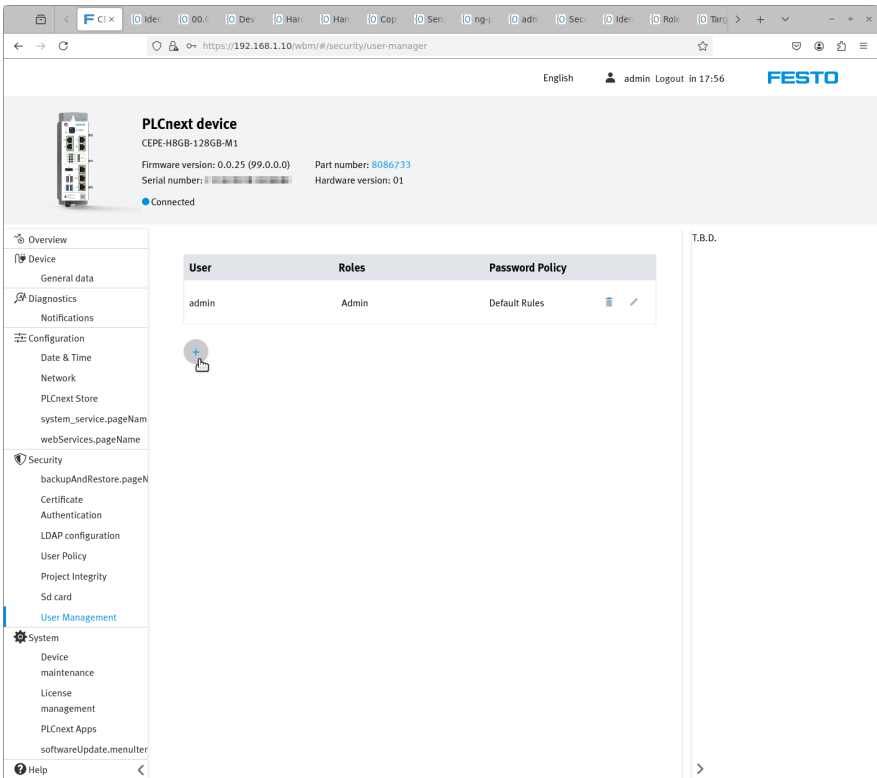
- Adding a user
- Editing existing user
- Deleting users



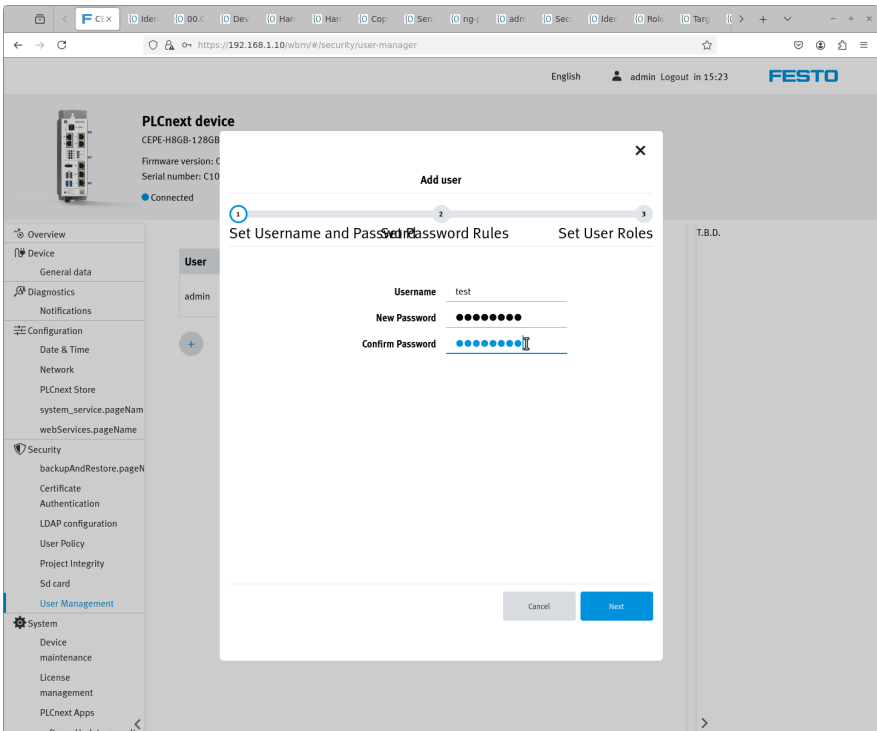
The 'User Management' page can only be used to set the default password of users. Each user can change their own password via 'System' → 'Device Maintenance', see → 7.7.6.11 Password Policies.

Adding a User

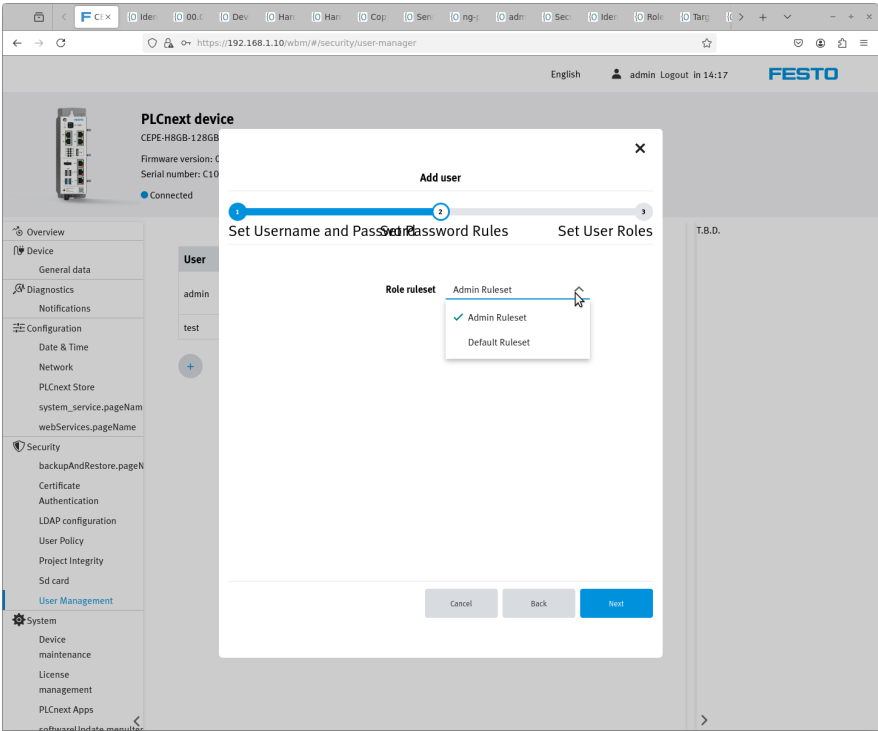
- 1. Click the +button to add a new user.



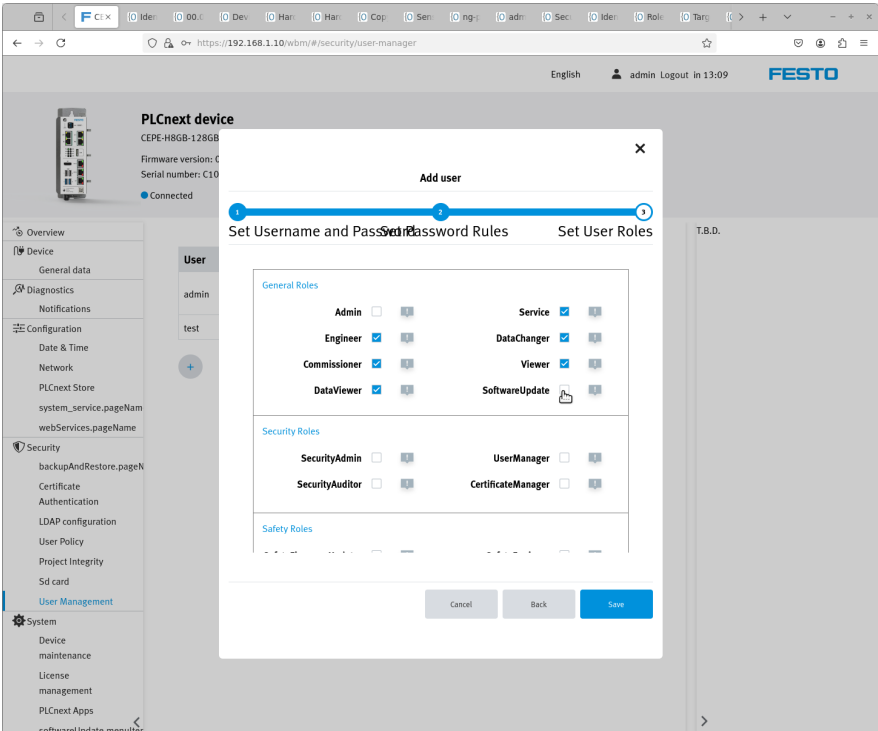
- 2. Enter the username, a default password, and the password confirmation.



3. Select the required password ruleset.

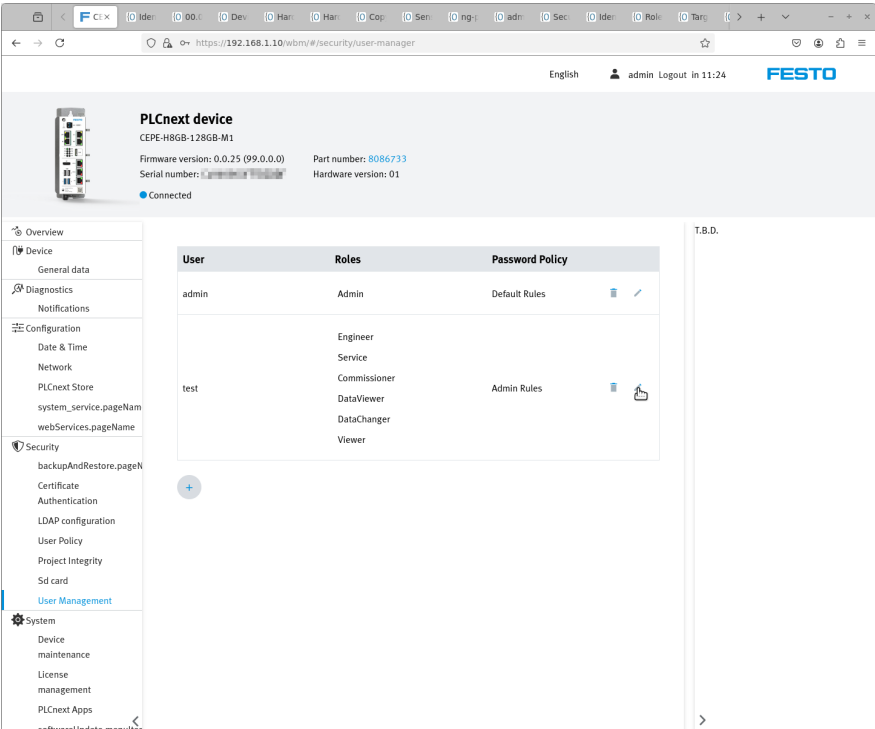


4. Select the roles for the new user and click 'Save'.

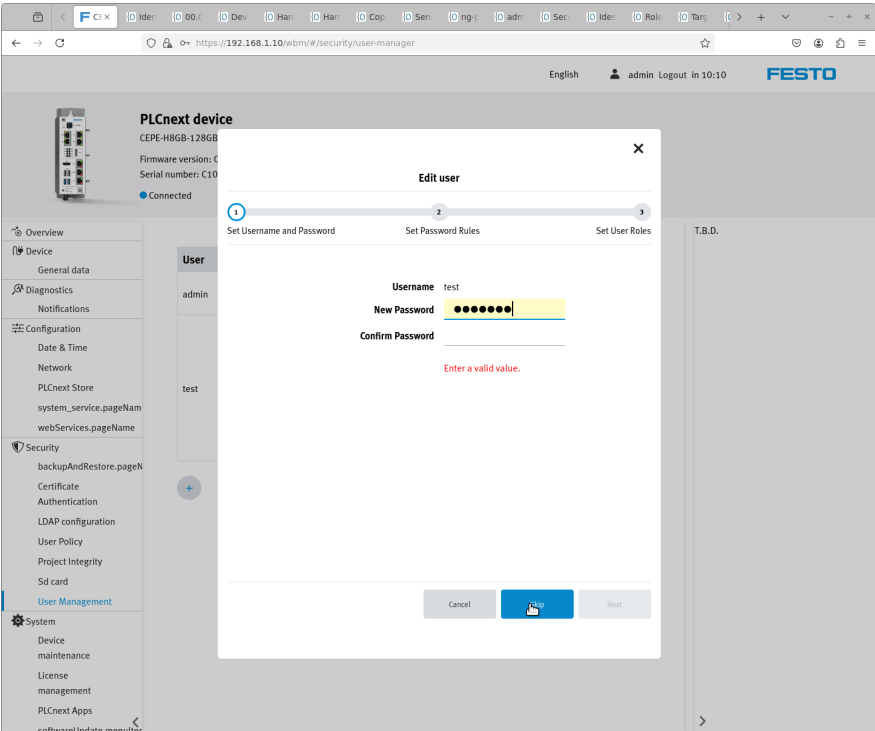


Edit existing User

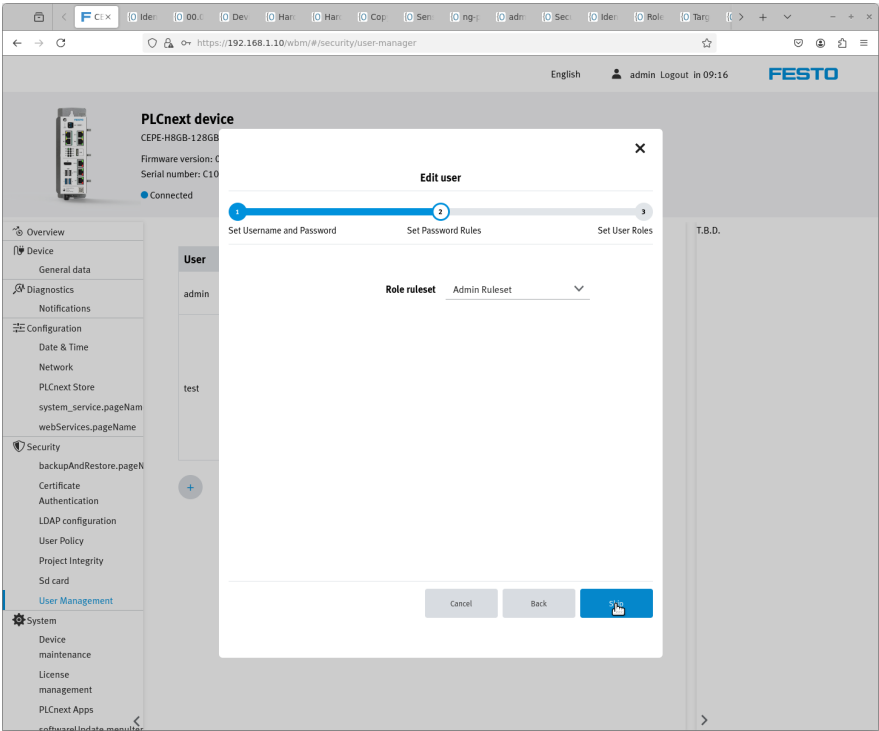
1. Click the edit icon next to the user entry.



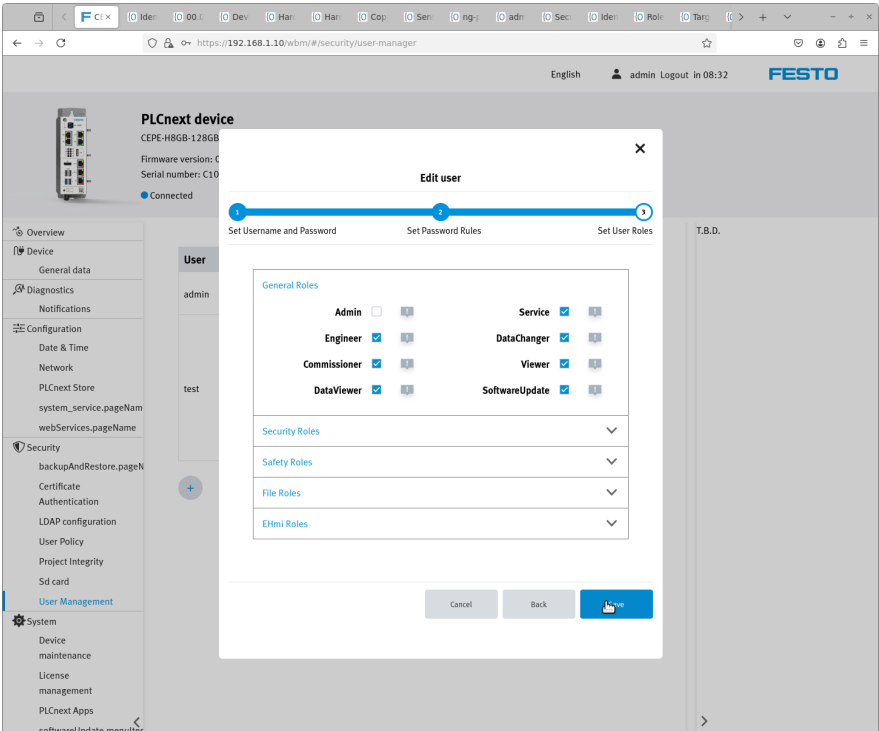
2. Change the user's default password or skip.



3. Change the password ruleset or skip.

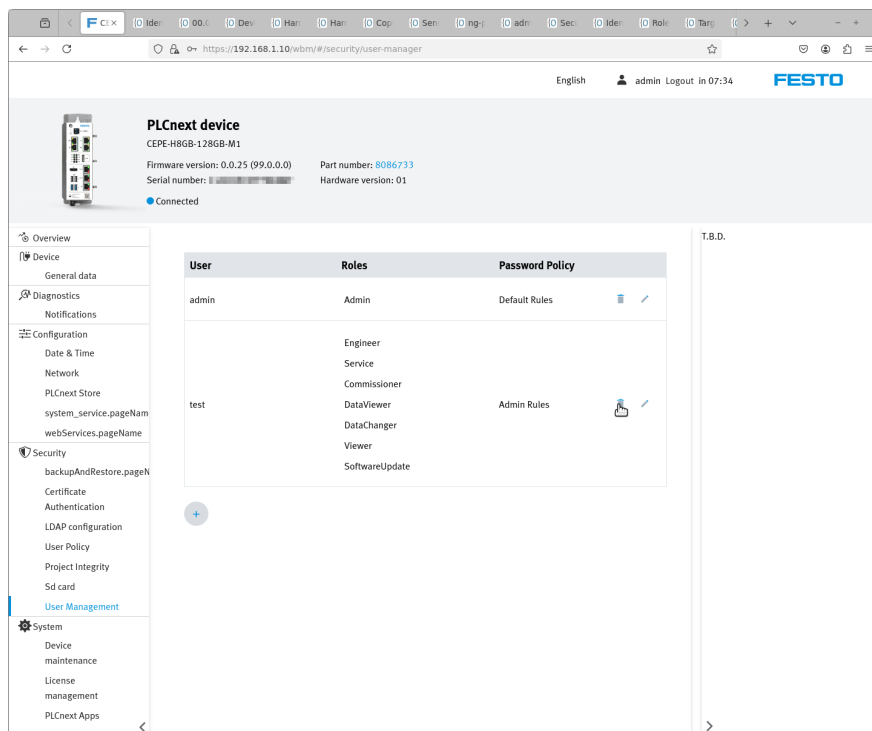


4. Change roles and click 'Save'.

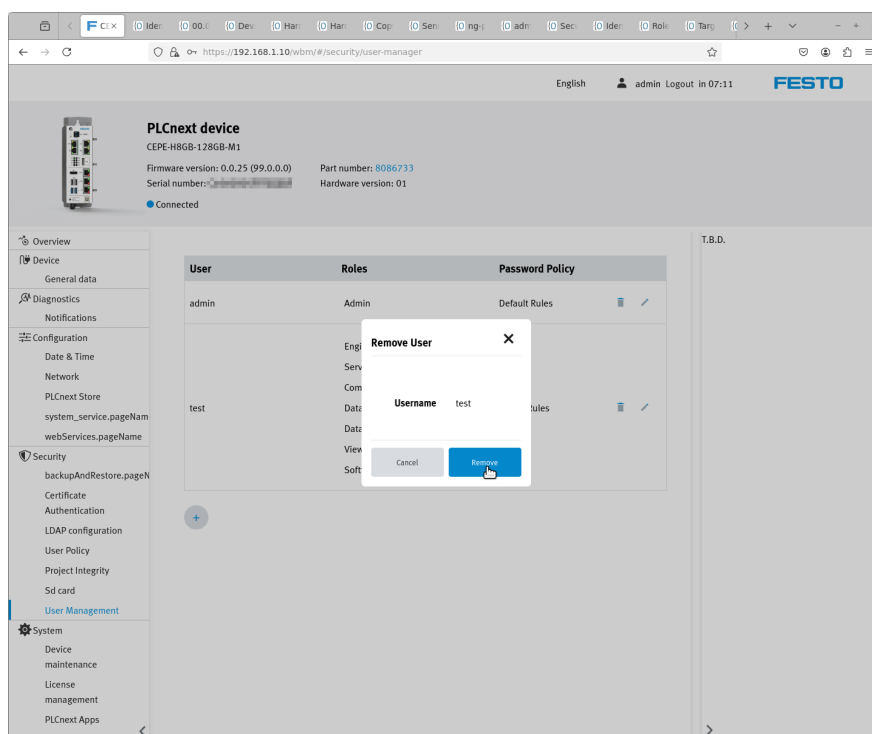


Deleting a User

1. Click the delete icon next to the user entry.



2. Confirm with 'Remove'.



Guidance

The 'User management' page can only be used to set the **default** password of Users. Each user can change their default password as shown in ➔ 8.9.1 Device maintenance.



