

AXC F 2000 EA

Firmware Change Notes

Change Note for the Firmware installed on the PLCnext Control AXC F 2000 EA



Change Notes
111756_en_01

© Phoenix Contact 2026-01-08

General Notes

This document contains all changes between Firmware Version V2025.0.3 (PLCnext Core 2025.0.3) and the current Firmware Version of the PLCnext Control AXC F 2000 EA (Part No.: [1551772](#)).

Current Firmware-Versions:

- V2025.0.4 (PLCnext Core 2025.0.4)
- V2025.0.3 (PLCnext Core 2025.0.3)

Follow these instructions



Make sure that you always work with the latest documentation.
This is available for download at www.phoenixcontact.com/product/1551772.

Table of Content

1 Order Data 3

2 Changes in version 2025.0.4 4

 2.1 New functions4

 2.2 Error corrections4

 2.3 Known limitations and errors.....5

3 Changes in version 2025.0.3 6

 3.1 Known limitations and errors.....6

1 Order Data

Products

Description	Type	Part No.	VPE
PLCnext Control	AXC F 2000 EA	1551772	1
Description	Type	Part No.	VPE
User Manual , English, Axioline F: Installing and starting up of the Axioline F controller AXC F 2000 EA	UM EN AXC F 2000 EA	111673	-
Package Insert for AXC F 2000 EA	PACKB AXC F 2000 EA	111577	-
User Manual, English, Axioline F: Diagnostic Register and Error Messages	UM EN AXL F SYS DIAG	8663	-
User Manual, English: Axioline F: System and Installation	UM EN AXL F SYS INST	7982	-
User Note, English, Measures to Protect Network-Enabled Devices with Ethernet Connection from Unauthorized Access	AH EN INDUSTRIAL SECURITY	107913	-

2 Changes in version 2025.0.4

PLCnext Core 2025.0.4

This chapter shows known issues with the release version of the Firmware installed on the PLCnext Control AXC F 2000 EA.

2.1 New functions

Factory Reset Type 1

The factory reset type 1 is available via Web-based Management (WBM), provided with date of manufacture from 2026 or later.

Incrementation of IPsec Policy ID

When configuring VPN IPsec via the Web-based Management, the system automatically increments the policy ID for every new policy entry.

Additional description for IPsec

Additional description and explanation of the VPN IPsec configuration in the Web-based Management.

IPsec save button disabled

After deleting an IPsec policy ID and saving the changes, the Save button becomes disabled.

License management in offline mode

You can activate the license offline, provided with date of manufacture from 2026 or later.

Modbus/TCP activation

Modbus/TCP is now part of the firmware. The activation is available via Web-based Management.

Proficloud activation

Proficloud activation is now available via Web-based Management.

2.2 Error corrections

Encryption of PSK password

The PSK password of the VPN IPsec configuration in the Web-based Management is not displayed in plain text anymore.

IPsec Number of the policy had be adjusted manually

The General configuration for the VPN IPsec policy ID has been adjusted manually for each new policy.

Wrong notification of Password change

After changing the password via the Web-based Management, the error message "Default password of the user active" is no longer displayed.

Reset type 1 did not work via the WBM

The reset to default setting type 1 (factory reset 1) did not work via the Web-based Management. It only worked via the reset button on the module.

"Save" button was not grayed out when changing IPsec policies

When changing IPsec policies, the button was sometimes not grayed out after saving, even though the changes had already been saved.

Wrong notification after password change

Although the default password of the user admin had been changed, an error message was displayed.

Proficloud was not allowed to be activated

When Proficloud was activated, the firewall was also activated. This blocked access to the controller.

Licensing of additional apps was not possible

Now you can activate additional licenses for apps.

2.3 Known limitations and errors

Rebooting for Factory Reset Type 1

After a type 1 factory reset, the device does not boot properly. In this case, repeat the procedure.

Netload Limiter cannot be activated

The Netload Limiter cannot be activated.

The WBM reports "Connection interrupted" at irregular intervals

Sometimes the Web-based Management disconnects and automatically reconnects. It does not have any influence on the functionality of the device.

The firewall configuration is deleted by changing a system service

When changing the state of any system service (activated ↔ deactivated) the user-defined firewall settings are deleted and must be re-entered.

3 Changes in version 2025.0.3

PLCnext Core 2025.0.3

This chapter shows known issues with the release version of the Firmware installed on the PLCnext Control AXC F 2000 EA.

3.1 Known limitations and errors

Labeling of the Ethernet Ports within the PLCnext Engineer is wrong

The Labelling of the Ethernet Ports in the PLCnext Engineer V.2025.9 show the wrong description:

The sequence is still correct:

- LAN1/X1
- LAN2/X2
- LAN3/X3

The issue will be fixed in a future version of the PLCnext Engineer.

Wrong notification on Password change

Although the default password of the user **admin** has been changed from the printed password to **Phoenix1234!** the following error message is displayed.

Default password of the user active.

Netload Limiter cannot be activated

The Netload Limiter cannot be activated

Licensing of additional Apps not possible

It is not possible to activate Licenses of additional Apps from the PLCnext Store.

The website reports "Connection interrupted" at irregular intervals

Sometimes the Web Interface disconnects and automatically reconnects. It does not have any influence on the functionality of the device.

Firewall configuration will be deleted when changing the status of a system service

When changing the state of any system service (activated <-> deactivated) the custom firewall settings will be deleted and have to be re-entered.

IPsec - Number of the policy must be adjusted manually

Under **/VPN IPsec/General configuration**, the policy ID must be adjusted manually for each new policy.

This is currently always set to 1 by default. This means that

1. it is not obvious that something needs to be entered here.
2. if it is not changed, an error message appears when saving - without any further indication of the cause.

The Reset to default setting type 1 (factory reset 1) does not work through the Web Interface

The reset to default setting type 1 (factory reset 1) does not work through the Web Interface.

It does work through the Reset Button on the device.

„Save“ button when changing IPsec policies does not grey out

When changing IPsec policies, sometimes after saving the button does not grey out, even though the changes have already been saved.

Proficloud shall not be activated

When the Proficloud service is activated, also the firewall is activated for the web interface. This prevents the access to the controller.

If activated the device has to be set to default setting type 1 (factory reset 1) via the reset button of the device to regain access.