

VIRTUAL PLCNEXT CONTROL - CHANGE NOTES

Change Notes for the Virtual PLCnext Control VPLCNEXT CONTROL 1000 VPLCNEXT CONTROL 2000 VPLCNEXT CONTROL 3000

Application note

112226_en_00

© Phoenix Contact 2025-08-13

1 General information

The Virtual PLCnext Control is a software-based virtual control for industrial use, suitable for edge applications and the control and monitoring of machines and processes.

This document contains all changes made between firmware version 2025.0 and the current firmware version of the Virtual PLCnext Control:

- VPLCNEXT CONTROL 1000 (item no. 1737875)
- VPLCNEXT CONTROL 2000 (item no. 1738453)
- VPLCNEXT CONTROL 3000 (item no. 1738454)

Current firmware version: **2025.6.0**

Observe the following general notes:

Toolchain

To be able to use all new functions of a firmware version, always use all elements of the toolchain in the same version. The toolchain includes, for example, PLCnext Engineer, SDK and PLCnext CLI.

Documentation

- Make sure you always use the latest documentation. It can be downloaded at:
VPLC 1000: phoenixcontact.com/product/1737875
VPLC 2000: phoenixcontact.com/product/1738453
VPLC 3000: phoenixcontact.com/product/1738454
- Further information on the PLCnext Runtime and programming can be found under plcnext.help
- Further information on security in the context of PLCnext Technology can be found under security.plcnext.help

Firmware releases

Feature releases or hotfixes of an LTS version are based on the previous versions of the respective branch. Therefore they only contain the features, changes, error corrections, and security updates of the previous version. Refer to “[Firmware releases VPLCNEXT CONTROL](#)” on page 2 to see on which release branch your firmware version is located and which features, changes, error corrections, and security updates your firmware version contains.

2 Table of contents

1 General information.....1

2 Table of contents.....2

3 Firmware releases VPLCNEXT CONTROL2

4 Changes in firmware version 2025.6.0.....3

4.1 New functions.....3

4.2 Error corrections.....3

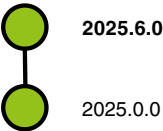
4.3 Known limitations and errors.....4

4.4 Security updates.....4

3 Firmware releases
VPLCNEXT CONTROL

Long-term
support

Feature
release



4 Changes in firmware version 2025.6.0

This section describes changes made between firmware version 2025.0.0 and firmware version 2025.6.0. All parts of the previously released version are included in the current version.

This section describes changes made between firmware version 2025.0.3 and firmware version 2025.6.0. All parts of the previously released version are included in the current version.



To be able to use all new functions of the firmware, you need PLCnext Engineer version 2025.6 or newer. Select the latest template for firmware version 2025.6 in the PLCnext Engineer project.



In order to update to firmware version 2023.0.0 LTS or newer at least a firmware version 2022.0 LTS or newer must be installed on the PLC. Older firmware versions will not accept the *.rauc firmware update file.

4.1 New functions

Virtual PLCnext Control

When restarting the virtual PLC via the RSC service (e.g. using WBM or PLCnext Engineer), previously only the PLCnext firmware was restarted. With firmware 2025.6, the Podman container is now restarted.

4.2 Error corrections

App

- If an OCI container app was updated while it was in the RUN state, the app disappeared from the web-based management 2 (WBM 2) without an error message. After restarting the PLC, the app was displayed again. To prevent this behavior, the app had to be set to the STOP state before updating. This known issue has been fixed.
- When installing an app that contains an EHMI part, this EHMI can only be accessed after the Virtual PLCnext Control container has been restarted via its host.

Backup

The backup and restore feature did use a maximum file name length of 256 bytes for the backup archive. In some cases this was too short and backup and restore did not work properly. The maximum file name size has been increased to 4096 bytes.

C/C++

Using the ANSI C API it was possible to trigger a Start() at the PlcManager while the PLC was in state "Starting". This led to an invalid PlcState "Running | Starting". Now the PlcManager waits until the "Starting" state has been finished.

WBM

- On the "password policy" tab of the WBM page "User policies" the values of the password interval rules "Password changes per interval" and "password change interval" were swapped with firmware version 2025.0.
- On the WBM page "Diagnostics - Profinet", the scrolling behavior has been corrected in the tree view.