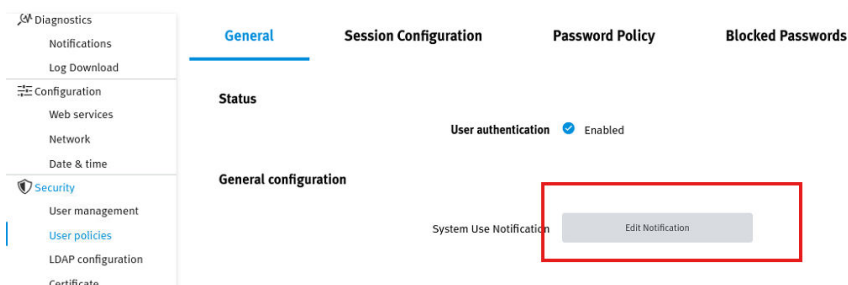
A global user management via LDAP is possible. When working with multiple devices (more than 3), Festo suggests a global, network-based user management via active directory server (LDAP). For more information on LDAP, refer to the ➔ 7.8 LDAP file-based configuration.

7.7.6.7 System Use Notification

The system use notification is displayed each time a user wants to log on to the controller. The system use notification is independent of the language of the user interface in WBM. You should therefore take all required languages into account when editing.

To edit the system use notification, proceed as follows:

1. Log in to the WBM.
 2. Open the 'Security' → 'User policies' in the WBM.
 3. On the 'General' tab, click the 'Edit Notification' button.
- ⇒ An input window opens.



4. Edit the System Use Notification.
 5. Confirm the entry by clicking the 'Save' button.
- ⇒ The text is then transferred to the controller and stored.

7.7.6.8 Creating Users

1. Open 'Security' → 'User Management'.
2. Click the '+' button.
3. Enter a username and an initial password following the password complexity rules.
4. Click 'Create user'.
5. Select a password ruleset and click 'Set Password Rules'.
6. Select the required roles and click 'Set User Roles'.

Create at minimum the following users:

- 'SecurityEngineer' + 'UserManager' ('Admin Ruleset')
- 'SecurityAuditor' ('Admin Ruleset')
- 'Engineer' ('Default Ruleset')

Default 'admin' user

The CEPE is delivered with a unique device-specific administrator password printed on the device, see ➔ 7.7.2 Get Familiar with the CEPE. Use it only for initial access.

Change the password immediately:

1. Log in to the WBM as 'admin'.
2. Open 'System' → 'Device Maintenance'.
3. Set a new administrator password.



The printed default password becomes valid again after a factory reset. Protect the device physically and treat the printed credentials as sensitive information.

For the complete user management reference including session configuration, password validity, and LDAP, see ➔ 7.7.6.5 User Management.

7.7.6.9 'admin' User

The 'admin' user is allowed to make changes via SSH. For the commissioning phase it is possible to configure the 'admin' user to make changes to CEPE configuration files. Afterwards the 'admin' must be deleted again in the 'User Manager'!

NOTICE

Unauthenticated access

More accesses are possible via the 'admin' user. This can disrupt production and reduce security.

- Do not start any plant with activated 'admin' user!

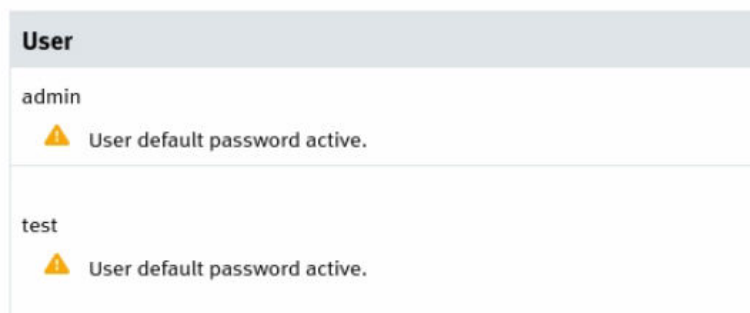
7.7.6.10 Changing the password

NOTICE

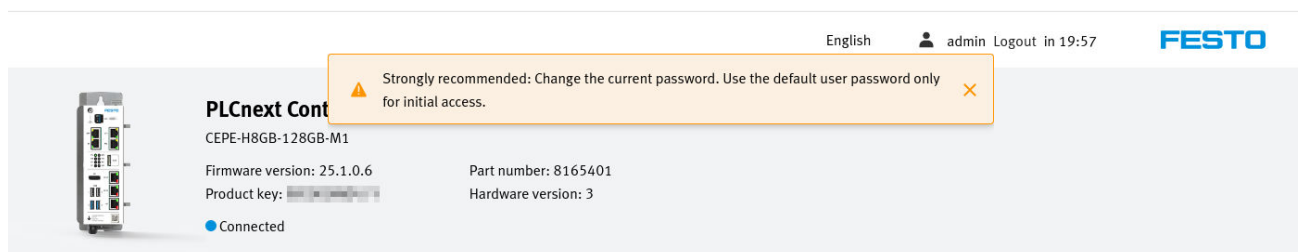
It is strongly recommended that you only use the default user password for the first access. Change the default password immediately after the first access.

- If you have created a user, you will see a corresponding message in the WBM to change the default password
- To protect your account and data, choose a strong, unique password and keep it confidential.
- Use a reputable password manager to store your passwords securely.
- The 'admin' password printed on the controller is valid again after resetting the controller to default settings.

Message to change the default password:

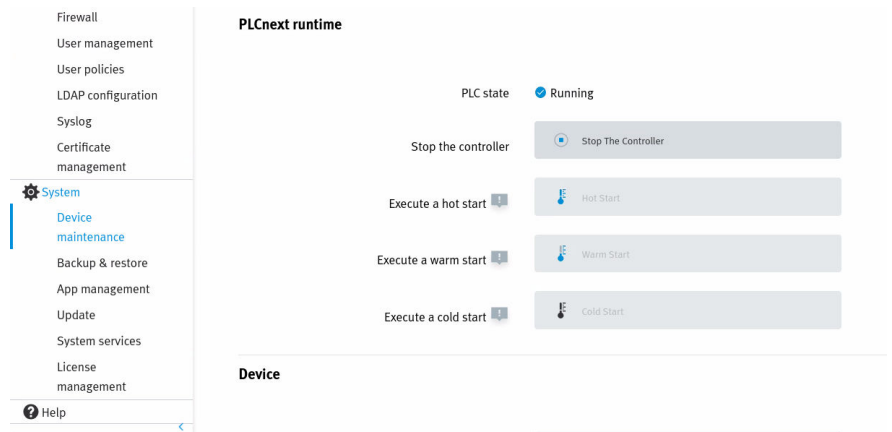


The system informs the user via the following pop-up message that the password should be changed:

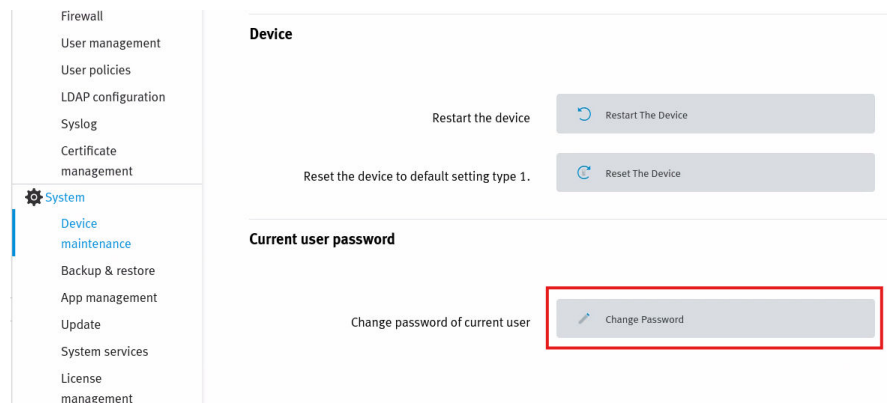


Following steps have to be done to change the default password of the currently logged in user:

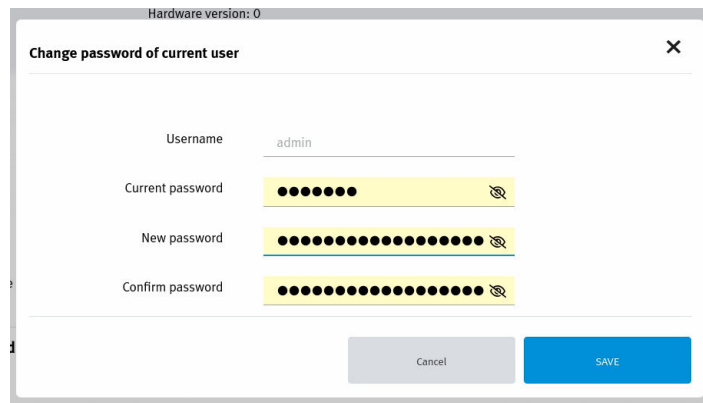
1. Go to the WBM page 'System' - 'Device Maintenance'.



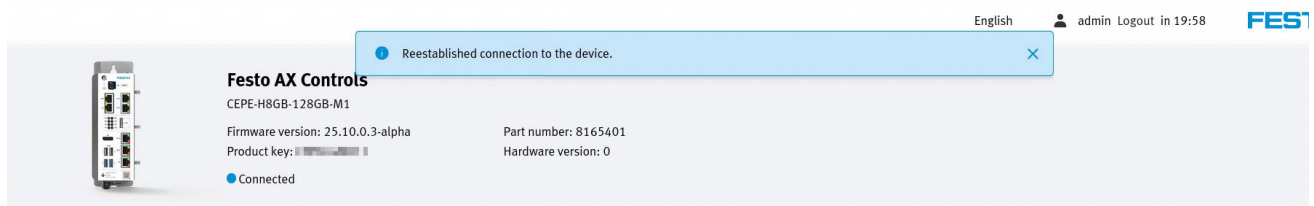
2. Scroll down and click the 'Change Password' button.



3. Fill out prompted Current password, enter the new password twice and confirm by clicking 'Save'.



4. Now the pop-up message is gone.



7.7.6.11 Password Policies

Two sets of password policies are available for selection in WBM user management when creating users - 'default' and 'admin'

- 'default' is 8 character minimum with no other restrictions
- 'admin' is 10 character minimum (default password length at production label: 16 chars)
 - 2 character ASCII minimum
 - 1 Lower and 1 Upper case minimum
 - 1 Digit minimum
 - 1 Symbol minimum - () { } # , ; . : ^ ? ! | _ ' ~ @ \$ % / \ = + - &
 - Username cannot be used in password
 - Last 5 password cannot be reused
 - expiration policy is not enabled
 - blocked password list is not enabled
 - frequent change restrictions are not enabled

7.7.6.12 System services

NOTICE

Activating further system services can compromise security

Before activating further system services, you must perform a risk and threat analysis of the system service and its impact on the security of the device and the application, taking into account the overall security context.

The WBM page 'System' → 'System Services' shows which services are enabled, disabled, and enabled by default.

Service ID	Service name	Factory default	Activation
APP MANAGER	App Manager	 Activated	
GRPC LOCAL SERVER	gRPC Remote Procedure Calls (Local)	 Activated	
MCD2	Festo Device Discovery	 Activated	
Mount USB1	mount USB1 to /media/usbstorage/usb1_fixed (Safe removal: stop all processes using USB1 before deactivating the service)	 Deactivated	
Mount USB2	mount USB2 to /media/usbstorage/usb2_fixed (Safe removal: stop all processes using USB2 before deactivating the service)	 Deactivated	
Mount USB3	mount USB3 to /media/usbstorage/usb3_fixed (Safe removal: stop all processes using USB3 before deactivating the service)	 Deactivated	
Mount USB4	mount USB4 to /media/usbstorage/usb4_fixed (Safe removal: stop all processes using USB4 before deactivating the service)	 Deactivated	
OPCUA	OPC UA Server	 Deactivated	
PLCNEXT STORE	PLCnext Store Connector	 Deactivated	
SOFTWARE UPDATE	Software Update via Device and Update Management	 Activated	
SSHD	SSH daemon Socket	 Deactivated	

General notes:

- To use services, it is necessary to enable the ports used by the service in the firewall, see Extended Firewall settings → 8.8.3 Firewall.
- The firewall blocks/ filters only incoming packets (Direction: Server).

Disabling unused system services can be helpful to gain the performance of running programs.

NOTICE

Before disabling a default service, verify its function in the overall application. Some apps or maintenance functions depend on enabled services and open firewall ports.



With changing a setting, the whole 'System Services' settings are overwritten, so settings induced by a App will be set back, too. Make sure to leave those settings untouched, or refer to the App documentation to re-enable its system services settings.

Enabling or disabling a system service

If you want to use a System Service that is not active by default in the factory settings, or if you want to re-enable a System Service that has been disabled before or you want to disable a system service:

1. To changes the activation state, click on the toggle switch of the wanted service(s) under 'Activation'.
2. Apply the change(s) with the 'Apply and reboot' button, and confirm the pop-up warning.
3. After a reboot, the service toggled activation state is active as indicated in this WBM page.

Overview to the available system services



Note: Service availability is subject to the device in use.

Service ID	Description	Direction	Factory default	Port (Firewall default)	Protocol	Certificate
Mount USB <X>	Mounts USB drive /media/usb-storage/usb<X>_fixed automatically	-	deactivated	-	-	-
AppManager	Deactivating the App Manager only prevents accessing the App management page of the WBM	Server	activated	TCP 443 (Accept)	TLS 1.3	HTTPS
GRPC LOCAL SERVER	Local gRPC communication service	Server	activated	Localhost	–	Socket Linux access rights
PLCNEXT STORE	Connection to the app store for app downloads and license management	Client	activated	TCP 8883 (Accept)	TLS 1.3 / MQTT	Official AWS root certificates
SOFTWARE UPDATE	Enables performing firmware updates via WBM	Client	activated	TCP 443 (Accept)	TLS 1.3	IdevID HTTPS
MCD2	Festo Multicast daemon. Multicast-based discovery and commissioning	Server	activated	UDP 10002 (Accept)	FGMC (Festo, proprietary)	–
SSHD	SSH access to the controller shell	Server	deactivated	TCP 22 (Drop)	SSH	-
WBM	Web interface for device configuration and monitoring	Server	activated	TCP 443 (Accept)	TLS 1.3	IdevID HTTPS
OPCUA	OPC UA server	Server	deactivated	TCP 48010 (Drop)	OPC UA	OPC UA Sign and Encryption
Remoting	Remote Service Call communication for engineering tools	Server	activated	TCP 41100 (Accept)	RSC (Proprietary) over TLS 1.2	IdevID Device Certificates

Tab. 29



To use services, it is necessary to enable the ports used by the service → 8.8.3 Firewall.

7.7.7 Setup Certificate

Configure the HTTPS certificate and TLS version during initial commissioning.

Configuring TLS

1. Login to the WBM.

- Open the 'Configuration' → 'Web Services' page.

Festo AX Controls
CEPE-H8GB-128GB-M1
Firmware version: 26.3.0.4-alpha
Product key:
Part number: 8165401
Hardware version: 0
Connected

NGINX web server

WARNING: Applying the configuration can affect the real-time behavior of the system. Avoid reconfiguration during productive operation.

TLS configuration

TLS version(s) ☐ TLSv1.2 ☒ **TLSv1.3**

Cipher Suites **Secure HTTPS TLS Ciphers**

TLSv1.2:ECDSA+DHE:!(NULL:!(AES
ECM8:ICAMEL:!(LUA:!(PSK:!(RSA:!(SHA:!(

HTTPS certificate

Identity store for HTTPS certificate **HTTPS-self-signed**

- Configure TLS. Select 'TLSv1.3' for highest security.

NOTICE

- If you cannot set TLS version TLSv1.3, set TLS version TLSv1.2.
- If you set TLS version TLSv1.2, you must set 'Secure HTTPS TLS Ciphers' as the cipher suite.
- If the target browsers do not support the secure cipher suite, set the 'Default HTTPS TLS Ciphers', but be aware that this is not considered a secure approach.

Generating self-signed HTTPS Certificate Configuration

- Log in to the WBM.
- Open the 'Configuration' → 'Web Services' page in the WBM.

Self-signed HTTPS certificate

Distinguished Name (DN)

Common Name (CN) **Festo HTTPS Interface List**

Organization (O) **Festo**

Organizational Unit (OU) **Festo SE & Co. KG**

Location (L) **Esslingen**

State or Province Name (ST) **BW**

Country (C) **DE**

Validity

Not before **06 / 18 / 2024** **11 : 57 AM**

Not after **12 / 31 / 9999** **11 : 59 PM**

Subject Alternative Names

Use Current IP Configuration

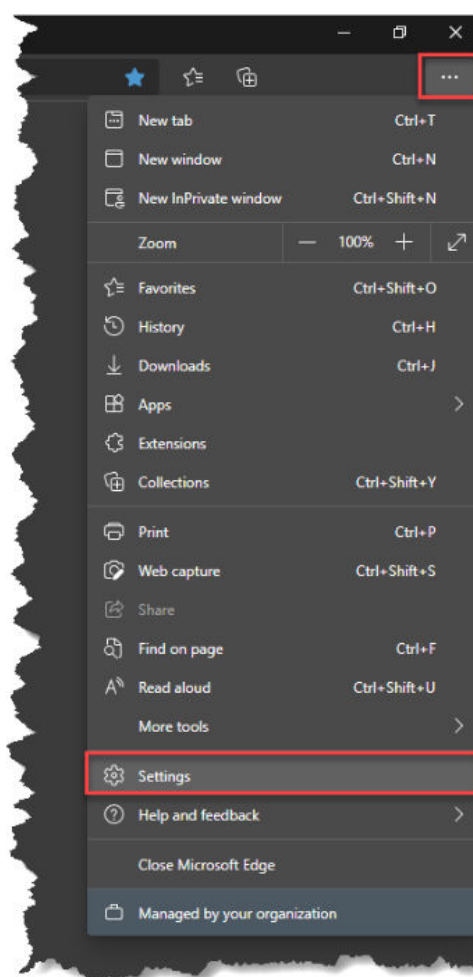
Subject Alternative Name	Type
192.168.1.10	IP address

- In the 'Identity store for HTTPS certificate' drop-down menu, select 'HTTPS-self-signed'.
- In the 'Self-signed HTTPS Certificate' area, enter the required information.

5. In the Subject 'Alternative Names' area, enter the required IP addresses.
6. Add more IP addresses if needed by clicking the '+'.
 - ⇒ If the certificate generation was successful, it will be displayed in a message at the top of the WBM.
7. Click the 'SAVE & APPLY PAGE' button.

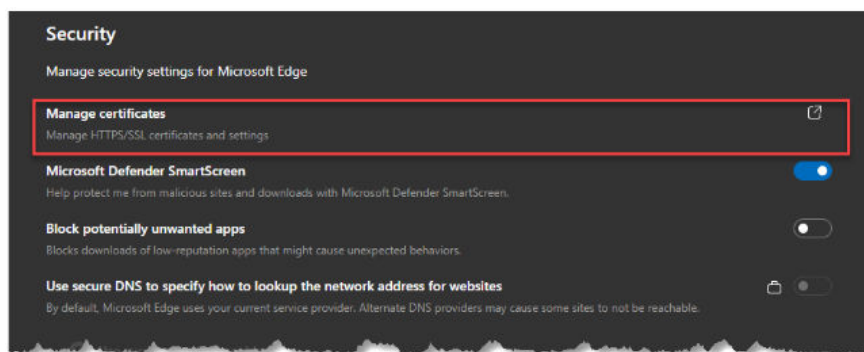
Uploading the certificate in the browser

1. Log in to the WBM.
2. Open the 'Security' → 'Certificate Authentication' page in the WBM.
3. Open the 'Identity Stores' tab.
4. In the 'HTTPS-self-signed' area, download the certificate you just generated by clicking the button 'Download from controller to local pc' next to the certificate.
5. Open your browser (Edge).
6. Open the 'Settings' menu.



7. Open the 'Privacy, search, and services' tab.

8. In the 'Security' section, click the 'Manage certificates' button.
⇒ A new window opens.

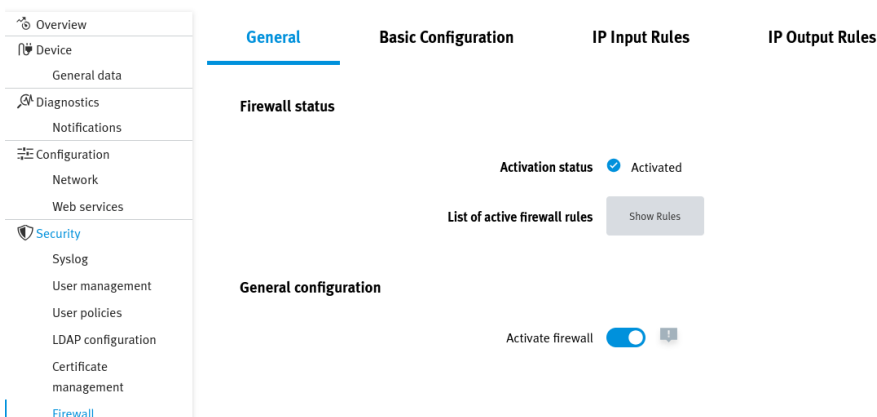


9. Open the 'Trusted root certificates' tab.
 10. Click the 'Import...' button.
⇒ The "Certificate Import Wizard" opens.
 11. Follow the instructions of the 'Certificate Import Wizard'.
 12. Select the certificate you want to import and click the 'Open' button.
 13. Click the 'Next' button.
 14. Select 'Place all certificates in the following store' and click the 'Browse...' button.
 15. Set the 'certificate store' option to 'Trusted root certificates' and click the 'OK' button.
 16. Click the 'Next' button.
 17. Click the 'Finish' button.
 18. If a warning note opens, read the warning note and in case you want to confirm it, click the 'Yes' button.
⇒ The certificate was uploaded in the browser.
 19. Check the status of the certificate in your browser.
- For the complete TLS and certificate reference including all certificate options, see ➔ 8.8.2 Certificate management.

7.7.8 Configuring basic firewall settings

Verifying the Firewall Status

1. Log in to the WBM.
2. Open the 'Security' → 'Firewall' page in the WBM.
3. On the 'GENERAL' tab, check in the Firewall status section whether the activation status is 'activated' and in the 'General configuration' section whether the checkbox 'Active firewall' is activated.



Reviewing the Basic Configuration

1. Check on the 'Basic Configuration' tab whether only the following incoming connections are enabled:

Service	Protocol	Port	Default Action
Remoting	TCP	41100	Accept
WBM (HTTPS)	TCP / HTTPS	443	Accept
Festo Multicast Protocol (mcd2)	UDP	10002	Accept

2. Optional: Export the list of activated firewall rules. This may be helpful if you want to save the firewall rules in your plant documentation. For information on how to proceed with that, refer to "Extended Firewall settings" → 8.8.3 Firewall.
3. Check whether further user-defined settings are necessary for your application.
4. If you need to allow further ports, open the 'IP INPUT RULES' tab or the 'IP OUTPUT RULES' tab. For further information see "Extended Firewall settings" → 8.8.3 Firewall.

APP CODESYS PLC (x86)

Service	Protocol	Port	Default Action
CODESYS WebVisu	TCP / HTTPS / Web-Socket	8443	Accept
CODESYS Control runtime system	UDP	1740 - 1743	Accept
CODESYS Control runtime system	TCP	11740	Accept
CODESYS Gateway	TCP	1217	Accept
CODESYS OPC UA	TCP	4840	Accept

Tab. 30

APP CODESYS PLC (x86) services (and ports) are explained in the CODESYS PLC - User Guide: → www.festo.com.

7.7.9 Security Logging

Log in to the WBM. For access instructions, see → 7.7.6.1 Connecting to Web-based Management.

- Open the 'Diagnostics' → 'Notifications' page.



The 'Admin', the 'SecurityEngineer', and the 'SecurityAuditor' have access to the security notifications.

The 'UserManager' assigns a Security Token to each user who logs in. The Security Token is displayed at the corresponding notifications for all activities.

The security token is a representation of a user logged in to Festo AX OS.

In the notifications, it replaces the user name with a series of characters.

When the user logs in for the first time, a notification is generated that assigns the user name to the security token.

For all subsequent actions, only the security token is used to identify the user.

Example: The user 'admin' receives the Security Token `D9E7FA4F`. The user is identified by this Security Token in the following messages.

Filter

Notifications

Severity	Time	Sender	Name	Notification
	2026-05-29 14:41:47	User Manager	Security.Arj.System.Um.SessionCreated	Session created. User: admin, User roles: Admin, Security Token: D9E7FA...
i	2026-05-28 18:27:04	User Manager	Security.Arj.System.Um.SessionClosed	Session with security Token 3D43A43E was closed due to timeout, currently ...
i	2026-05-28 18:08:56	Security Store Manager	Security.Arj.Services.SecurityStoreManager.TrustSto...	Trust Store empty added. Current Security Token: 3D43A43E
i	2026-05-28 18:03:34	Web Configuration Manager	Security.Arj.Services.Wcm.CertificateRegenerated	Self-signed HTTPS certificate regenerated. Subject: C=DE,ST=BW,L=Essling...
i	2026-05-28 18:03:34	Web Configuration Manager	Security.Arj.Services.Wcm.IdentityStoreChanged	Identity Store for HTTPS certificate set. Store name: HTTPS-self-signed, new ...
i	2026-05-28 18:02:27	Web Configuration Manager	Security.Arj.Services.Wcm.HttpsTlsConfigSet	Cipher Suites Set: SecureCiphers, TLS Versions: TLSv1.3
i	2026-05-28 17:55:40	User Manager	Security.Arj.System.Um.SessionCreated	Session created. User: admin, User roles: Admin, Security Token: 3D43A43...
i	2026-05-28 14:42:41	User Manager	Security.Arj.System.Um.SessionClosed	Session with security Token 0D537D2E was closed due to timeout, currently...
i	2026-05-28 14:21:28	User Manager	Security.Arj.System.Um.SessionCreated	Session created. User: admin, User roles: Admin, Security Token: 0D537D2...

Session created. User: admin, User roles: Admin, Security Token: D9E7FA4F, Object name: Wbm, currently opened Sessions 2

Export CSV File

The Security Engineer and the Security Auditor have access to the security logging. On the basis of the notifications it is possible to see how the CEPE is booted, whether integrity is given, and general information about all activities of the logged-in users, including who changed what, when, and how, in the sense of non-repudiation according to IEC 62443.



To see all messages and remove the filter, click the 'RESET FILTER' button.

Filter

Severity >= Internal

Archive name <All archives>

Sender

Maximum number of notifications 1024

Time from mm / dd / yyyy

Time to mm / dd / yyyy

Reset Filter

Apply Filter

For more information on security logging, refer to the topic ➔ 8.6 Diagnostics.

Ensuring Audit Storage Capacity

Notification Manager: Configurable file size, default 10 MB. When the limit is reached, a configurable number of messages are deleted, default 16. Security messages are handed over to syslog. Logrotate is executed every hour. The sysloging interface for external logging can be configured.

7.7.10 Further setup

Apps and Licenses

Install the Apps you want to use for development, see ➔ 8.9.3 App management. Apps are software applications from libraries up to complete programs that are provided by the App Store. After registering you can download apps from ➔ www.festo.com or the PLCnext Store ➔ www.plcnextstore.com/ (filter for devices from Festo).

Do not use Third-party Apps provided in another source then ➔ www.festo.com or ➔ www.plcnextstore.com/. This will introduce a high security risk for you Industrial network and safety.

7.7.11 User Data Protection

This section documents the methods for collecting, using, processing, and transmitting user data on the controller and the security measures applied to protect this data.

Scope and Definition of User Data

User data refers to all settings and modifications made on the device on behalf of the user, including but not limited to:

Data class	Abbrev.	Description
Configuration Data	CD	Configuration data is located on the devices used to build automation infrastructures and systems
Log Data central	LD	Log data stored on a central Syslog server
Log Data onboard	LO	Log data available on the device, logging can be configured
Application Data	AD	Application data is located on the devices
Process Data	PD	Process data transferred between the devices and processed there
System Data	SD	System data (licenses, access data, keys, certificates) located on the devices
Recipe Data	RD	Recipes (which may also include proprietary data and trade secrets)
Parameter Data	PAD	Variable values (e.g., min, max)
Backup Data	BD	Backed-up data

Tab. 31

Data elements are classified as:

- **Personal data:** data that can be linked to a specific user or account (e.g. user-names, login IDs, IP addresses when linked to an account).
- **Sensitive data:** security-relevant or confidential data (e.g. password hashes, private keys, security-related identifiers).

Methods of User Data Collection

All user data is collected exclusively through explicit user actions via the following control network connections, see ➔ 8.9.5 System services for technical details:

Control network connections	Protocol	Primary Data Classes	Details / Examples
Web-Based Management (WBM)	HTTPS/TLS	CD, SD, PAD, BD, AD	Configuration changes (CD), user/account data & credentials (SD), parameter settings (PAD), backup/restore (BD), application configs (AD)
Remote Service Calls (RSC)	TLS	CD, LD, LO, BD, AD	Remote engineering modifies configuration (CD), retrieves logs (LD/LO), exports system/log dumps (BD), diagnostics data (AD)
LDAP	TLS	SD	User accounts, roles, authentication metadata (SD)
Syslog-ng (central logging)	TLS	LD	Central collection of log data (LD) only
Local Logging (onboard)	–	LO	Device-internal logs (LO), configurable logging level and scope
NTP	NTP	SD (limited)	Time synchronization data (system time, timezone indirectly → SD)

Tab. 32

User data is not collected automatically or transmitted without explicit user action. The following features interact with user data:

- **Logging:** user actions in WBM, CLI/SSH commands, and application events are logged with username, action type, timestamp, and client IP.
- **User Management:** account IDs, credentials, roles, and password policy metadata are stored.
- **Network and Firewall Configuration:** IP addresses, routes, firewall rules.
- **Certificates:** TLS certificates, certificate chains, and associated metadata.

Use and Processing of User Data

- **Licenses:** Codemeter license identifiers and activation data.
- **System Time:** time zone configuration (may indicate site location).

Main processing activities:

- **Logging:** system-wide logging of events and user actions. Export via Log Dump for diagnostics.
- **Backup and Restore:** creation of backup archives containing user data. Restoration of device configuration from backups.
- **Reset and Restore:** deletion or reset of user accounts and configuration to initial state.
- **Authentication:** verification of user credentials (username and password hash).
- **Authorization:** enforcement of user roles and permissions for WBM pages and RSC services.
- **Accountability:** logging of user actions (who performed which action and when).

Transmission of User Data

All user data is transmitted only on behalf of the user via encrypted control network connections, see also → 7.10 Security Hardening.

Control network connections	Protocol	Transmitted Data
Web-Based Management (WBM)	HTTPS/TLS	Configuration changes, user management operations, backup downloads, log dumps, notifications
Remote Service Calls (RSC)	TLS	System and log dump archives, configuration and diagnostic data, user management operations

Tab. 33

Security Measures for User Data

The following security measures protect user data during collection, storage, use, processing, transmission, provision, and disclosure:

- **Collection:** user data is collected only through authenticated sessions. Access requires valid credentials and is restricted by role-based access control, see → 8.8.4 User management.
- **Storage:** user credentials are stored as password hashes (not plaintext). Private keys and certificates are stored in protected directories. The OverlayFS mechanism protects system integrity, see → 6.3 Overlay file system.
- **Use and Processing:** access to user data is restricted to authorized roles. The system enforces the principle of least privilege.
- **Transmission:** all transmission uses encrypted protocols (TLS 1.2/1.3, SSH). No unencrypted transmission of user data occurs.
- **Provision and Disclosure:** the diagnostics explicitly excludes security-sensitive files (keys, certificates) by blacklisting file types (.pem, .key, .crt, .p12, .der, .pfx).
- **Deletion:** factory reset removes user data including accounts, configuration, and logs. Certain data (licenses, device identification) may be retained as documented in → 7.13 Reset Procedures.

CODESYS PLC (x86) user data handling is explained in the CODESYS PLC - User Guide: → www.festo.com.

For user management configuration, see → 7.7.6.5 User Management.

For logging configuration, see → 7.11 Configuring Central logging.

For backup and restore procedures, see → 8.9.6 Backup and Restore.

7.8 LDAP file-based configuration

7.8.1 Concept

The LDAP server enables central management of the users in a network (e.g. a Microsoft Active Directory). The PLCnext user authentication can be connected to an LDAP server. A central user management allows to manage user accounts, their passwords and group memberships at a central level. With an LDAP server there is no need to setup user accounts and passwords on every single controller.

The benefits are:

- If a password change is necessary, it only needs to be changed once inside the LDAP directory and not in every controller.
- New users can be added without the need of configuring every controller.
- New user permissions and rights can be rolled out in a very simple way.
- A blocked user affects the entire system and not only a single controller.

The `User Manager` supports the TLS protocol for the connection to an LDAP server (LDAPS, LDAP with StartTLS). It supports the authentication of users against the LDAP server with user name and password by using the LDAP bind command. The LDAP authentication is performed in addition to the local user data base. If the authentication is successful for one of the two sources, the authentication is considered successful. No further authentication is necessary.

If the authentication fails because of a wrong or unknown user name or due to a communication error with the source, the authentication is continued with the next source. The local user database (managed via WBM) is always the first source. After this the LDAP servers are used in the configured order.

If one authentication fails because a wrong password was entered, the login fails and no further sources are used.

The `User Manager` validates the server certificate of the LDAP server. The validity check is made using a configurable `TrustStore` which is referenced by its name.

7.8.2 Reference

Configuration of an LDAP connection

In order to set up an LDAP connection, you need to create an XML configuration file as described below.

Be aware of the XML entities when editing XML configuration files! There are symbols in the XML code that cannot be represented as attribute values because they have a syntactical function.

For example, the characters `<` and `>` are used for opening and closing XML tags. To be able to use these characters as attribute values in their genuine meaning "less than" or "greater than", entities are required.

The following entities are predefined in the XML specification. Make sure to use these entities in attribute values to avoid XML parsing errors.

Character	Entity
Ampersand (&)	<code>&amp;</code>
Single quote (')	<code>&apos;</code>
Double quote (")	<code>&quot;</code>
Less than (<)	<code>&lt;</code>
Greater than (>)	<code>&gt;</code>

Tab. 34

Overview on configuration options

It is possible to configure up to 10 LDAP server connections. To set up a User Manager to LDAP connection you have the following configuration options:

Option	Description	Default	Optional/Mandatory
LDAP host/IP	DNS name or IP address of the LDAP server		Mandatory
Port	TCP port of the LDAP server	"389"	Optional
timeout	The network timeout after a connection attempt to the ldap server failed	"10s"	Optional
Enable TLS	Activate/deactivate TLS	"true"	Optional
Use StartTLS	Usage of StartTLS instead of TLS (this option only has an effect when TLS is activated)	"true"	Optional
TrustStore name	Name of the Trust Store, that is used for verification.	"ldap"	Optional
cipherList	List of permitted TLS cipher suites for the LDAP connection	"NORMAL:-VERS-TLS1.0:-VERS-TLS1.1:-VERS-DTLS1.0:-SHA1:-SIGN-RSA-SHA1:-SIGN-ECDSA-SHA1:-RSA"	Optional
Base DN	DN (Distinguished Name) where the LDAP search for users starts		Mandatory
Search filter	LDAP filter that is used for the search for users.		Mandatory
Bind DN	DN that is used for the bind before the search		Optional
Bind password	Password for the "Bind DN"		Optional
Group attributes	List of LDAP attributes that save the group membership of a user, e. g. "memberof"		Mandatory
LdapGroup / Role Mapping	Mapping configuration of LDAP groups to PLCnext roles		Optional

Tab. 35

Configuration files

The configuration for the LDAP connection is set using XML configuration files. All of the important settings can be configured directly in the Ldap.config configuration file on the controller. To modify the configuration, the XML file can be edited using any editor. You will find the file in the /opt/plcnext/config/System/Um directory of your controller. The file system is accessed via the SFTP protocol. Use a suitable SFTP client software for this, e.g., WinSCP.

Example of an LDAP configuration file

```
<?xml version="1.0" encoding="UTF-8"?>
<LdapConfigurationDocument
  xmlns="http://www.phoenixcontact.com/schema/ldapconfiguration"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.phoenixcontact.com/schema/ldapconfiguration"
  schemaVersion="1.0">
  <LdapServer hostname="192.168.1.40" port="389" order="1">
    <LdapSecurityOptions tlsEnabled="true" useStartTls="true" trustStore="ldap" />
    <LdapSearchOptions baseDN="dc=example,dc=org" searchFilter="(uid=$$USER$$)" />
    <LdapLoginOptions bindDN="cn=admin,dc=example,dc=org" bindPassword="admin" />
    <GroupAttributes>
      <GroupAttribute name="memberOf" />
    </GroupAttributes>
    <GroupMappings>
      <GroupMapping ldapGroup="cn=plcAdmin,dc=example,dc=org" localRole="Admin" />
      <GroupMapping ldapGroup="cn=plcReader,dc=example,dc=org" localRole="Viewer" />
    </GroupMappings>
  </LdapServer>
</LdapConfigurationDocument>
```

LDAPServer

One configuration file can be filled with the configuration of up to 10 LDAP servers. Every server is configured with the element `<LdapServer>` and `</LdapServer>`. The element can be extended with the following attributes:

– `hostname`

Add the host name or the IP address of the LDAP server. This information is obligatory.

– `port`

The port is chosen automatically. Port 389 for connections without TLS or StartTLS and port 636 for TLS connections. If necessary you can specify the port where the LDAP server can be reached.

– `order`

The server entries are ordered according to the order number (int32) specified in this attribute. They are sorted and processed according to this order number for an authentication request.

– `timeout`

The network timeout after a connection attempt to the LDAP server failed. Enter a value with one of the following units:

- `ns` (nanoseconds)
- `us` (microseconds)
- `ms` (milliseconds)
- `s` (seconds)
- `h` (hours)

The `LdapServer` element can contain the following XML elements for further configuration:

– `LdapSecurityOptions`

Settings for TLS. The following attributes can be used to specify the settings:

- `tlsEnabled`: Activate (`true`) or deactivate (`false`) TLS for the LDAP server
- **Recommendation**: use `true` for security reasons

- `useStartTls`: Activate (`true`) or deactivate (`false`) the usage of StartTLS. When the usage of StartTLS is deactivated and TLS is activated, a direct TLS connection to the LDAP server is established.

- `trustStore`: Specifies the name of the TrustStore for the verification of the LDAP server certificate. In case the name contains an empty string (""), the certificate verification is switched off, which means that the connection to the LDAP server is established without verifying its certificate. In case a TrustStore is empty, the verification process fails, which means that the connection to the LDAP server cannot be established at all.

Recommendation: set certificate for security reasons

Note: If a TrustStore is changed that is referenced by an LDAP server configuration (e.g. by adding certificates for LDAP), a restart must be performed. The changes only take effect after the restart.

- `cipherList`

The `cipherList` attribute configures allowed TLS cipher suites which are supported by the LDAP client to establish a TLS connection to the LDAP server. This setting is only enabled, if TLS or StartTLS is activated. The format must follow the rules of GnuTLS → gnutls.org/manual/html_node/Priority-Strings.html.

A secure setting is established by default (can only be ensured with a current firmware version). The rules comply with the recommendations of the Technical Guideline on the use of TLS TR-02102-2 → TR-02102-2 by the German government institution "Federal Office for Information Security", with the following exceptions:

Curve25519 is enabled, CHACHA20 and POLY1305 are allowed.

Note: The default value can be subject to change in new firmware versions. The setting will be updated if new recommendations are published.

- `LdapSearchOptions`

Settings for the user search in the LDAP server. The following attributes can be used to specify the settings:

- `baseDN`: The LDAP DN (Distinguished name) that serves as starting point for the search for users over all child nodes.
- `searchFilter`: LDAP search filter that is used for the search for users. The variable "\$\$USER\$\$" is automatically replaced with the login.

- `LdapLoginOptions`

Login settings for the LDAP server. Before the user search can be performed, a authentication (bind) is required.

- `bindDN`:
Distinguished Name of the user the search in the LDAP directory is performed with.
- `bindPassword`:
Password of the "bindDN" user in the LDAP server.

Direct bind to LDAP server without user search

You have the possibility to configure the LDAP server so that the search for the correct user is not performed in the LDAP. For this purpose a bind with the user name and password that is entered into the login mask is executed. The bind will

be performed with the configured `bindDN`. The attribute contains the `$$USER$` placeholder which is replaced with the login and the password which was entered for the login.

In order to activate the direct bind, proceed as follows:

– Add "`$$USER$$`" to the attribute `bindDN`.

Example: `bindDN="uid=$$USER$$,dc=example,dc=org"`

As a result the settings `baseDN`, `searchFilter` and `bindPassword` will be ignored.

7.9 Security context

To achieve security in an automation system, a holistic approach is necessary. An adequate security concept must cover the technologies used, the defined processes, and the people involved. Both technological and organizational measures must be taken into account.