OPC UA server

If the OPC UA server's endpoint has been configured with an IP address that does not match to the IP configuration of the PLC, the OPC UA server threw an exception and the firmware exited. In this situation now the OPC UA server emits the notification `Arp.Services.OpcUAServer.StartFailed`. The firmware starts up and after correction of the endpoint configuration a project download turns the OPC UA server into operation.

OPC UA client

The behavior of the PLC's built-in OPC UA client has been improved for a better coherency in the following cases:

- A value change at the server side could be missed by OPC UA client if this change occurred while the connection between client and server is cut.
- After the PLC program is started (also if "Write and start project" is executed in PLCnext Engineer) the OPC UA client now retrieves the latest values from the configured server. After receiving these values, which may take some time, the OPC UA client writes them to the configured variables (thus overwriting the variables' initial value).

System

- If with firmware 2025.0 the static logger was used by a component, which was executed in the PLCnext firmware process, no messages have been logged. This error has been fixed.
- When activating the Security Profile, the IP configuration sometimes got lost and the PLC started with the default IP configuration. The PLC needed to be re-booted another time. This known issue has been fixed.

Proficloud

If too many OUT port variables have been marked as “IoT” in PLCnext Engineer or as “Proficloud” attribute in C++, a System Watchdog (SWD) occurred. With firmware 2025.6, no SWD occurs in this case. Instead, a warning is issued in the “Arp.log” file, indicating that not all variables are sent to the Proficloud or to an MQTT broker.

Virtual PLCnext Control

- Software watchdogs (SWD) could cause reboot loops. The System Monitoring now prevents these loops.
- The RSC method `IDeviceControlService::ResetToFactoryDefaults()` previously stopped the PLC but did not perform the requested reset. Since this reset is not permitted for Virtual PLCnext Control, the method now has no effect when executed.
Note: This RSC method is also used by PLCnext Engineer.
- When the container is restarted or the host system is rebooted, the folder `/var/tmp/` is now cleared.

EHMI

When retrieving a range of array values via REST call, the entire array was returned. This issue has been fixed and now only the values within the requested range are returned.

4.3 Known limitations and errors

The known limitations and errors can be found in the PLCnext Info Center at:

https://www.plcnext.help/en/known_issues.htm

Here you will find a constantly updated overview of all known issues.

4.4 Security updates

The following security updates have been made in this release. For more information about the specified CVE numbers, see:

- <https://nvd.nist.gov/vuln>
- <https://cert.vde.com>

Information on the Phoenix Contact “PSIRT” can be found at: <https://www.phoenixcontact.com/psirt>

Abseil CPP

- CVE-2025-0838

Curl

- CVE-2025-4947

FastCGI

- CVE-2025-23016

Git

- CVE-2025-46835
- CVE-2025-48384
- CVE-2025-48385
- CVE-2025-48386

Less

- CVE-2024-32487

Libxml2

- CVE-2025-6021
- CVE-2025-49794
- CVE-2025-49795
- CVE-2025-49796

Libssh

- CVE-2025-5318

Libpam

- CVE-2025-6020
- CVE-2024-10041

OpenVPN

- CVE-2025-2704

Perl

- CVE-2024-56406

Podman

- CVE-2024-11218
- CVE-2025-6032

Setuptools

- CVE-2025-47273

Sqlite

- CVE-2025-29088
- CVE-2025-29087
- CVE-2025-3277

Sudo

- CVE-2025-32462
- CVE-2025-32463

Syslog-ng

- CVE-2024-47619

TPM2

- CVE-2024-29040

WBM

- With firmware 2025.0, the user role “SecurityAdmin” has been renamed to “SecurityEngineer” but the permissions stayed the same. With that release, a minor issue is present: The “SecurityEngineer” user role must be used together with the “Admin” user role, because the user role “SecurityEngineer” incorrectly had no access rights for the user management as well as to activate/deactivate system services via WBM. This known issue has been fixed.

Container

OCI container applications did not work in “Virtual PLCnext Control”. Container Apps can now be used. An additional configuration is necessary for rootless container networking: /dev/net/tun has to be mounted and /proc/* needs to be unmasked. This is only necessary if container apps are to be used.

PROFINET

A specific invalid UDP datagram sent to a PROFINET UDP port could cause a segmentation fault (SIGSEGV).