Technical automation solution measures include:

- network segmentation and architecture
- firewall configuration, management of network segmentation, and device protection
- user management with Role-based Access Control (RBAC)
- local and centralized (LDAP) user management configuration
- Transport Layer Security (TLS) for secure communication
- certificate management for asymmetric cryptography and key management
- local and centralized security logging
- network-wide time synchronization
- network-wide device and update management
- secure configuration of the automation application
- local and centralized backup and restore

Generic Concept – Defense-in-Depth

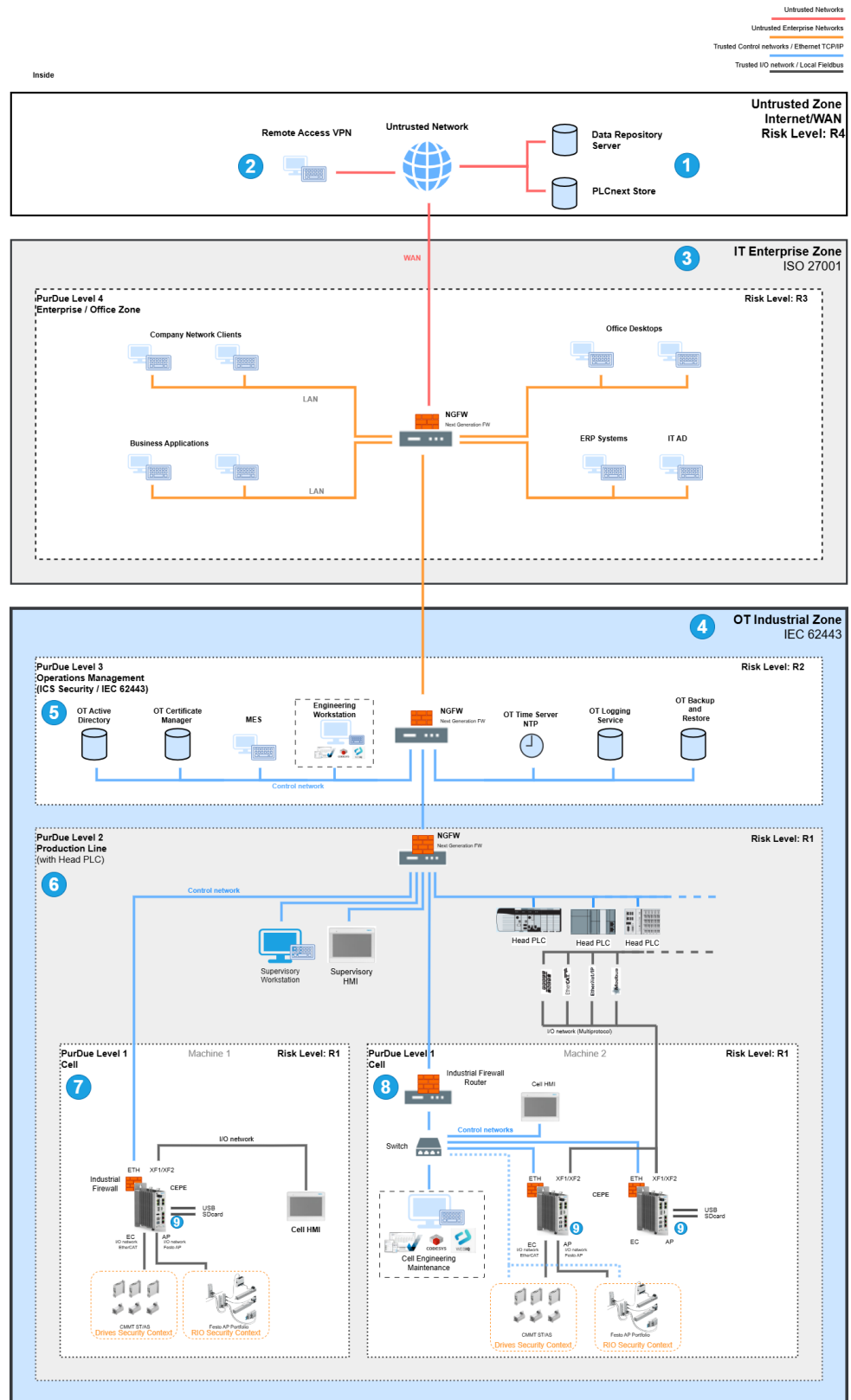
Defense-in-depth design of automation systems is an important IEC 62443 process measure to achieve reliable security. The result is a generic layered architecture that leads step-by-step to a fully segmented network layer structure that describes the Festo AX OS security architecture and the security use cases in the so-called security context.

A generic defense-in-depth design results in three layers or zones:

- **Perimeter security**: outer boundaries of the network, protected by physical measures such as fences, doors, physical access controls
- **Network security**: enterprise/office zone and service management zone (DMZ), protected by well-known IT security concepts
- **System integrity**: OT devices and applications, protected by IEC 62443 concepts

Festo AX OS Security Context

The following describes the Festo AX OS generic security context (zones and conduits) focusing on OT security based on IEC 62443-4-2 requirements.



1 Cloud connectivity

- PLCnext Store: for downloading and managing apps
- Data Repository Server: Provides data for patch management/asset management

2 Remote maintenance

3 Enterprise / Office zone

- Factory IT
- ERP (Enterprise Resource Planning) systems
- Business Applications
- Company IT Network Clients
- Production control systems.
- Protected by Next Generation Firewall (NGFW)

4 **System integrity**

Factory OT consisting of zones 5 to 8

5 **Operations Management**

Manages and optimizes production execution.

- MES (Manufacturing Execution System)
- OT Certificate Management
- OT Logging Service (e.g. syslog-ng server)
- OT Backup and Restore
- OT Active Directory (e.g LDAP)
- OT Time Server (e.g. NTP, , GPS-based time base)
- Engineering Workstation (e.g. Festo Automation Suite, CODESYS IDE)
- Next Generation Firewall (NGFW) with DPI/IDS/IPS

6 **Production Line**

SCADA, Supervisory Control and Data Acquisition

- Real-time monitoring of production progress
- Supervisory control functions via the Supervisory Workstation
- Supervisory HMIs (process visualization, alarm management)

7 **Machine/Cell Level**

Collects and processes of data from the process and the sub-process.

This zone is composed as follows:

- Festo AX Controls Device with I/O networks
- The controller integrates a firewall and is handling the communication with the other zones (conduits).
- Cell HMI for controlling and visualization purposes
- Industrial Fieldbus (EtherCAT and/or Festo AP) I/O network connections
- Engineering Port (e.g. Festo Automation Suite, CODESYS IDE)

8 **Production line level Sub-process**

Performs a specific automation function in a peripheral unit (remote station).

This zone is composed as follows:

- Multiple Festo AX Controls Device with I/O networks
- Cell HMI for controlling and visualization purposes
- Ethernet switch
- Industrial Firewall (Firewall and network segmentation, VPN if required)
- Engineering Port (e.g. Festo Automation Suite, CODESYS IDE)

9 **Device**

Protection of critical interfaces and ports from unauthorized physical access.



Security is an overall **system design** requirement. The security context defined here must fit your required automation system use cases. **Perform a risk and threat analysis** and design sufficient security measures. Based on that analysis, you can activate or deactivate additional security features (User Management, Certificate Authority, Firewall, Syslog, etc.) via the WBM. Make sure that the device continues to meet the necessary security requirements even after your own configurations.

Consider the general security instructions as described in
 ➔ www.festo.com/psirt.

Eight Security Layers

The security context is based on the Defense-in-Depth concept providing eight security layers (zones/conduits):

Perimeter Security (outer layer):

- physical and digital isolation by network segmentation
- logical access controls
- use of specifically configured firewalls (must correspond to identified threats and vulnerabilities)
- documentation of all remote access points

Network Security layers (Enterprise / DMZ):

- identifying all network devices and hosts
- analysis of protocols and traffic
- auditing of wireless communication/traffic
- analysis of switch/router configurations
- OS vulnerability checks and patch management
- ensured use of individual user accounts

Measures in the DMZ:

- Active Directory / RADIUS server for authentication
- firewall or VPN component handles communication with other zones (conduits)
- restricted access, foreign computers restricted from connecting

System Integrity – Manufacturing zone:

- control center (SCADA)
- NTP server providing GPS-based time base to other devices
- Ethernet switch
- engineering system
- monitored network for clear-text transfer and use of encryption

System Integrity – Machine / Production line level:

- CEPE controller with I/O devices, integrating firewall handling communication with other zones
- wired vs. wireless communications analysis
- Ethernet vs. serial communications analysis
- Ethernet devices tested in lab for vulnerabilities
- removed vendor default passwords

Physical layers (Cabinet):

- install devices in a lockable and supervised control cabinet following a risk analysis
- ensure only authorized persons have access to the cabinet key
- run cables protected against unauthorized access

Physical layers (Device):

- critical interfaces and ports protected against unauthorized physical access
- security seals (security void) to protect housing and indicate opening attempts
- disabled communication on external interfaces (e.g. USB connector, JTAG)

7.10 Security Hardening

The automation system design must fit the security context and the generic use cases described in this Manual.

The CEPE supports the following functions by default:

- boot integrity
- least functionality
- no root access
- authorization with password complexity rules, lifetime restrictions, and timeouts (brute force protection)
- specialized security user roles for device configuration and security monitoring
- central user management support via LDAP
- zone and denial of service protection
- firewall configuration for each dedicated Ethernet MAC address via WBM
- validation of incoming and outgoing data via external interfaces
- certificate authority (CA) managing device identity and trusted partners
- integrity and authenticity of data in rest and data in transmission
- secure communication TLS 1.3 and OPC UA (signed and encrypted)
- security logging with protected security logging
- connection to a central logging server
- explicit deactivation and activation of Festo AX OS features via WBM
- lockable cabinet with supervision generating security notifications
- additional communication protocols can be activated via apps or libraries after performing a risk/threat analysis

The manufacturing zone should provide central time synchronization, logging, patch management, and controlled engineering access. The machine level should expose only the conduits that are required for operation.

Security Architecture

To fulfill IEC 62443-4-1 requirements, a threat analysis of the Festo AX OS Runtime System and hardware is performed. The threat analysis is based on the STRIDE model:

- **Spoofing:** impersonation of identities
- **Tampering:** unauthorized modification of data
- **Repudiation:** denial of having performed an action
- **Information disclosure:** exposure of data to unauthorized parties
- **Denial of service:** disrupting availability
- **Elevation of privilege:** gaining unauthorized access levels

Key elements of the threat analysis:

- review the integrity and authenticity of data in rest and data in transmission
- review authorization of human users and software components to access data
- review firewall protection of communication interfaces and denial of service protection

Festo AX OS provides TLS 1.3 based communication on necessary communication interfaces (e.g. HTTPS, OPC UA). For other communication channels like LDAP or Syslog-ng, TLS can be activated according to user needs. Authorization is handled by an RBAC user management for human users and certificate management for software components.

Security Measures

Data in rest:

The CEPE stores data on an internal (non-removable) flash storage.

Data in transmission:

To support secure communication via TLS, different options of cryptographic keys can be configured in the Certificate Authentication WBM page.

1. Self-signed certificates are preconfigured for HTTPS and OPC UA. Additional self-signed certificates can be configured according to user needs. For configuring the self-signed HTTPS certificate, → 8.8.2 Certificate management
2. Certificates from an asset owner's PKI can be installed. To configure dedicated asset owner identities, keys and certificates generated by a PKI can be installed in the Identity Store on the device.

Options 1 and 2 offer more flexibility for device replacement but less strict security as private keys are stored in the file system. Additional system security measures might be needed to protect the device against physical access.

User Management:

The User Management provides authentication and authorization on each communication interface. Only authorized users can access (read/write) data via a communication interface. See → 7.7.6.5 User Management and → 8.8.4 User management.

Software information integrity and authenticity:

Software information security is provided by different mechanisms:

1. Signature verification of firmware containers
2. Application project integrity checks, see → 7.7.6.4 Check the integrity state
3. App signature verification
4. Backup and restore with integrity check, see → 8.9.6 Backup and Restore
5. Each Festo AX OS-related software provided for download from the Festo website provides an SHA-512 value → 7.7.4 Software.

Malicious code protection:

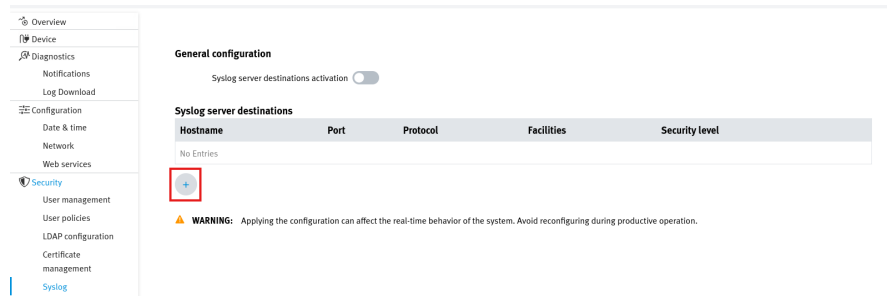
Authentication and authorization are provided by the User Management: only authorized users get access (read/write) to the CEPE's data. Engineering tool-chains generating code must be installed on secure managed PCs only. An integrity check is performed as shown in → 7.7.6.4 Check the integrity state. In the security context, one especially supervised engineering PC is installed in the manufacturing zone for engineering access to the PLCnext Control devices during maintenance phases.

7.11 Configuring Central logging

Logging in the security context only makes sense in a network. When configuring the Syslog, you set to which higher-level server the data is sent and which data it is. For information on basic security logging, see → 7.7.9 Security Logging

1. Log in to the WBM. For access instructions, see → 7.7.6.1 Connecting to Web-based Management
2. Open the 'Security' → 'Syslog' page.

- To add a new Syslog server destination configuration, select the '+' button.



Add a new Syslog server destination

General options

Hostname

Protocol

Truststore

Port

Filter options

Facilities

auth ☒

cron ☐

daemon ☐

kern ☐

local ☐

syslog ☐

user ☐

- Provide the following information:
 - ‘Hostname’: IP address of the device host to which the logging messages are sent
 - ‘Protocol’: configure ‘TLS’
 - ‘Truststore’: select the trust store
 - ‘Port’: select the port on which the devices exchange data
 - ‘Facilities’: choose what kind of data is exchanged. Choose ‘auth’ in any case
 - ‘Severity Level’: select ‘>=Information (info)’

- Click the ‘ADD’ button

In addition to the settings in the WBM, you must also make settings on the higher-level server.

- Make the necessary changes in the `syslog-ng.conf` file. The specified IP address and the selected port must be enabled in the firewall. For further information, see Extended Firewall settings → 8.8.3.1 Example Extended Firewall settings.

7.12 Configuring Software Updates

Firmware updates via WBM

Note:

Only users with the Admin or SecurityEngineer role have access to the Update page in the WBM.

- Log in to the WBM.
- Open the ‘System’ → ‘Update’ page in the WBM.

- Click the 'UPDATE' button of the firmware you want to install on your CEPE.

Status

Device health  Normal

Update list

Name	Version	
Firmware	26.3.1.4	

⇒ The 'Update Firmware' window opens

- Click the 'PREPARE AND STOP' button.

Update Firmware

Information

Status

Idle

Hardware version

0

Current version

26.3.1.4

Backup version

26.3.1.4

Pending version

N/A

Installation

Resume automatically after installation.



PREPARE AND STOP

- When the CEPE is prepared for update, deactivate the toggle switch 'Resume automatically after installation'.

Update Firmware

Information

Status

 PreparedForUpdate

Hardware version

0

Current version

26.3.1.4

Backup version

26.3.1.4

Pending version

N/A

Installation

Resume automatically after installation.



Select File

No file selected.

Select a file to upload!

RESUME

START UPDATE

6. Click the ‘SELECT FILE’ button and select the corresponding firmware file.

Update Firmware

Information

Status

PreparedForUpdate

Hardware version

0

Current version

26.3.1.4

Backup version

26.3.1.4

Pending version

N/A

Installation

Resume automatically after installation.

'Resume' must be operated manually after installation.

Select File

No file selected.

Select a file to upload!

RESUME

START UPDATE

7. Click the ‘START UPDATE’ button.

Update Firmware

Information

Status

PreparedForUpdate

Hardware version

0

Current version

26.3.1.4

Backup version

26.3.1.4

Pending version

N/A

Installation

Resume automatically after installation.

'Resume' must be operated manually after installation.

Select File

CEPE_26.3.1.4-alpha_updatepackage.raucb

RESUME

START UPDATE

8. The software package is transferred and evaluated, the signature is checked. Then the CEPE is rebooted.

Update Firmware

Information

Status

PreparedForUpdate

Hardware version

0

Current version

26.3.1.4

Backup version

26.3.1.4

Pending version

N/A

Installation

Resume automatically after installation.

'Resume' must be operated manually after installation.

The software package is transferred.

22% complete

RESUME

START UPDATE

Update Firmware

Information

Status

PreparedForUpdate

Hardware version

0

Current version

26.3.1.4

Backup version

26.3.1.4

Pending version

N/A

Installation

Resume automatically after installation.

'Resume' must be operated manually after installation.

The software package has been transferred.

(368.7 MB)

The software package is being evaluated.

RESUME

START UPDATE

9. Carry out the firmware update again so that it is installed on both partitions.

10. The respective partition is displayed during the update process:

Update Firmware

Information

Status

Installing: Copying image to rootfs.0

Hardware version

0

Current version

26.3.1.4

Backup version

26.3.1.4

Pending version

26.3.1.4

Installation

Resume automatically after installation.

The software package has been transferred.

(368.7 MB)

Copying image to rootfs.0

54% complete

RESUME

START UPDATE

Update Firmware

Information

Status

Installing: Copying image to rootfs.1

Hardware version

0

Current version

26.3.1.4

Backup version

26.3.1.4

Pending version

26.3.1.4

Installation

Resume automatically after installation.

'Resume' must be operated manually after installation.

The software package has been transferred.

(368.7 MB)

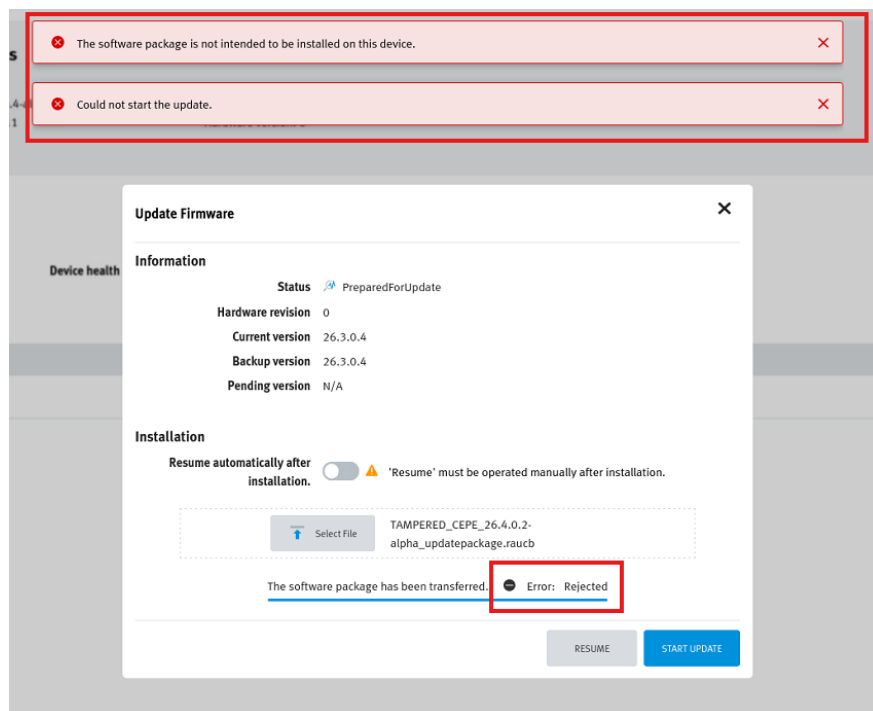
Copying image to rootfs.1

90% complete

RESUME

START UPDATE

- If the signature does not match, that is, an incorrect signature is stored, or the firmware does not match the signature, a corresponding message is displayed.



Getting a Firmware Update File

- Note the currently installed firmware version displayed on the 'Device' → 'General Data' page.
- Download the firmware file from → www.festo.com/sp
- Unzip the *.zip firmware file.
- From the unzipped folder, locate the *.raucb update container file. Downloaded software is provided with an SHA512 value. Verify the checksum before installation (see → 7.7.4 Software)

OverlayFS and User Data Preservation

The CEPE uses an OverlayFS to store user data separately from the base system. This allows firmware updates (including the root filesystem) without modifying user data. The OverlayFS is stored in the user data partition. It cannot be guaranteed that user data is 100% compatible with new firmware or apps. It is recommended to create a backup using the backup function before performing a firmware or app update, see → 8.9.6 Backup and Restore.

Installing on Both Partitions

After a successful update, install the same firmware version a **second time** so that both boot partitions contain the approved version. The respective active partition is displayed during the update process.

NOTICE

If the firmware update is not performed twice, the previous version remains on the inactive partition. After five failed boots, the system may fall back to the outdated version.

Failsafe Behavior

The firmware update uses an A/B partition scheme for failsafe operation:

Power failure during file upload phase:

- Nothing is modified; the firmware must be re-uploaded.

Power failure during SSD write phase:

- The system boots into the partition that was active before the update.
- The partition being written to is marked as bad.
- An additional firmware update will repair the failed partition.

**Post-Update Verification**

1. Verify the result in 'Device' → 'General Data'.
2. Confirm the firmware version matches the expected certified version.
3. Keep the controller on stable power during transfer and reboot.

NOTICE

If the previously installed firmware version is still displayed after the firmware update, an error occurred. Repeat the firmware update.

Issues with Updating the Firmware

If the boot process fails several consecutive times, the inactive and the active boot partition change their roles. This behavior keeps the controller accessible even if the firmware update fails. The same behavior can occur when the boot process is interrupted by power loss. In this case the controller boots with its previously installed firmware version. To prevent unintended firmware downgrades, install the same firmware version once again after a successful update. This way both the active and the inactive boot partition contain the same firmware version.

7.13 Reset Procedures**General information**

There are two reset types that you can use to reset the controller: reset type 1 and reset type 2.

Both reset types delete all the settings you have made. Reset type 2 also provides a recovery system that can be used to install new firmware.

- Perform reset type 1 if you wish to delete all the settings you have made.
- Perform reset type 2 if the firmware installed on the device is compromised or faulty and the controller is no longer booting correctly as a result.

Component to be deleted during the reset	Reset type 1	Reset type 2
Licenses	X	X
IEC 61131-3 applications	✓	✓
High-level language applications	✓	✓
Configured bus configuration	✓	✓
Network settings (192.168.1.10)	✓	✓
Changes and extensions that you have made to the operating system, to the firmware, or in the WBM	✓	✓
After the reset: Recovery system is started	X	✓

Tab. 36

How to reset with reset type 1

To reset your controller with reset type 1, proceed as follows:

NOTICE**Unintentional reset with reset type 2**

If you do not release the reset button in time, the controller is reset with reset type 2. In this case, the controller is not restarted automatically after resetting. You must open the recovery system and perform one of the possible actions.

1. Press and hold the reset button.
2. Power on the device.
3. Keep the button pressed for approximately 5 seconds
4. A housing LED starts flashing, indicating the start of the factory reset sequence.
5. Release the reset button.
6. Factory reset type 1 starts.
7. Factory reset type 1 completes.
8. The housing LED stops flashing.
9. The device reboots automatically at the end of the sequence.
10. After the reset:
Before starting up the controller again, perform all the steps that were necessary for the initial startup of the controller.



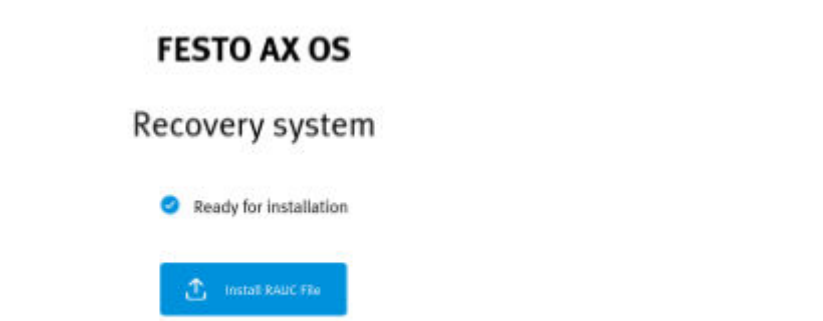
Alternatively, you can also reset the controller via the WBM with reset type 1 (System → Device maintenance).

How to reset with reset type 2

To reset your controller with reset type 2, proceed as follows:

1. Press and hold the reset button.
2. Power on the device.
3. Keep the button pressed
4. After approximately 5 seconds, the housing LED starts flashing, indicating the start of the factory reset type 1 sequence.
5. Kepp the button pressed.
6. After approximately 5 more seconds, the housing LED starts flashing at double frequency, indicating the factory reset type 2 sequence.
7. Release the reset button.
8. Reset Type 2 starts
9. Reset Type 2 finishes
10. The housing LED stops flashing.
11. The device automatically restarts into the recovery system at the end of the sequence.
12. Connect the controller to your PC using a suitable Ethernet cable.
13. Open your web browser.
14. Open the recovery system via the URL `http://`.

15. Select a firmware image file to install.



16. Upload the firmware file.



17. The system will install the firmware and restart into normal mode.



18. The Recovery System allows any firmware version that is equal to or higher than the version flashed at production. It does not have access to information about the latest installed firmware.

If the recovery system does not open:

- Check whether the URL you entered in the web browser actually starts with http://.
- The recovery system cannot be opened via an HTTPS connection.



As long as the recovery system is active, the reset button has no function.

19. You can perform the following actions in the recovery system:

- Install new firmware
- Restart the controller with the existing firmware

7.14 Troubleshooting Guide

Cannot connect to WBM

- verify PC address and subnet
- verify https://192.168.1.10 or the configured target address
- check that 443/TCP is not blocked by the firewall
- verify power supply and PS LED status

Firmware update appears unsuccessful

- verify the firmware version in 'Device' → 'General Data'
- repeat the update if the displayed version did not change
- perform the same update a second time so both boot partitions are aligned

Network misconfiguration

- reconnect through a known-good commissioning setup
- use the configured fallback engineering method, such as Festo Automation Suite, to rediscover or readdress the controller
- if necessary, use reset type 1 to restore the default IP settings

Additional WBM Diagnostics

Always record the original symptom, LED state, and the last configuration change before starting corrective action, see ➔ 8.6.5 Example Notifications Filter and Download.

8 Web-based Management

8.1 Establishing a connection to WBM

Each Festo AX Controls device features a Web-based Management (WBM). In the WBM, you can access static and dynamic controller information and modify certain controller settings. You can call WBM via Ethernet interface of the controller. The WBM systems all have the same structure and are generally described in the following.

Initial access: Connecting

To establish a connection to WBM on the device, proceed as follows:

1. Connect the device to your PC via one of the devices' Ethernet interfaces (assuming that the https port 443 has not been blocked by a firewall)
2. Make sure your PC and the device are in the same network.
3. Open a web browser on your PC.
4. In the address field, enter the URL `https://ip.address.of.interface`, see the default setting for your device in the respective → 3.3 Hardware documentation.
The default setting for CEPE is `https://192.168.1.10`, subnet mask `255.255.255.0`.
5. Enter the user name and the password. Notes for Login → 8.2 Login to Web-based Management.

Initial access: TLS certificate

For secure communication, the controller's web server uses a self-signed TLS certificate automatically generated by the controller. Before the controller's web server can be accessed, you must authorize the TLS certificate in your web browser.



Note:

- The controller generates the TLS certificate during the boot phase.
- The certificate is used for all Ethernet interfaces of the controller.
- The certificate is regenerated after the controller is reset to factory settings.
- Consider that self signed certificate has security constraints.
The browser might warn about unsecure connection to self signed certificate, this can be replaced by the user own certificate chain.



Note:

Certificate directory settings: On the WBM 'Certificate management' page you can either select to use an existing `IdentityStore` or to use self-signed certificates.

- When using an existing `IdentityStore` the symbolic links are changed and refer now to the specified `IdentityStore`.
- When using self-signed certificates a self-signed certificate is generated at `/opt/plcnext/Security/IdentityStore/HTTPS-self-signed/*.*` and the symbolic links refer to that `IdentityStore`.

8.2 Login to Web-based Management

The WBM login page is displayed if you're accessing the WBM for the first time on this controller.

Initial access as an administrator

When you access WBM for the **first time**, log in as the administrator.

- Enter the user name ‘admin’ in the ‘Username’ input field.
- Enter the administrator password in the ‘Password’ input field.

The default administrator password is printed on the controller. For more information, refer to the ➔ 3.3 Hardware documentation

- To open the WBM, click on the ‘Login’ button.

The WBM start page opens.

Highly recommended:

- Use the administrator password for initial login only.
- Once you have logged in successfully, change the administrator password to prevent unauthorized administrator access ➔ 8.8.4 User management.



Note: After changing the access data for the administrator, it is no longer possible to log in with the administrator password printed on the controller. The password printed on the controller is valid again after resetting the controller to default settings.

Logging in as a user

Log in using your user credentials:

1. Enter your user name in the ‘Username’ input field.
2. Enter your password in the ‘Password’ input field. The password can be obscured (not displayed as plain text).
3. To open WBM, click on the ‘Login’ button.
⇒ The WBM start page opens.

Password expiration notification

When the user password is about to expire, a note is displayed in the header after logging into the WBM.

For further information on how to set an expiration date for a password, refer to Password policy ➔ 8.8.5 User policies.

Session timeout notification

Two minutes before the current WBM session expires, a corresponding note is displayed in the header.

- If you want to extend the current session, click the ‘Prolong session’ button.

For further information on how to set the maximum session time, refer to ➔ 8.8.5 User policies.

8.3 Start page – areas and functions**Changing the user interface language**

You can change the language for the WBM user interface in the top right of the web browser window.

- Click the ‘Deutsch’ or ‘English’ link to choose the language.

The WBM user interface then immediately switches to the chosen language.

Navigation panel

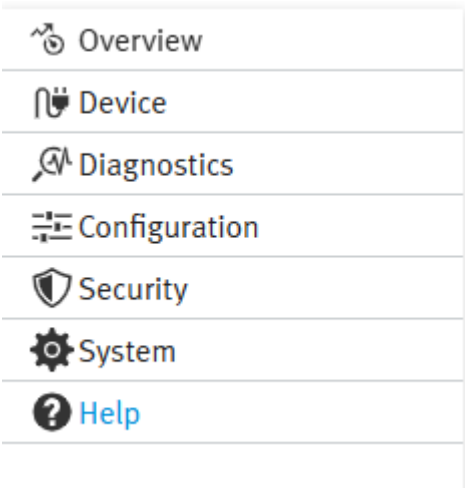


Fig. 4: Navigation panel

The WBM is split into the following main areas:

- Overview
- Device
- Diagnostics
- Configuration
- Security
- System
- Help

Device information

On the top of each page, you will find general details about the device, e.g., hardware and firmware versions, the order number as well as the Product Key.

8.4 Overview

The ‘Overview’ page provides status and diagnostic indicators and further system information.

Date and Time

Display of the system time and the system uptime. Use the service access via SSH to set the system time.

Utilization

CPU load and memory utilization overview.
Memory usage and PLC state overview.

Device health

Display of the current board temperature. For information on the permissible temperature ranges, refer to the operating manual of your controller.

8.5 Device

General Data

On the ‘General Data’ page, you will find general details about the device, e.g., hardware and firmware versions, the order number, as well as manufacturer details.

8.6 Diagnostics

8.6.1 Log Download

With the button ‘Download’ on the ‘Diagnostics’ page, a log file is generated and can be saved.



8.6.2 Notifications page

On the Notifications page, you can read and download notification logs. Any user with access rights to the WBM can view and download the information on the page.

The page consists of notification filter options, buttons for applying filters and exporting notifications in CSV format as well as an overview table of all notifications and a full text display for selected notifications.

8.6.3 Notifications filter

You can filter notifications according to the following criteria.

To activate the filter settings, click on the 'Apply Filter' button. The notifications table is then updated accordingly.

Archive name

You can filter notifications by their archive name. You have the following setting options:

- All: To receive notifications from every archive
- Archive name: To receive notifications of a specific archive (The archives default and security are available by default)

Severity

You can filter notifications by their severity level. Higher levels are included when filtered by a lower level, meaning:

- Filtering on Default (or Internal) displays all notifications because all other security levels are higher.
- Filtering on Information displays notifications from severity levels
 - Information
 - Warning
 - Error
 - Critical
 - Fatal
- Filtering on Warning displays notifications from severity levels
 - Warning
 - Error
 - Critical
 - Fatal
- Filtering on Error displays notifications from severity levels
 - Error
 - Critical
 - Fatal

- Filtering on Critical displays notifications from severity levels
 - Critical
 - Fatal
- Filtering on Fatal displays notifications only from severity level Fatal because all other security levels are lower.

Sender

You can filter notifications by their sender name.

Note: The notifications selected by the filter form the basis for the Sender drop down menu. At least the filter Maximum number of notifications is always activated. Only the sender names of the notifications listed in the table are displayed in the 'Sender' drop down menu.

You have the following options:

- Select a sender name from the drop down menu. The listed sender names correspond to the names in the notifications table.
 - Enter a sender name or part of a sender name in the input field. Use this option if the sender name has not yet been listed in the notifications table.
- Filtering displays notifications from senders that match or partially match the search term you entered.

Maximum number of notifications

Enter the maximum number of notifications to be displayed.

The maximum number must not exceed 4000 (Default setting = 1024).

Time from and Time to

You can limit the time period for which notifications are displayed by filling in the input fields 'Time from' and 'Time to':

- 'Time from': Notifications that are not older than the specified time or date are displayed.
- 'Time to': Notifications that are not more recent than the specified time or date are displayed.

The entry of the date is mandatory and may be supplemented by a time.

8.6.4 Notifications table**Severity levels**

The severity of each notification is displayed by icons, meaning:

-  Internal
-  Information
-  Warning
-  Error
-  Critical
-  Fatal

Sort criteria for notifications table

By default, the notifications in the notifications table are sorted in descending order based on the time stamp. You have the option of using the individual columns of the notifications table as sort criteria.

To sort the notifications, click on the header of the corresponding table column:

- 'Severity' or 'Time' (timestamps) are sorted in ascending/descending order.
- 'Sender' (sender names) or Name (notification names) are alphabetically sorted in ascending/descending order.

The arrows at the column headers have the following meaning:

- Double arrow: The table is not sorted by this column.
- One arrow pointing up: The table is sorted by this column in ascending order.
- One arrow down: The table is sorted by this column in descending order.

CSV file download

The listed notifications can be exported in CSV format.

- Click on the 'Export CSV' button. and select a location for the CSV file.

Example see ➔ 8.6.5 Example Notifications Filter and Download

Payload display

The text field displays the full text/payload of a selected notification from the notification table. The text field is empty if no notification is selected.

Update of the notifications table

While a connection is established, the notification table is updated every second.

8.6.5 Example Notifications Filter and Download

The notifications page allows filtering and downloading diagnostic messages:

- 1. Go to ‘Diagnostics’ → ‘Notifications’.
- 2. Apply the desired filters.
Available filter options:
 - Archive name: select active or archived notifications
 - Severity: filter by severity level (Info, Warning, Error, Critical)
 - Sender: filter by the component that generated the notification
 - Time range: display only messages within a specific time window
- 3. Click on ‘Export CSV File’ to export the filtered notifications as a CSV file.

Filter

Severity >= Internal

Archive name external

Sender

Maximum number of notifications 1024

Time from mm / dd / yyyy

Time to mm / dd / yyyy

Reset Filter

Apply Filter

Notifications

Severity	Time	Sender	Name	Notification
Info	2025-05-29 18:48:24	BuiltInDeviceSelfTest	External.BuiltInDeviceSelfTest.INFO	Starting SBIST (Startup Built-in Self Test)
Info	2025-05-29 18:48:24	BuiltInDeviceSelfTest	External.BuiltInDeviceSelfTest.INFO	Starting SBIST (Startup Built-in Self Test)
Warning	2021-01-03 23:16:02	BuiltInDeviceSelfTest	External.BuiltInDeviceSelfTest.WARNING	FAN control in state WARNING, system/subsystem temperature above 89°C! Temperature: 90°C
Error	2021-01-03 23:15:57	BuiltInDeviceSelfTest	External.BuiltInDeviceSelfTest.ERROR	FAN control severe error! state is fan_error, fan control data: (temperatures: (zynq_temperature: 89, main_board_temperatures: (cpu: 45.0, pcb: 40.0)), fan_c...
Warning	2021-01-03 23:15:42	BuiltInDeviceSelfTest	External.BuiltInDeviceSelfTest.WARNING	FAN control in state WARNING, system/subsystem temperature above 89°C! Temperature: 90°C
Error	2021-01-03 22:14:27	BuiltInDeviceSelfTest	External.BuiltInDeviceSelfTest.ERROR	FAN control severe error! state is fan_error, fan control data: (temperatures: (zynq_temperature: 89, main_board_temperatures: (cpu: 55.8, pcb: 46.0)), fan_c...
Warning	2021-01-03 22:14:17	BuiltInDeviceSelfTest	External.BuiltInDeviceSelfTest.WARNING	FAN control in state WARNING, system/subsystem temperature above 89°C! Temperature: 90°C
Error	2021-01-03 22:14:12	BuiltInDeviceSelfTest	External.BuiltInDeviceSelfTest.ERROR	FAN control severe error! state is fan_error, fan control data: (temperatures: (zynq_temperature: 89, main_board_temperatures: (cpu: 51.2, pcb: 46.0)), fan_c...
Warning	2021-01-03 22:14:07	BuiltInDeviceSelfTest	External.BuiltInDeviceSelfTest.WARNING	FAN control in state WARNING, system/subsystem temperature above 89°C! Temperature: 90°C

No notification selected

Export CSV File

8.7 Configuration

In this section of the Web-based Management, the following pages can be included:

- ➔ 8.7.3 Network
- ➔ 8.7.1 Date & Time
- ➔ 8.7.2 Web services
- ➔ 8.7.4 PLCnext Store

8.7.1 Date & Time

Status

Shows the current system time in UTC.
The system clock can either be synchronized with an NTP server or set manually.

NTP client configuration

You can add, remove or edit existing NTP server entries for the device to syn-
chronize to. When adding or editing an entry, hover over the information icon for
an explanation what each option does.

In the WBM, multiple NTP servers can be added, their minimum and maximum polling times configured and they can be set to active or inactive. Chrony is used as NTP service on the device. NTP servers that are set to active in the WBM are added to the Chrony configuration file `/etc/chrony.conf`. The chronyd daemon takes over the synchronization of the system clock and the hwclock to the NTP server time.

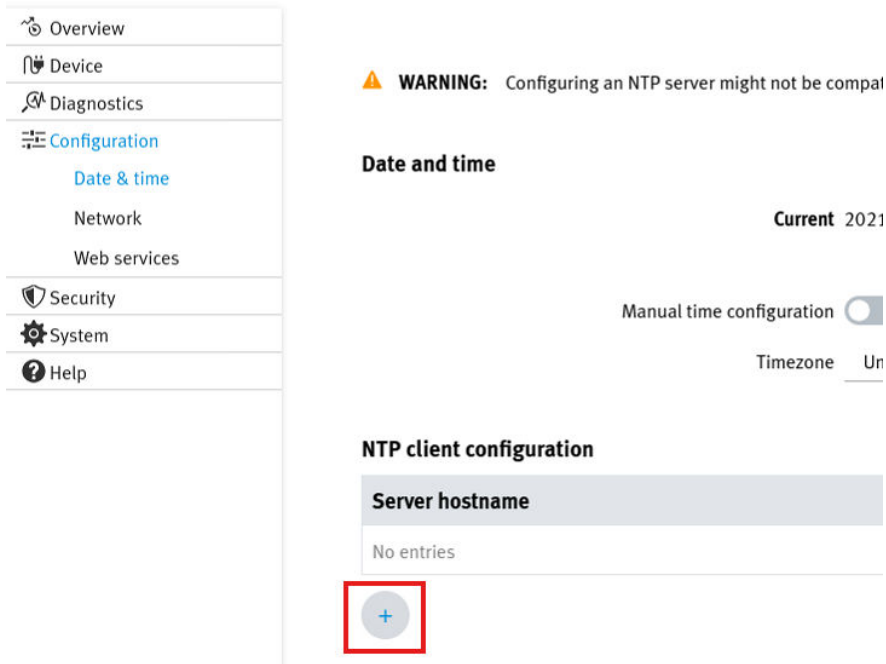
NOTICE

Configuring an NTP server might not be compatible to industrial ethernet usage.

Centralized security logging only makes sense if all devices have a synchronized time. NTP is already supported today. TimeServer provides all devices with the same time base. For each device you have to configure which time server it should use.

Adding a NTP server entry

- 1. Log in to the WBM.
- 2. Open the 'Configuration' → 'Date & Time page'.



3. To add a new NTP server entry, click the '+' button.
⇒ A new window opens.

Adding an NTP server entry



Server configuration

Server hostname This field is required.

Status

MinPoll

MaxPoll

PollTarget

Use iBurst function ☐

Cancel

Add

4. Provide the following information:
 - Server hostname: IP address of the NTP server
 - Status: Active
 - Min. polling time: The shortest interval at which the NTP client retrieves the current time from the NTP server.
 - Max. polling time: The longest interval at which the NTP client retrieves the current time from the NTP server.
 - **Note:** The relationship between the minimum and maximum polling time is that together they determine the frequency of the time queries. The NTP client dynamically adjusts the polling intervals within these limits based on the stability and accuracy of the time source and the network conditions.



Note: Make sure that the firewall basic configurations and the input rules on the Firewall page ('Security' → 'Firewall') in the WBM are correct.

Basic Configuration:

English admin

Festo AX Controls
CEPE-H8GB-128GB-M1
Firmware version: 26.4.0.4-alpha Part number: 8165401
Product key: Hardware version: 0
Connected

The firewall configuration was saved.

Overview
Device
Diagnostics
Configuration
Date & time
Network
Web services
Security
User management
User policies
LDAP configuration
Certificate management
Syslog
Firewall

General **Basic Configuration** IP Input Rules IP Output Rules

ICMP configuration

Allow incoming ICMP requests ☒
Allow outgoing ICMP requests ☒

Basic rules

Seq.	Direction	Protocol	To port	Comment	Action
1	Input	Udp	123	NTP (Network Time Protocol)	Continue
2	Input	Tcp	41100	Remoting (e.g. PLCnext Engineer)	Accept

Input Rules:

Overview
Device
Diagnostics
Configuration
Date & time
Network
Web services
Security
User management
User policies
LDAP configuration
Certificate management
Syslog
Firewall
System

General **Basic Configuration** **IP Input Rules** IP Output Rules

Seq.	Interface	Protocol	From IP	From port	To IP	To port	Comment	Action
1	ETH	Udp	0.0.0.0	any	0.0.0.0	123		Accept

There are some parameters to be set, e.g. what deviation from the time is acceptable, the maximum unavailability, etc.

Manual Settings

If NTP is not available, the system time can be set manually via WBM:

1. Open 'Configuration' → 'Date & Time'.
2. Select 'Manual time' configuration
3. Ensure NTP is inactive (no active NTP servers configured).
4. Enter the desired date and time.
5. Click 'APPLY'.

Device
Diagnostics
Configuration
Date & time
Network
Web services
Security
User management
User policies
LDAP configuration
Certificate management
Syslog
Firewall
System
Device maintenance
System services
Backup & restore
License management

WARNING: Configuring an NTP server might not be compatible to industrial ethernet usage.

Date and time

Current 2021-01-01 03:25:04

Manual time configuration ☒

WARNING: If an NTP client is active then manual settings will be overridden.

Date and time: 01 / 01 / 2026 12:00:01

Timezone: Universal (UTC +00:00)

NTP client configuration

Server hostname	Status
No entries	

REVERT PAGE **SAVE & APPLY PAGE**

8.7.2 Web services

The Web Services page provides access to the configuration of Web Services, e.g. HTTPS certificate used for nginx web server.

On the WBM 'Certificate Management' page you can either select to use an existing IdentityStore or to use self-signed certificates.

- When using an existing IdentityStore the symbolic links are changed and refer now to the specified IdentityStore.
- When using self-signed certificates a self-signed certificate is generated at `/opt/plcnext/Security/IdentityStore/HTTPS-self-signed/*.*` and the symbolic links refer to that IdentityStore.
- When creating a self-signed certificate via the 'Certificate Management' WBM page, the `/opt/plcnext/Security/IdentityStores/HTTPS-self-signed-Backup` directory is not modified.

nginx web server

You can either select an HTTPS certificate of an Identity Store from the selection field or let the controller create a self-signed certificate by choosing 'HTTPS-self-signed'.

NOTICE

Applying the configuration may affect the real-time behavior of the system. Operated stations may show a delay which can cause crashes.

- Avoid reconfiguring the Web Services during productive operation.

TLS configuration

Perform TLS configuration using the following options:

- Check TLSv1.3 and/or TLSv1.2 to be used for nginx configuration.
- Select a predefined cipher suite to be used for nginx configuration.
- Click 'SAVE & APPLY PAGE' in the lower-right corner of the screen to activate the configuration on the controller.



Security note:

- If you cannot set TLS version TLSv1.3, set TLS Version TLSv1.2.
- If you set TLS version TLSv1.2, you must set Secure HTTPS TLS Ciphers as the cipher suite.
- If the target browsers your audience will use does not support the secure cipher suite, set the Default HTTPS TLS Ciphers, but be aware that this is not considered a secure approach.

HTTPS certificate

The HTTPS certificate is used by the PLCnext web server to authenticate the controller towards the browser.

In the configuration table for the nginx web server you have the possibility to select the HTTPS certificate from one of the Identity Stores stored on the controller.

- Select an Identity Store in the selection field. The corresponding HTTPS certificate is applied.
- To apply the configuration to the system, click 'SAVE & APPLY PAGE'.

Self-signed HTTPS certificate

The current configuration of the self-signed HTTPS certificate is shown in the following table. You can adjust this configuration and regenerate the certificate to apply the changes in the configuration. The following configuration options are available:

Distinguished Name (Dn)

You can configure the following DN attributes:

- Common Name (CN)
- Organization (O)
- Organizational Unit (OU)
- Location (L)
- State or Province Name (ST)
- Country Name (C)

Validity

- Valid not before: Date in format DD.MM.YYYY - hh:mm:ss (if the input field remains empty, the current date of the controller is used)
- Valid not after: Date in format DD.MM.YYYY - hh:mm:ss (if the input field remains empty the date point 31.12.9999 - 23:59:59 is used)

Subject Alternative Names

The IP addresses from the network configuration of the controller are suggested by default. You have the possibility to extend or adjust them.

- Subject Alternative Name: Enter an IP address or DNS name (depending on the setting in the Typefield)
- Type: Select the type of the subject alternative name from the drop-down list. Below and in the table you will find the buttons to add and remove subject alternative names.

If the web server is to be accessible via different IP addresses of the interfaces without error message, all IP addresses must be entered as Subject Alternative Name of type IP address (e.g. for controllers with more than one Ethernet adapter). If the controller is also accessible via DNS names, these must also be entered.

8.7.3 Network

LAN Interfaces tab

For the Ethernet interface on the controller, this page lists the following information:

- Naming of a LAN interface in the form "TCP/IP (LAN <n>)"
 - IP Address
 - Subnet Mask
 - Default Gateway
 - DNS Server Addresses
 - MAC Address
- Naming of 1st physical port
- Data Rate – can be 10 or 100 or 1000 Mbit/s (on LinkUp when link is active only)
- Duplex Mode – can be Full Duplex or Half Duplex (on LinkUp when link is active only)
- Link Status – can be LinkUp (a connection to another Ethernet device is established) or LinkDown (No connection to another Ethernet device is established)
- and so on...

8.7.4 PLCnext Store

PLCnext Store page

The PLCnext Store page can be activated on the page ➔ 8.9.5 System services. The PLCnext Store page provides status information on the connection between the controller and the PLCnext Store.

You can also specify if you want to operate the controller with or without PLCnext Store connection.



For the Festo AX Controls devices there are selected apps from PHOENIX CONTACT available.

Enabling the PLCnext Store connection



For security reasons, we recommend disabling the PLCnext Store Connector service when the controller is in productive operation. See → 8.9.5 System services.

If you want to operate the controller with PLCnext Store connection, you have to enable the PLCnext Store service of the controller. When the PLCnext Store service of the controller is enabled, the controller tries to establish a connection to the PLCnext Store.

1. Enable the 'Enable PLCnext Store Service' checkbox.
2. Click on the 'Apply' button.
 - ⇒ The PLCnext Store connection for the controller is enabled. Now you can specify which service you want to use.

Disabling the PLCnext Store connection

If you want to operate the controller without PLCnext Store connection, you have to disable the PLCnext Store service of the controller. In this case, it is not technically possible to establish a connection between the controller and PLCnext Store.

1. Disable the Enable PLCnext StoreService checkbox.
2. Click on the 'Apply' button.
 - ⇒ The PLCnext Store connection of the controller is disabled.

8.8 Security

8.8.1 Security Note



For developing secure-by-design, IEC 62443-2 compliant applications with PLCnext Technology, get a good grasp of the concepts used in the Security context.

8.8.2 Certificate management

The 'Certificate management' page is used to manage certificates for secure controller communication. You need some background knowledge on the terms that are used in this context and the data to provide with the certificate.

General management of stores

Trusted certificates and revocation lists of possible communication partners are displayed on the 'TRUST STORES' tab.

Your own certificates are displayed on the 'IDENTITY STORES' tab.

The sections are ordered alphabetically by their names.

Naming of stores

Use only the following characters when naming 'TRUST STORES' and 'IDENTITY STORES':

- letters [a - z][A - Z]
- numbers [0 - 9]
- hyphen [-]
- underscore [_]

They can be used with the interfaces for TLS communication, e.g., TLS_SOCKET block in IEC 61131-3, or TlsSocket class in C++ or C#.



Note: The naming is case-sensitive!

Location of stores

On this WBM page you can either select to use an existing Identity Store or to use self-signed certificates.

- When selecting to use an existing Identity Store the symbolic links are changed and refer now to the specified Identity Store.
- When selecting to use self-signed certificates then a self-signed certificate is generated at `/opt/plcnext/Security/IdentityStore/HTTPS-self-signed/*.*`, and then the symbolic links refer to that Identity Store.

The `/opt/plcnext/Security/IdentityStores/HTTPS-self-signedBackup` directory is not modified.



Note:

- The controller generates the TLS certificate during the boot phase. That certificate is used with all physical Ethernet interfaces of the controller, but not with all IP addresses unless they have been specified.
- For a secure access via a web browser to the Web-based Management or to a PLCnext Engineer HMI application on the device, that specific IP address set up for the controller must be authorized. The certificate is then regenerated when the controller is reset.

Trust Stores



A certificate to add to a Trust Store consists of the certificate itself, and optionally a certificate revocation list (CRL) that is checked for evaluation. Therefore, each Trust Store has a complete set of folders.

- `/opt/plcnext/Security/TrustStores/<name>/trusted`
 - The directory contains CA certificates that are trusted.
- `/opt/plcnext/Security/TrustStores/<name>/trusted/crl`
 - The directory contains files with CRLs for the CA certificates.
- `/opt/plcnext/Security/TrustStores/<name>/issuers`
 - The directory contains CA certificates that are not automatically trusted but that are necessary for creating a certificate chain.
- `/opt/plcnext/Security/TrustStores/<name>/issuers/crl`
 - The directory contains files with CRLs for issuer certificates.

By default, these entries are already set up as Trust Stores in a 'Festo AX Controls' device:

- Code Signing
- Empty (reserved for internal processes; therefore this entry cannot be edited or deleted via the WBM)
- Festo Device Root
- OPC UA-configurable

- PLCnext Store
- PLCnext Store Developer

These are the steps to manage Trust Stores:

- Check if the default stores suit your purpose; if necessary,  add,  remove, or  edit a Trust Store.

These are the steps to provide certificates and/or certificate revocation lists (CRLs):

- Click the  button to open the regarding Trust Store section; there you can add , remove , or  view a certificate and/or CRL.
- To  add a certificate and/or CRL, choose the type in the dialog box:

You can either upload a certificate as a .pem file (Base64 format), or paste the content of the certificate as a text string in PEM Base64 format.

Identity Stores

Trust Stores

Identity Stores

IDevID

Element	Type	Description	Validity
	Key Pair	RSA 4096	RSA Key Pair
	Certificate	Key Certificate	Common Name: Festo AX CEPE IDevID Sub-CA01 Valid from: 2025-04-25 08:10:15 Valid until: 9999-12-31 23:59:59
	Certificate	Issuer Certificate	Common Name: Festo AX Device Root-CA01 Valid from: 2025-04-25:08:10:15 Valid until: 9999-12-31:23:59:59

HTTPS-self-signed

Element	Type	Description	Validity
	Key Pair	RSA 2048	RSA Key Pair
	Certificate	Key Certificate	Common Name: Festo HTTPS Interface List Valid from: 2024-06-18 11:57:11 Valid until: 9999-12-31 23:59:59

On the 'IDENTITY STORES' tab, you can create and manage different Identity Stores.

By default, these entries are set up as 'IDENTITY STORES':

- 'IDevID' (reserved for internal processes; therefore this entry cannot be edited or deleted via the WBM)
- 'HTTPS-self-signed'
- 'OPC UA-self-signed'

Each Identity Store usually contains an RSA key pair and the corresponding key certificate. As an option, you can add further issuer certificates to an Identity Store. The 'IDevID' and 'OPC UA-self-signed' Identity Stores are part of the system and supplied with the controller.

These are the steps to manage Identity Stores:

- Check if the default stores suit your purpose; if necessary,  add,  remove, or  edit an identity Store.

These are the steps to provide certificates and/or key pairs:

- Click the  button to open the regarding identity Store section; there you can  view,  download, or  edit a certificate and/or key pair.
- To  edit a  **Certificate** in the dialog box, choose the source in the dialog box:
 - If you choose to enter a certificate, you can either upload it as a **.pem** file (Base64 format), or paste the content of the certificate as a text string in PEM Base64 format.
 - If you choose to generate a certificate signing request (CSR), you are downloading the generated file to request an X.509 certificate from a certificate authority (CA).
- To  edit a  **Key Pair** in the dialog box, choose the source in the dialog box: You can either upload a key pair as text or file, or choose a suitable encryption method to generate a new key pair, that is added to that Identity Store.

Downloading public keys or key certificates

You can download the content of the public key of a key pair as a **.pem** file that is to be used on the corresponding Trust Store of a communication partner:

- If a key pair is available, you can download it as a **.csr** file.
- If a key certificate is available, you can download it as a **.crt** file.

8.8.3 Firewall

PLCnext Technology relies on the proven and commonly used Linux firewall **nftables**. On the device, you don't need to configure the firewall rules via cryptic shell commands. Just choose from the predefined basic rules, or add your own rules to the set.

For an Example see ➔ 8.8.3.1 Example Extended Firewall settings

General

By default, the firewall is activated.

- Check and adapt the predefined rules in the ‘Basic configuration’ tab.
- When deactivated, activate the firewall at the toggle switch, then click ‘SAVE & APPLY PAGE’.
- ➔ The firewall becomes Activated.

Only if the firewall is active, you can generate an overview of all enabled firewall rules and save it in a ***.txt** file.

- Click on ‘Show Rules’
- ➔ The ***.txt** file with the activated firewall rules is being generated and opens in a dialog box.
- To save the active rules to a ***.txt** file, click ‘Save to file’ in the dialog box.
- ➔ The ***.txt** file is saved to your specified ‘Download’ folder on the host computer.

Basic configuration

The Basic Configuration tab provides predefined firewall rules. You can specify or add your own firewall rules on the ‘IP Input Rules’ or ‘IP Output Rules’ tabs.

ICMP configuration

In the ‘ICMP configurations’ section at the top, you specify how incoming and outgoing ICMP echo requests are to be treated. By default, incoming and outgoing ping commands are allowed. This is necessary for testing rules.

Basic rules

In the ‘Basic Rules’ section, you can specify firewall rules for different incoming connections, which you can enable or disable in the ‘Action’ column. The configuration baseline is stored in the **/etc/nftables/plcnext-filter** file in the controller file system.

Options for activating and deactivating these rules for specific connections can be done via the 'Action' column:

Option	Description
Accept	Connection requests are accepted. A connection can be established.
Drop	Connection requests are not responded. The packet is dropped. After saving this setting, established connections are dropped.
Reject	Connection requests are rejected. The sender receives a response via the rejected connection.
Continue	The rule is not executed. Choose this option to skip the basic configuration and use a user-specific rule for the port instead.

Tab. 37

To change a basic rule, proceed as follows:

- In the 'Basic configuration' tab, set a basic rule to 'Continue' in the 'Action' column. This way, this rule is skipped.
- Create and configure a new rule in the 'IP Input Rules' tab.
Example: You can specify incoming SSH connection requests via TCP port 22 in more detail by excluding certain IP addresses or exclusively establishing access of some IP addresses.
- To make sure that all newly applied rules are actively used (even for already established connections!), click 'SAVE & APPLY PAGE'.



Note: If you select the 'Reject' or 'Drop' action for HTTPS with activated firewall by clicking 'SAVE & APPLY PAGE', then you can then no longer change back the firewall rules via the WBM.

- To stop the firewall in this case, you have to reset the controller to the default settings.

For more detailed information, please refer to the user manual for your controller.

Note that during a reset to the default settings, user-specific data (applications, configuration, etc.) is deleted.

Once the firewall is deactivated, you can again access the WBM.

User Configuration

In addition or as an alternative to the basic rules, you can define and activate your own, user-specific firewall rules for different filter categories in the tabs 'IP Input Rules' and 'IP Output Rules'. Below and in the table you will find the buttons to add, remove, or edit rules.

The following parameters are to be defined:

Column	Description
Interface (Input Rules only)	You can configure Input Rules specifically for an interface. From the drop-down list, select the desired Ethernet interface to which the filter rule is to be applied. The Output Rules apply to all interfaces.
Protocol	From the drop-down list, select the TCP, UDP, UDPLITE protocol or all of them.
From IP	In the From IP field, enter an IP address, if applicable. You can specify all IP addresses, a single IP address or a range. An IP address range is specified with a - without spaces between the IP addresses. Example: 192.168.1.10-192.168.1.20 If you leave the field empty (0.0.0.0), all IP addresses are selected.

Column	Description
From Port	In the From Port field, enter the corresponding ports, if applicable. The rule applies to connections coming in from this address. You can specify all ports, single ports, or a value range. A port range is specified with a - without spaces between the port numbers. Example: 22-30 If you leave the field empty (any), all ports are selected.
To IP	In the To IP field, enter an IP address, if applicable. You can specify all IP addresses, a single IP address or a range. An IP address range is specified with a - without spaces between the IP addresses. Example: 192.168.1.10-192.168.1.20 If you leave the field empty (0.0.0.0), all IP addresses are selected.
To Port	In the To Port field, enter the corresponding ports, if applicable. The rule applies to connections going out to this address. You can specify all ports, single ports, or a value range. A port range is specified with a - without spaces between the port numbers. Example: 22-30 If you leave the field empty (any), all ports are selected.
Comment	Here, enter a description of the filter rule.
Action	The options described in Action column can be used as actions for the filter rules.

Tab. 38

To activate the settings you configured and transmit them to the system, click on the 'SAVE & APPLY PAGE' button. If a configuration is already present on the system, it is overwritten during this process.

To drop the new configuration and call the basic settings, click on the 'REVERT PAGE' button.

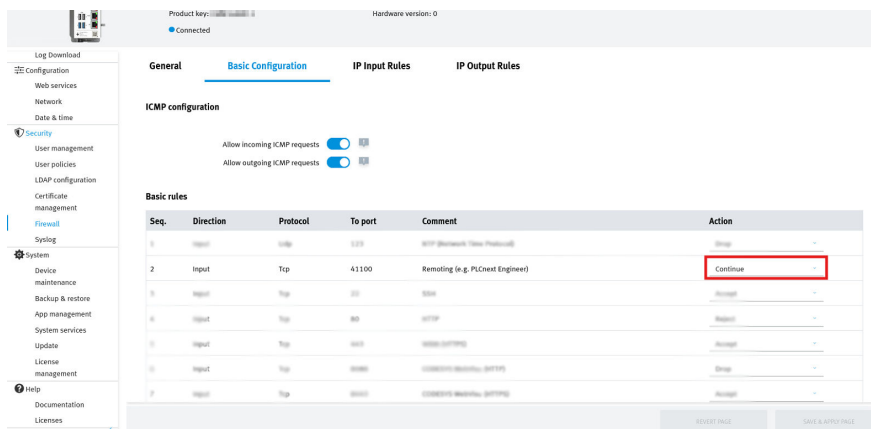
8.8.3.1 Example Extended Firewall settings

Below are examples of how to make the firewall settings on your device.

Adapting The Basic Rules To Your Own Rules

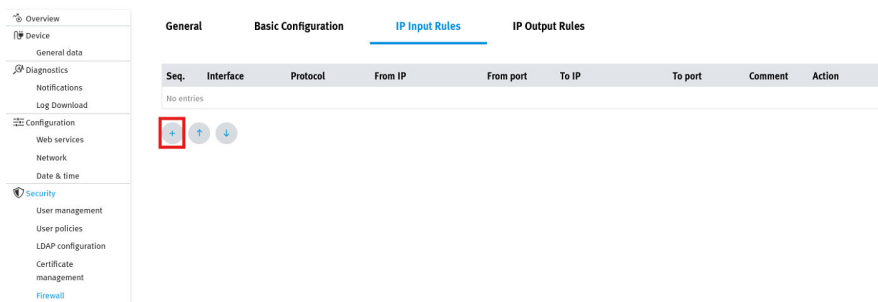
To configure access according to the security context, proceed as follows:

1. Log in to the WBM.
2. Open the page 'Security' → 'Firewall' in the WBM.
3. Open the 'BASIC CONFIGURATION' tab.
4. In the 'Basic Rules' section, select 'Continue' from the drop-down list for 'Remoting' in the 'Action' column.



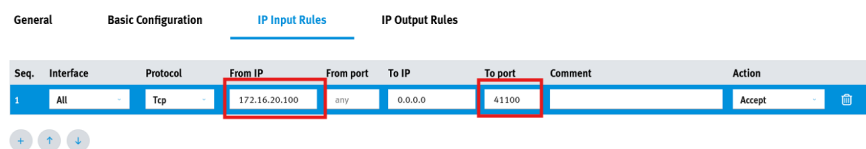
5. Click the 'SAVE & APPLY PAGE' button.
6. Open the 'IP INPUT RULES' tab.

7. Add a new rule via the '+' button.



8. Provide the following information:

- Select the interface via which the controller is connected to the engineering station in the manufacturing zone.
- Enter the corresponding IP address of the engineering station in the superordinate network.
- Enter the target port. Refer to ➔ 7.7.8 Configuring basic firewall settings



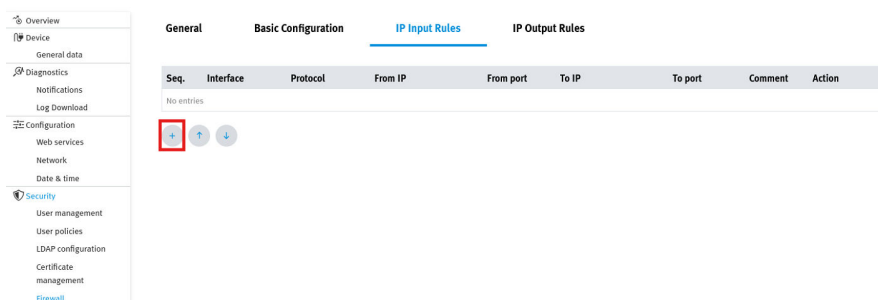
9. Click the 'SAVE & APPLY PAGE' button.

10. Reboot your device.

⇒ Now you have access from the superordinate network.

Inserting Your Own Firewall Rules

1. Log in to the WBM.
2. Open the 'Security' → 'Firewall' page in the WBM.
3. Open the 'IP INPUT RULES' tab.
4. Add a new rule via the '+' button.



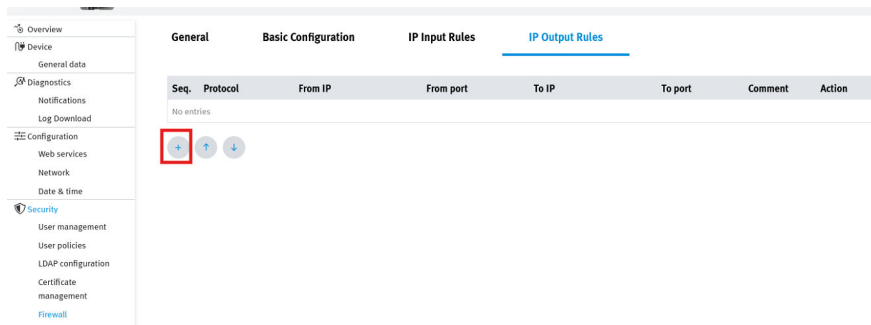
5. Provide all necessary information depending on your individual security context:

- Select the interface.
- Enter the target ports.
- Select 'Accept' in the 'Action' column.

6. Click the 'SAVE & APPLY PAGE' button.

7. Open the 'IP OUTPUT RULES' tab.

8. Add a new rule via the '+' button.



9. Provide all necessary information depending on your individual security context:
 - Select the interface.
 - Enter the target ports.
 - Select 'Accept' in the 'Action' column.
10. Click the 'SAVE & APPLY PAGE' button.

Plant Documentation

If you want to use the list of active firewall rules in your plant documentation, you can export the list from the WBM. Proceed as follows.

Firewall Status Section

If the firewall is activated, you can generate an overview of all active firewall rules in a *.txt file.

1. Open the 'Security' → Firewall page in the WBM.
2. Open the 'GENERAL' tab.
3. In the Firewall status section, click the 'SHOW RULES' button.
 - ⇒ The *.txt file with the active firewall rules is being generated and opens in a dialog box.
4. To save the active rules to a *.txt file, click the 'SAVE TO FILE' button in the dialog box.
 - ⇒ The *.txt file is saved to the directory selected in the next step.

For the initial firewall setup during commissioning, see ➔ 7.7.8 Configuring basic firewall settings .

8.8.4 User management

By default, on a Festo AX Controls device only a single user is configured and assigned to the 'Admin' user role.

Of course, other users and user roles need to be assigned, once the controller is put into production, which is done by means of the User management WBM page. The procedure is designed to be mostly selfexplanatory: By clicking the '+' icon, you'll be led through a step-by-step configuration.

The CEPE uses role-based access control. User Management provides authentication and authorization on each communication interface. Only authorized users can access (read/write) data via a communication interface.

Role Categories

The platform provides roles in the following categories:

- **Security roles:** 'SecurityEngineer', 'SecurityAuditor', 'UserManager', 'Certificate-Manager'
- **General roles:** 'Admin', 'Engineer', 'Commissioner', 'Service', 'DataViewer', 'DataChanger', 'Viewer'

Recommended Role Model

Role	Purpose	Typical Access
'Admin'	Initial configuration, emergency service tasks, selected maintenance. May have SSH-capable access during commissioning.	Full system configuration. Do not use as an everyday production account.
'SecurityEngineer' + 'UserManager'	Configures certificates, firewall, security settings, syslog, user management, and security policies.	'Security' → all pages, 'System' → 'Update'
'SecurityAuditor'	Reviews security notifications, audit trails, and security-relevant configuration evidence.	'Diagnostics' → 'Notifications' (read-oriented)
'Engineer'	Manages controller applications, app-related tasks, and normal engineering activities.	Application pages, 'System' → 'System Services'

Tab. 39

User roles

The following table defines the permissions associated with each user role for access to WBM pages.

The table shows the access permissions for the following roles:

- 'Admin'
- 'SecurityEngineer'
- 'SecurityAuditor'
- 'CertificateManager'
- 'UserManager'
- 'Engineer'
- 'Commissioner'
- 'Service'
- 'DataViewer'
- 'DateChanger'
- 'Viewer'

Note: Visibility of WBM pages depends on the device and firmware release in use. In addition, some WBM pages could have been deactivated by settings in the System Services WBM page.

WBM pages/Features			User role										
			Admin	SecurityEngineer	SecurityAuditor	CertificateManager	UserManager	Engineer	Commissioner	Service	DataViewer	DateChanger	Viewer
Overview			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Device section - General Data			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Diagnostics section - Notifications						✓	✓	✓					✓
Configuration section	Network (r) read-only access (r/s) read access and reset statistics	IP configuration	✓	✓	(r/s)		(r/s)	(r/s)	(r/s)	(r/s)			
		Network - Netload limiter	✓	✓	(r/s)				(r)	(r)			
	Date and Time		✓	✓									
	PLCnext Store		✓	✓									
	Web Services		✓	✓									
Security section	Firewall		✓	✓									
Legend: ✓ = full access, (r) = read-only access, (r/s) = read access and reset statistics, (c) = can only change the user password, (nr) = cannot reboot or reset the device.													

WBM pages/Features		User role										
		Admin	SecurityEngineer	SecurityAuditor	CertificateManager	UserManager	Engineer	Commissioner	Service	DataViewer	DateChanger	Viewer
Security section	Syslog	✓	✓									
	Certificate management	✓	✓	✓								
	User management	✓	✓		✓							
	User policies	✓	✓									
	LDAP configuration	✓	✓		✓							
System section	Device maintenance (c) can only change the user password (nr) cannot reboot oder reset the device	✓	✓		(c)	(c)	(nr)	(nr)	(nr)	(c)	(c)	
	App management	✓	✓				✓					
	System services	✓	✓									
	Backup & restore	✓	✓									
	License management	✓	✓									
	Update	✓	✓									
Shell		✓										
Update firmware, software and projects		✓									✓	
Legend: ✓ = full access, (r) = read-only access, (r/s) = read access and reset statistics, (c) = can only change the user password, (nr) = cannot reboot or reset the device.												

Tab. 40

Assigning Roles via WBM

1. Open 'Security' → 'User Management'.
2. Select the user to modify.
3. Click the role assignment area.
4. Select the desired roles from the available categories (Security roles, General roles).
5. Click 'SET USER ROLES'.

RBAC Rules

- assign only the minimum required rights (principle of least privilege)
- separate configuration, audit, and engineering duties where possible
- derive LDAP access from group membership, not direct per-user exceptions
- the 'Admin' user must only be used during commissioning – not in production operation

NOTICE

Avoid shared accounts. Every action on the controller must be attributable to an individual user for non-repudiation per IEC 62443.

8.8.5 User policies

General

User authentication

In the WBM the authentication with a user name and password is required for access to certain components of the controller.

In the delivery state, the 'admin' user is already created with administrator rights, and a unique default password is printed on the controllers' housing.



Security note: Use the default 'admin' password only for initial access and change it as soon as possible!

The modified administrator credentials are stored in the overlay file system which is located on the internal flash memory.

System use notification

The system use notification is displayed each time a user wants to log on to the controller via WBM or via SFTP and SSH. The system use notification is independent of the language of the user interface in WBM. You should therefore take all required languages into account when editing.

To edit the system use notification, proceed as follows:

- Click the ‘Edit Notification’ button.
- Edit the System Use Notification in the input window that opens.
- Confirm the entry by clicking the ‘Save’ button.

The text is then transferred to the controller and stored.

Note: The displayed text is stored in a .txt file on the controller by default and can also be changed or replaced if necessary. The file can be found on the file system of the controller under `/opt/plcnext/config/System/Um/SystemUseNotification.txt`. To change the file, you must be logged in as Linux user ‘admin’.

**Session Configuration
tab**

Configuring parameters

Configure session and lockout parameters in ‘Security’ → ‘User Policies’ on the ‘Session Configuration’ tab:

GeneralSession ConfigurationPassword PolicyBlocked Passwords

Session time

Maximum session time20 min

Failed login attempts

Issue timeout to admin users

Initial timeout10 s

Timeout increment30 s

Maximum timeout3600 s

Maximum concurrent sessions32

Parameter	Default Value	Description
Maximum session time	20 min	After this period of inactivity the session is automatically closed. Do not set this to 0 – this locks out everyone from the WBM.
Exclude ‘Admin’ users from timeout	false	When set to true, excludes admin users from timeout penalties on repeated login failures.
Initial timeout	10 s	Penalty time after three failed password attempts
Timeout increment	30 s	Additional penalty time after each further failed attempt
Maximum timeout	3600 s	Maximum penalty time between login attempts
Maximum concurrent sessions	32	Number of simultaneous communication channels permitted. Minimum value: 2.

Tab. 41



For security reasons, the 'Maximum concurrent sessions' value should be as low as possible. Each communication to the controller needs its own session, including WBM access. To determine the minimum viable value: count concurrent sessions required by your project (WBM, OPC UA, remoting, etc.) and add 2 to prevent locking yourself out. All changes made in the 'Session Configuration' tab are saved only by pressing the 'Apply and reboot' button. The controller only reboots if all settings can be applied error-free.

Applying changes and rebooting

All changes made in the 'Session Configuration' tab are saved only with pressing the 'Apply and reboot' button under the table. The controller will only reboot if all settings can be set in the system error-free.

If an error occurs, the firmware notifies only for the first error, but all touched settings are set back.

Password policy

In the Password Policy tab, all restrictions for user passwords can be set up, grouped as specific rulesets for users on the same trust level. See → 7.5 Password complexity rules for all further details.

Blocked passwords

In this tab, you will find a list of examples of blocked passwords like '12345678', 'qwertz' or 'admin'. You can add other passwords to the list by clicking on '+'.

8.8.6 LDAP configuraton

In this WBM page you can activate or deactivate the use of a central management of the users in a network (e.g. a Microsoft Active Directory). Note: More background information on configuration attributes and their default values can be found in the → 7.8 LDAP file-based configuration topic.

The overview page shows a table of existing LDAP configurations containing these columns:

Column	Description
Seq. (sequence)	Sequence number of the LDAP server (the LDAP servers are contacted in this order)
Host Name	Host name or IP address of the LDAP server
Port	TCP port of the LDAP server
Base DN	DN (Distinguished Name) where the LDAP search for users starts.
Bind DN	DN (Distinguished Name) of the user with which the search in the LDAP directory is performed (optional).
Comment	Local user specific comment

Tab. 42

Around the table you will find the buttons to add, remove, or edit an LDAP server configuration, and arrow buttons to moves a selected LDAP server configuration row upwards/downwards.

Basic configuration

In the Basic Configuration area you have the following setting options:

General configuration

Option	Description
Seq.	Sequence number of the LDAP server configuration (automatically assigned by the WBM 2)
Hostname	DNS name or IP address of the LDAP server

Option	Description
Port	TCP port of the LDAP server (optional). The port is chosen automatically, port 389 for connections without TLS or StartTLS and port 636 for TLS connections. If necessary you can specify the port where the LDAP server can be reached.
Timeout	Timeout after a connection attempt to the server failed. Enter an integer value in the input field and choose a unit from the drop-down list.

Tab. 43

Security options

Option	Description
TLS mode	Select the TLS mode from the drop-down list: – ‘TLS’: TLS is activated but StartTLS is deactivated – ‘StartTLS’: Both TLS and StartTLS are activated – ‘Deactivated’: Both TLS and StartTLS are deactivated
Trust Store	Select the Trust Store that is used for verification by entering a Trust Store name in the input field. All Trust Stores that match or start with the entry can be selected from the drop-down list. If you leave the input field empty, you can select from all existing Trust Stores.
Cipher list	List of permitted TLS cipher suites for the LDAP connection. See ➔ 7.8 Cipher lists

Tab. 44

Search options

Option	Description
Base DN	The LDAP DN (Distinguished name) that serves as starting point for the search for users over all child nodes.
Search filter	LDAP search filter that is used for the search for users. The variable "\$\$USER\$\$" is automatically replaced with the login.

Tab. 45

Login options

Option	Description
Bind DN	Enter the Distinguished Name of the user the search in the LDAP directory is performed with.
Bind password	Enter the password of the Bind DN user in the LDAP server.
Confirm bind password	Confirm the password of the Bind DN.

Tab. 46

Local options

Option	Description
Comment	Optional: Enter a comment on the LDAP server configuration.

Tab. 47

Enhanced Configuration

In the ‘Enhanced configuration’ area you have the following setting options.

Group Attributes

In this area you can add, remove, or edit Group Attributes of the LDAP server configuration.

Note: A group attribute for the initial group is mandatory. As long as this name is missing, the ‘Enhanced configuration’ heading is red and the new configuration cannot be added permanently.

LDAP Group Mappings

In this area you can manage a list of ‘LDAP Group Mappings’ to user roles. This setting is optional.

8.8.7 Syslog

In the Syslog WBM page you can configure connections for logging via syslog-ng, which is a system-wide, real-time capable log management tool.

The ‘Syslog server destinations’ table shows the configured server destinations to be used for defined facilities and severity levels. The table provides this information:

- ‘Hostname’: The hostname or IP address of the syslog-ng server destination to send the logging messages to.
- ‘Port’: The port on which the syslog-ng server waits for syslog messages. Make sure the port is enabled in the ➔ 8.8.3 Firewall settings.
- ‘Protocol’: Transmission protocol to the server. For secure transmission, TLS is recommended which depends on a Trust Store.
- ‘Facilities’: Specifies the system type of the messages to be logged.
- ‘Severity Level’: The severity level and its short term of the messages to be logged.

These levels are available:

- >= Internal (debug)
- >= Information (info)
- >= Warning (warning)
- >= Error (err)
- >= Critical Error (crit)
- >= Fatal Error (alert)
- Emergency (emerg)



Note: The >= before level terms means that lower severity levels also include higher levels. Examples:

- Selecting err will not send messages on the debug, info, or warning level.
- Selecting debug will also send messages that are on all other levels.

Adding and using a syslog server destination

When opening this WBM page for the first time, the Syslog Server Destinations table will be empty:

- To add a new server configuration entry, click on ‘+’ at the bottom of the table.
➔ The ‘Add a new Syslog server destination’ entry dialog opens.
- Set the hostname, transmission protocol, and transmission port for the destination.

Note: The specified address and the selected port must be enabled in the ➔ 8.8.3 Firewall settings for outgoing requests.

- If the TLS protocol is selected then a ➔ 8.8.2 Certificate management for verification must be defined; just click the input field.
- At the ‘Filter options’, select at minimum one facility and choose a severity level.
- Click ‘OK’ to add the new configuration entry to the table.
➔ The new entry is then available in the ‘Syslog server destinations’ table.
- Proceed with entries for other connections and facilities if needed.
- To save all changes made to the configuration, click the ‘Save and apply page’ button below the ‘Syslog server destinations’ table.
➔ The configuration is written to the XML configuration file.

Activating a syslog configuration

- Activate the toggle switch and click ‘Save and apply page’ below the table.
- The configuration is saved as an XML file in /opt/plcnext/config/Services/Syslog/Syslog.config.
- This XML file is then converted into a syslog-ng capable configuration file and loaded to run the logging.

Deactivating a syslog configuration

- Deactivate the toggle switch and click ‘Save and apply page’ below the table.
- An empty syslog-ng configuration file is generated, so no messages will be sent to a server destination. An existing XML configuration file will be left unaltered, though. So when you need the same configuration again you can just activate it. Also, if no destination is defined when activating no messages will be sent.

8.9 System**8.9.1 Device maintenance****PLCnext Runtime**

This controls the runtime of the system. The PLCnext Runtime and the CODESYS Runtime are linked together. Changing the state in the WBM or via CODESYS IDE results in status changes of both Runtimes and showing the status on both locations.

Device

With the ‘Restart the device’ button, you can restart the device.
With the ‘Reset the device’ button you can reset the device to default setting type 1.

Current user password

With the the ‘Change password’ button you can change the current password.

Password Policies

Password rules are configured in Security → User Policies.

The password complexity rules are predefined and depend on the rights of each user. Adapt the rule sets to the conditions of your application. Further information → 7.5 Password complexity rules.

‘Admin Ruleset’

Recommended for roles: ‘Admin’, ‘SecurityEngineer’, ‘SecurityAuditor’, ‘UserManager’, ‘CertificateManager’, ‘Engineer’.

- the username must not be included in the password
- the last 5 passwords must not be reused
- minimum length: 10 characters
- must include at least one uppercase and one lowercase letter
- minimum 1 digit
- minimum 1 symbol from the set: {}()#;,:.^?!|_ '~@\$%/\+=-.*&

‘Default Ruleset’

Suitable for roles with lower security exposure:

- the username must not be included in the password
- the last 5 passwords must not be reused
- minimum length: 8 characters
- must include at least one uppercase and one lowercase letter
- minimum 1 digit

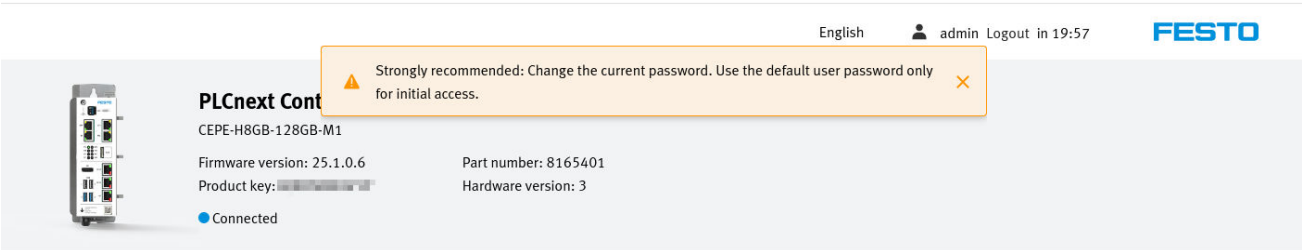
Change default password

After a user account with password was created, the respective user must change the default password. If you do not change the default password, appropriate warnings will be received.

NOTICE

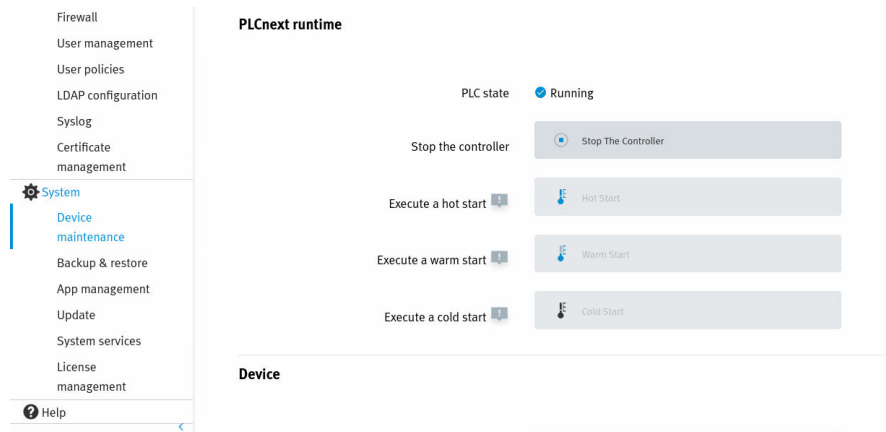
It is strongly recommended that you only use the default user password for the first access. Change the default password immediately after the first access.

The system informs the user via the following pop-up message that the password should be changed:

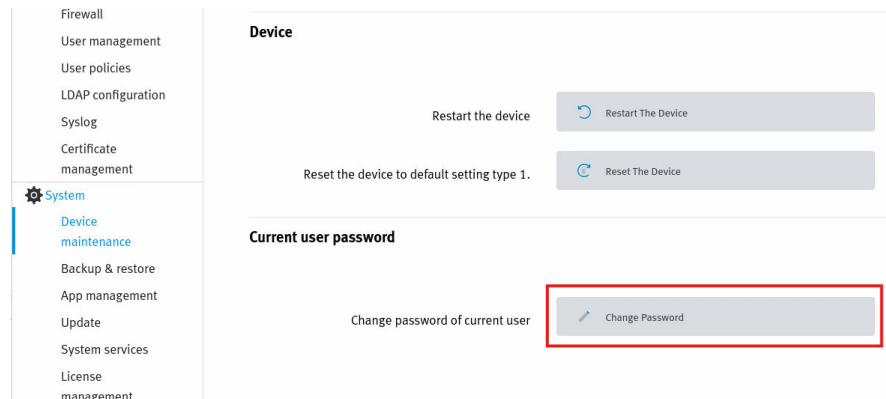


Following steps have to be done to change the default password of the currently logged-in user:

1. Go to the WBM page 'System', 'Device Maintenance'.



2. Scroll down and click the 'Change Password' button.



- Fill in the current password, the new password (twice), and confirm by clicking 'SAVE'.

Hardware version: 0

Change password of current user

Username: admin

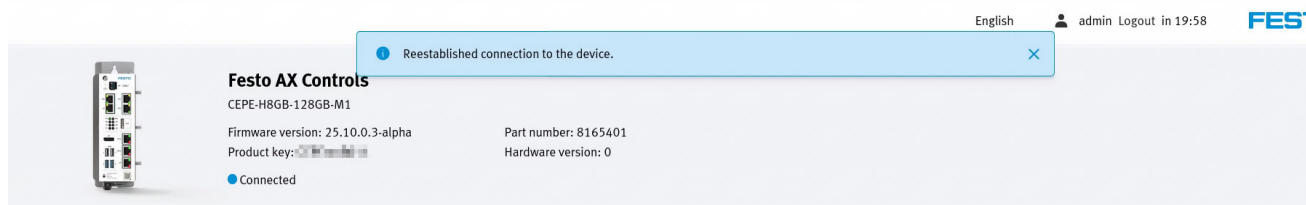
Current password: [masked]

New password: [masked]

Confirm password: [masked]

Cancel SAVE

- The pop-up message is now gone.



Checking Password Validity in the WBM

- Open 'Security' → 'User Management'.
- Review messages indicating whether passwords are still valid and whether a user has already changed their default password.
Alternatively, use 'Diagnostics' → 'Notifications' to see password-related notifications.

Password Policy Configuration

Configure password rulesets in 'Security' → 'User Policies' on the 'Password Policy' tab:

The tab allows configuring:

- password expiration time
- minimum password length
- complexity requirements (uppercase, lowercase, digits, special characters)
- password history depth (reuse prevention)

Blocked Passwords

'Security' → 'User Policies' on the 'Blocked passwords': A list of passwords, which can not be used to change initial password.

Additional Notes

- the printed 'admin' password is unique per device
- expiration and blocked-password controls can be configured according to the site policy
- the 'Admin ruleset' should be the default for all elevated roles

Strong passwords are effective only when combined with limited user roles, session controls, and restricted network access.

For the initial user creation procedure during commissioning, see → 7.7.6.8 Creating Users. For user management and session configuration, see → 8.8.4 User management.

8.9.2 License management

License Overview

The 'License Overview' tab on the License Management page displays the licenses of apps that are installed on the controller.

The following information is displayed:

Column	Description
Container	Serial number of the container. A container is used to manage licenses
Storage Location	Storage location of the license container
Firm Code	Identification of the licenser
Firm text	Description of the licenser
Product Code	Unique identification code of the licensed software
Feature Map	Specifies with which scope of functions the app is installed
Product text	Description of the license

Tab. 48

- Click the 'Refresh' button to refresh the overview of the licenses on the controller.

Checking for details

- Click on the 'Details' button to obtain further information on an app license. In addition to the information given in the 'License Overview' overview, the following fields can be found in the 'Details' window:

Field	Description
Activation Time	Date when the license is valid.
Expiration Time	Date when the license is invalid.
Usage Period	Usage period in days
Status	Current status of the license (License valid or License invalid)

Tab. 49

Offline Activation

On the 'Offline Activation' tab, licenses can be activated offline with a license ticket ID provided by the App Store. The term "offline" in this context means that the device which runs the licensed app does not have to be connected to the App Store during the license activation. This might be necessary if the device is located in an area without proper Internet connection, or for preventing security issues.

In the WBM, the Offline Activation Wizard will guide you through the activation process and provides further information.



Note: There are two file formats for offline activation.

- The Basic file format has these suffixes:
 - *.WibuCmRaC for the license context
 - *.WibuCmRaU for the license update
 - *.WibuCmRaR for the license receipt
- The PLCnext Store file format with extended meta information has these suffixes:
 - *.PLCnextRaC
 - *.PLCnextRaU
 - *.PLCnextRaR

Container Management

License container can be deleted.



Deleting license container will lead to a loss of activated licenses and should be avoided or handled advisedly.

8.9.3 App management

App management page

On the 'App management' page, you can install and uninstall apps. After successful installation you can also start and stop the apps from here. Additional apps can have an adverse affect on real-time behavior. Do not operate the 'App management' page when the controller is in productive operation.

Apps are software applications from libraries up to complete programs that are provided by the App Store. After registering you can download apps from → www.festo.com (search for your product) or the PLCnext Store → www.plcnextstore.com/ (filter for devices from Festo).



You can find Application notes for Apps from Festo under → www.festo.com/sp, search for the device type → Downloads → Expert knowledge.

Installing an app

To install an app, proceed as follows:

- Click on the 'Install App' button.
- In the file explorer that opens, select the app (*.app) to be installed.
- Click on the 'Open' button.

The selected app container is installed on your controller.

After successful installation, the app is displayed in the 'Installed Apps' table.



Note:

- After resetting your controller to factory default, every app will be deleted but the licenses will be retained.
- All Apps except for libraries may activate or deactivate System services in your firmware. Check and adjust configurations after installation.



To use apps, it can be necessary to enable the ports used by the app → 8.8.3 Firewall.

Uninstalling an app

- To uninstall an app, click on the button 'Uninstall'.

Installed Apps table

The table lists all installed apps with further app-specific information. This information is read out of the app_info.json file that is a part of every app container. The file contains information such as app name, a unique app ID, the app version, the minimum firmware version that is required, the app manufacturer and the license status. The license status indicates if the app is free, partly or fully limited:

- Fully limited app

A fully limited app has to be licensed before usage. It cannot be started without a valid license.

- Partly limited app

A partly limited app can be used partly, e.g. time restricted use or limited functionality. It can be started without a valid license but has to be registered for unrestricted usage.

- Free app

A free app can be used for free without restrictions.

Offline licenses are managed via the ➔ 8.9.2 License management page in the 'System' area of the Web-based Management.

Starting an app

Free or partly limited apps as well as apps with valid license can be started by clicking on the button 'Start'.

Note that the starting of several applications may require a restart of the controller. You will be notified of the forthcoming restart by a dialog that opens.

The app status 'RUN' is indicated in the column 'App Status'.

Stopping an app

- To stop an app, click on the button 'Stop'.

The App status 'STOP' is indicated in the column 'App Status'.

8.9.4 Update

Getting a firmware update file

On this WBM page, you can install a firmware update of the controller.

To update the controller firmware, proceed as follows:

- First of all, note the currently installed firmware version which is displayed on the General Data page, so you can check for the firmware update to be successful ➔ 8.5 Device .
- Download the firmware file:
For previous firmware versions, see the regarding product page on ➔ www.festo.com/sp. There you find all firmware versions and hotfixes that are available for your device.
- From the unzipped folder, copy the *.raucb update container file to the selected destination directory.

Note: the preferred method is updating the firmware with the Festo Automation Suite.

Selecting the firmware file

- Click on the 'Browse...' button.

In the file explorer that opens, select the *.raucb firmware file to be installed.

- Click on the 'Open' button.

The firmware file to be installed is now displayed in WBM.

Starting the firmware update

- To start the firmware update, click on the 'Update' button.

➔ The update file is transferred to the controller.

➔ Once the file has been successfully transferred, the firmware update is started.

➔ When the firmware update is done, the controller is restarted automatically.

The status of the file transfer and the status of the update process are displayed in the WBM as progress bars.

Checking the firmware version

- Refresh the browser tab showing this WBM page and log into WBM again.
- Open the ‘General Data’ page.
- Check whether the correct firmware version is displayed.

If the previously installed firmware version is still displayed after the firmware update (see ➔ Getting a firmware update file), an error occurred during the firmware update.

- In this case, repeat the firmware update.



Note:

If the boot process failed five consecutive times then the inactive and the active boot partition will change their roles, too. This behavior has been implemented to keep the Festo AX Controls device accessible even if the firmware update fails.

The behavior can also occur when the boot process is interrupted e.g. by power loss. In this case you will observe that the Festo AX Control boots with its previously installed firmware version. To prevent such unintended firmware downgrades, Festo recommends that after a finally successful firmware update, the same firmware should be installed once again. This way both the active and the inactive boot partition will contain the same firmware version.

8.9.5 System services

NOTICE

Activating further system services can compromise security

Before activating further system services, you must perform a risk and threat analysis of the system service and its impact on the security of the device and the application, taking into account the overall security context.

The WBM page ‘System’ ➔ ‘System Services’ shows which services are enabled, disabled, and enabled by default.

Service ID	Service name	Factory default	Activation
APP MANAGER	App Manager	Activated	☒
GRPC LOCAL SERVER	gRPC Remote Procedure Calls (Local)	Activated	☒
MCD2	Festo Device Discovery	Activated	☒
Mount USB1	mount USB1 to /media/usbstorage/usb1_fixed (Safe removal: stop all processes using USB1 before deactivating the service)	Deactivated	☐
Mount USB2	mount USB2 to /media/usbstorage/usb2_fixed (Safe removal: stop all processes using USB2 before deactivating the service)	Deactivated	☐
Mount USB3	mount USB3 to /media/usbstorage/usb3_fixed (Safe removal: stop all processes using USB3 before deactivating the service)	Deactivated	☐
Mount USB4	mount USB4 to /media/usbstorage/usb4_fixed (Safe removal: stop all processes using USB4 before deactivating the service)	Deactivated	☐
OPCUA	OPC UA Server	Deactivated	☐
PLCNEXT STORE	PLCnext Store Connector	Deactivated	☐
SOFTWARE UPDATE	Software Update via Device and Update Management	Activated	☒
SSHd	SSH daemon Socket	Deactivated	☐

General notes:

- To use services, it is necessary to enable the ports used by the service in the firewall, see Extended Firewall settings ➔ 8.8.3 Firewall.
- The firewall blocks/ filters only incoming packets (Direction: Server).

Disabling unused system services can be helpful to gain the performance of running programs.

NOTICE

Before disabling a default service, verify its function in the overall application. Some apps or maintenance functions depend on enabled services and open firewall ports.



With changing a setting, the whole 'System Services' settings are overwritten, so settings induced by a App will be set back, too. Make sure to leave those settings untouched, or refer to the App documentation to re-enable its system services settings.

Enabling or disabling a system service

If you want to use a System Service that is not active by default in the factory settings, or if you want to re-enable a System Service that has been disabled before or you want to disable a system service:

1. To changes the activation state, click on the toggle switch of the wanted service(s) under 'Activation'.
2. Apply the change(s) with the 'Apply and reboot' button, and confirm the pop-up warning.
3. After a reboot, the service toggled activation state is active as indicated in this WBM page.

Overview to the available system services



Note: Service availability is subject to the device in use.

Service ID	Description	Direction	Factory default	Port (Firewall default)	Protocol	Certificate
Mount USB <X>	Mounts USB drive /media/usb-storage/usb<X>_fixed automatically	-	deactivated	-	-	-
AppManager	Deactivating the App Manager only prevents accessing the App management page of the WBM	Server	activated	TCP 443 (Accept)	TLS 1.3	HTTPS
GRPC LOCAL SERVER	Local gRPC communication service	Server	activated	Localhost	—	Socket Linux access rights
PLCNEXT STORE	Connection to the app store for app downloads and license management	Client	activated	TCP 8883 (Accept)	TLS 1.3 / MQTT	Official AWS root certificates
SOFTWARE UPDATE	Enables performing firmware updates via WBM	Client	activated	TCP 443 (Accept)	TLS 1.3	IdevID HTTPS
MCD2	Festo Multicast daemon. Multicast-based discovery and commissioning	Server	activated	UDP 10002 (Accept)	FGMC (Festo, proprietary)	—
SSHd	SSH access to the controller shell	Server	deactivated	TCP 22 (Drop)	SSH	-
WBM	Web interface for device configuration and monitoring	Server	activated	TCP 443 (Accept)	TLS 1.3	IdevID HTTPS
OPCUA	OPC UA server	Server	deactivated	TCP 48010 (Drop)	OPC UA	OPC UA Sign and Encryption
Remoting	Remote Service Call communication for engineering tools	Server	activated	TCP 41100 (Accept)	RSC (Proprietary) over TLS 1.2	IdevID Device Certificates

Tab. 50



To use services, it is necessary to enable the ports used by the service → 8.8.3 Firewall.

The following Services are available via dedicated WBM pages:

Service	Description	Direction	Active by Default	Port (Firewall default)	Protocol	Certificate
NTP	Network time synchronization client.	Client	deactivated	UDP 123 (Accept)	NTP	–
Syslog	Security notifications registered are pushed to the Linux Syslog, see ➔ 7.11 Configuring Central logging.	Client	deactivated	Configurable (Accept)	TLS	Syslog-ng, own Trust Store configuration
LDAP	Centralized user management client.	Client	deactivated	TCP 389 (Accept)	TLS	LDAP, own Trust Store configuration

Tab. 51

Proprietary Protocols

The CEPE uses the following proprietary protocols:

Protocol	Service	Purpose
FGMC (Festo Generic Multicast)	MCD2	Multicast-based device discovery and commissioning on the local network segment.
RSC (Remote Service Call)	Remoting	Engineering tool communication for project download, debugging, and remote service access.

Tab. 52

All other services use open, standardized protocols (OPC UA, TLS, SSH, HTTP/S, NTP, LDAP, MQTT, TCP/UDP).

No undeclared proprietary protocols are present on the CEPE. All communication protocols used by the firmware are listed in the service table above or documented with the respective app.

Physical Interfaces

For physical interfaces check ➔ 7.7.2 Get Familiar with the CEPE.

USB Mount Service

Depending on WBM configuration of system services, usb mount services shall be enabled/disabled

Enabling of mounting of usb-massstorages is done via udev-rules. See

<https://www.kernel.org/pub/linux/utils/kernel/hotplug/udev/udev.html>

Using mount-command from udev-rule is not allowed.

Note that running programs that access the network or mount/unmount filesystems is not allowed inside of udev rules, due to the default sandbox that is enforced on systemd-udev.service.

8.9.6 Backup and Restore

Backups are used for fast recommissioning after reset or failure.

Included in Backup Packages

– Configuration data (top-level view):

- network settings
- time configuration
- system services
- web services
- certificates
- firewall settings
- users
- syslog settings
- app configuration
- SSH access settings

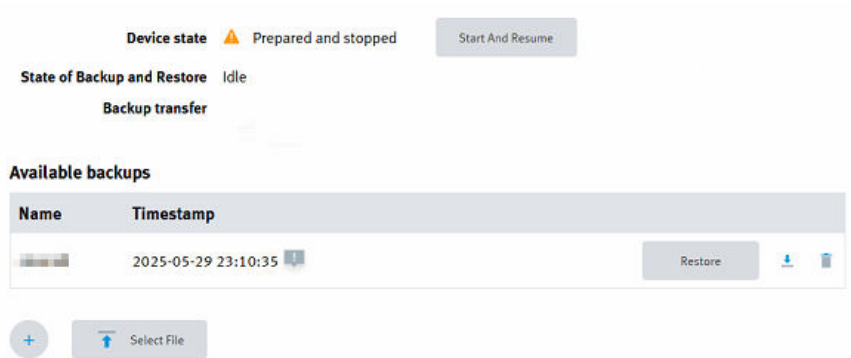
- Application data:
 - PLC program
 - APP application default data (depending on app development)

Not Included

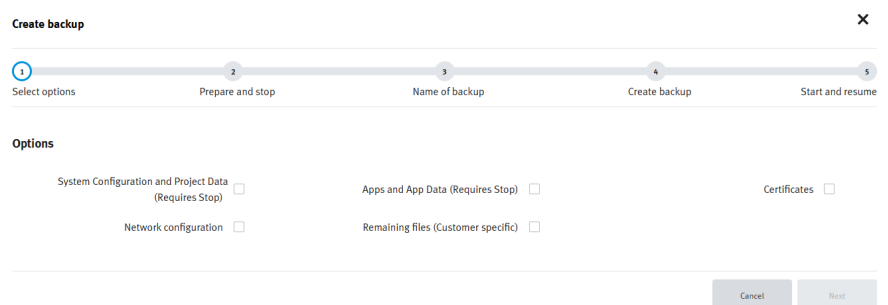
- firmware image itself – must be installed before restore
- licenses that remain bound to the hardware and must be handled separately

Creating a backup

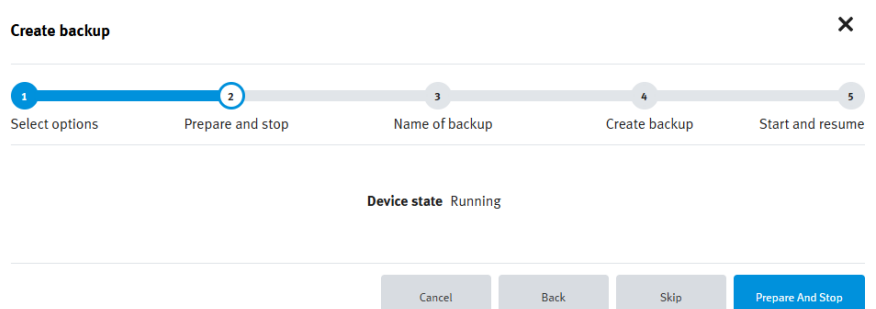
1. Log in to the WBM.
2. Open 'System' → 'Backup & Restore'.



3. Click the '+' button to create a new backup.
4. In step 1, select the data categories to include:
 - 'System Configuration and Project Data': everything configured in the WBM (Firewall, Services, passwords, etc.)
 - 'Apps and App Data': all installed apps, including app runtime data
 - 'Certificates': certificates of the device
 - 'Network Configuration': device-specific network configuration (IPv4 settings, etc.)
 - 'Remaining files': files manually added to the system by the user which the system is not aware of



5. Click 'Next'.
6. In step 2, click 'Skip' if no runtime stop is required, or 'Prepare and Stop' if prompted:



7. In step 3, enter a meaningful name for the backup file, then click 'Next':

The screenshot shows the 'Create backup' dialog box with a progress bar at the top. The progress bar has five steps: 1. Select options, 2. Prepare and stop, 3. Name of backup (highlighted), 4. Create backup, and 5. Start and resume. Below the progress bar, there is a text input field labeled 'Name of backup' with a small '1' icon next to it. At the bottom right, there are three buttons: 'Cancel', 'Back', and 'Next'.

8. In step 4, enter and confirm a password to encrypt the backup, then click 'Next':

The screenshot shows the 'Create backup' dialog box with a progress bar at the top. The progress bar has five steps: 1. Select options, 2. Prepare and stop, 3. Name of backup, 4. Create backup (highlighted), and 5. Start and resume. Below the progress bar, there is a section labeled 'Status of backup' with the value 'Idle'. Below that, there is a 'Password' field with a red error message 'This field is required.' and a small '1' icon next to it. At the bottom right, there are three buttons: 'Cancel', 'Back', and 'Create Backup'.

9. Click 'Create Backup' and wait for the procedure to complete:

The screenshot shows the 'Backup' dialog box with a progress bar at the top. The progress bar has five steps: 1. Select options, 2. Prepare and stop, 3. Name of backup, 4. Create backup (highlighted), and 5. Start and resume. Below the progress bar, there is a section labeled 'Status' with the value 'Idle'. Below that, there is a 'Current state' field with the value 'Idle'. At the bottom right, there are three buttons: 'Cancel', 'Back', and 'Create Backup'.

10. In step 5, click 'Start' AND 'Resume':

The screenshot shows the 'Create backup' dialog box with a progress bar at the top. The progress bar has five steps: 1. Select options, 2. Prepare and stop, 3. Name of backup, 4. Create backup, and 5. Start and resume (highlighted). Below the progress bar, there is a section labeled 'Device state' with the value 'Prepared and stopped'. At the bottom right, there are two buttons: 'Finish' and 'Start And Resume'.

11. The new backup file appears in the ‘Available backups’ table:
⇒ Backups are stored on the device at /opt/plcnext/data/Services/BackupAndRestore.

Available backups

Name	Timestamp	
	2025-05-29 23:10:35	Restore  
	2025-06-05 17:56:18	Restore  

Downloading a Backup

- To download a backup file to your local machine:
1. In the ‘Available backups’ table, click the download button for the desired backup.

Available backups

Name	Timestamp	
	2025-05-29 23:10:35	Restore  
	2025-06-05 17:56:18	Restore  

2. The download state is displayed:

Device state

 Prepared and stopped

Start And Resume

State of Backup and Restore

Idle

Backup transfer

Download:  (23.9 MB)

.backup 

Uploading a Backup

- To upload a previously downloaded backup file:
1. Click the ‘Select file’ button.



2. After upload, the backup file is shown in the list:

iB-128GB-M1

version

ey: LW

ted

1

Transfer of backup to device successful.

X

Status

Device state

 Prepared and stopped

Start And Resume

State of Backup and Restore

Idle

Backup transfer

Upload:  (23.9 MB)

.backup 

Available backups

Name	Timestamp	
	2025-05-29 23:10:35	Restore  
	2025-06-05 17:56:18	Restore  

Performing a Restore

- 1. Log in to the WBM.
- 2. Open ‘System’ → ‘Backup & Restore’.
- 3. In the table of available backups, select the backup to restore:
 - ⇒ Backups created for another device will be marked. Backups from a different major version cannot be applied (e.g. backup from 25.x.x.x on firmware 26.x.x.x).

Available backups

Name	Timestamp	
	2025-05-29 23:10:35	Restore 
	2025-06-05 17:56:18	Restore 

- 4. In step 1, select the data categories you want to restore, then click ‘Next’:

Restore backup foo

1

2

3

4

5

Select options

Prepare and stop

Restore

Restart the device

Start and resume

Options

System Configuration and Project Data

Apps and App Data

Certificates

Network configuration

Remaining files (Customer specific)

⚠ ATTENTION: If the device has been compromised a manual factory reset is required.

Cancel

Next

- 5. In step 2, click ‘Prepare and Stop’ if prompted:

Restore backup foo

1

2

3

4

5

Select options

Prepare and stop

Restore

Restart the device

Start and resume

Device state Running

⚠ ATTENTION: For the selected set of options, the device needs to be stopped.

Cancel

Back

Skip

Prepare And Stop

- 6. In step 3, enter the backup password and click ‘Restore’:

Restore backup foo

1

2

3

4

5

Select options

Prepare and stop

Restore

Restart the device

Start and resume

Status of restore Idle

Password

This field is required.

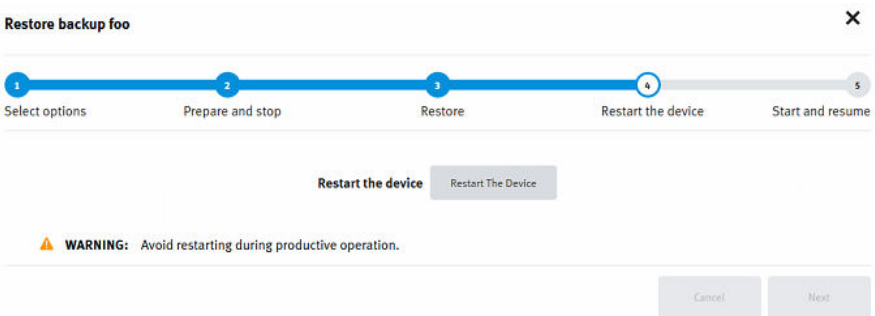
⚠ ATTENTION: After restoring, an immediate reboot is required to activate the changes. Do not make any other changes in between.

Cancel

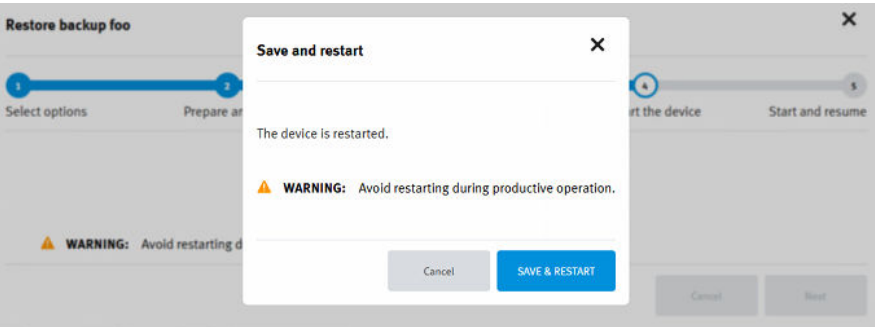
Back

Restore

7. In step 4, click ‘Restart the Device’:



8. After the device restarts, log in to the WBM and verify the restore completed successfully:



Restore Behavior

- restore returns the selected data categories to the backed-up state
- backup integrity is verified before restore
- the correct firmware version must be present before restore

NOTICE

A restore overwrites current settings with backed-up data. Use it only on the intended device or a validated replacement device with compatible hardware and firmware.

For reset procedures, see ➔ 7.13 Reset Procedures.

8.10 Help

Documentation

Licenses

Links to further information.

Licensing information on open source software.

Festo AX controls controllers work with a Linux operating system. All license information can be called up via the ‘Licenses’ page on .

Licenses for all of the open source software used are shown.

Festo SE & Co. KG

Ruiter Straße 82
73734 Esslingen
Germany

Phone: +49 711 347-0
www.festo.com