Release Notes

LCOS LX
7.10 Rel

Table of contents

1. Preface

The LANCOM family of operating systems—LCOS, LCOS SX, LCOS LX, and LCOS FX—forms the trusted basis for the entire LANCOM range of products. Within the scope of the hardware specified by the products, the latest firmware version is available for all LANCOM products and is offered by LANCOM Systems for download free of charge.

This document describes the innovations within LCOS LX software release 7.10 Rel, as well as the improvements since the previous version.

Before upgrading the firmware, please pay close attention to chapter 7 "General notes" of this document.

Latest support notes and known issues regarding the current LCOS LX version can be found in the support area of our website www.lancom-systems.com/service-support/instant-help/common-support-tips.

2. The release tag in the software name

Release Candidate (RC)

A Release Candidate has been extensively tested by LANCOM and includes new LCOS featurses. It is suitable for testing and is not recommended for use in productive environments.

Release Version (REL)

The release version has been extensively and successfully tested in practice. It contains new features and improvements over previous LANCOM operating system versions and is therefore recommended for use in productive environments.

Release Update (RU)

A release update is a further development of an initial release version in productive environments and contains minor improvements, security fixes, bug fixes and smaller features.

Security Update (SU)

Contains important security fixes for the respective LANCOM operating system version and ensures that your security level remains very high on an ongoing basis in your productive environment.

3. Device-specific compatibility to LCOS LX

LANCOM products regularly receive major firmware releases throughout their lifetime which provide new features and bugfixes. LCOS LX release updates including bugfixes and general improvements are available on a regular basis for devices which do not support the latest LCOS LX version. You can find an overview of the latest supported LCOS LX version for your device under www.lancom-systems.com/lifecycle.

4. Notes on LCOS LX

Information on default settings

Devices delivered with LCOS LX automatically connect to the LANCOM Management Cloud (LMC). This functionality provides zero-touch installation for new devices. In case you do not want to use the LMC, this feature can be disabled while running the default setup wizard for the initial configuration, or at any time from within LANconfig under Management > LMC. You can manually re-enable the usage of the LMC whenever you want.

5. Known restrictions

- → Local configuration changes are not transferred to the LMC.
- → The scripting of the device from the LMC is currently not supported, but the use of add-ins is.

6. History LCOS LX

LCOS LX - improvements 7.10.0117 Rel

New Features

General

→ Syslog messages can now be viewed in the LCOS LX menu tree.
→ The LCOS LX menu tree now allows navigation into individual line entries using the ‘cd’ command.
→ Connected USB devices are now displayed in both the LCOS LX menu tree and the WEBconfig dashboard.

Wi-Fi

→ Support for Multi-Link Operation (MLO) on Wi-Fi 7 access points
→ Dedicated encryption profile available for Wi-Fi 7-compliant wireless operation
→ The default encryption profile is now P-PSK-WPA2-3.

Bugfixes / improvements

General

→ If requests were continuously opened on port 443 of an access point, the HTTP service consumed more and more memory and no longer released it.
→ The cURL library has been updated to version 8.12.1 due to the vulnerabilities CVE-2024-6197 and CVE-2024-7264.
→ The SSL library wolfSSL has been updated to version 5.7.6 due to the vulnerabilities CVE-2023-6936, CVE-2023-6935, CVE-2023-6937, CVE-2024-154, and CVE-2024-5991.
→ If an ePaper USB stick was unplugged from the access point and plugged back in, the interface usb0 was no longer included in the standard bridge group ‘br-lan’. As a result, the stick could not communicate with the local network.
→ In the command line output of the ‘Status/WLAN/Radio’ table, the temperature of the Wi-Fi modules was always displayed with the value ‘0’ (0 degrees Celsius).
→ The ‘Network name’ selection field in the LEPS configuration could contain a maximum of 32 characters. As a result, a reference to a selected WLAN network profile with a longer name appeared incomplete and a warning was displayed. The ‘Network name’ selection field may now be a maximum of 64 characters long.

- → In PoE mode, the LANCOM access points LX-7300 and LX-7500 require a switch with support for 802.3bt for all wireless functions. With 802.3at, the access points can be operated in restricted Wi-Fi mode. If these access points were connected to a switch with support for 802.3at, it could happen that only 13 W instead of 25.5 W was assigned to the access points. This deactivated the wireless functionality of the access points.
  If the negotiation via LLDP between access point and switch does not work (only 13 W assigned), the access point now requests a fixed value of 25.5 W from the switch after 70 seconds.
- → ARP requests from the access point's management network were also sent in the L2TP tunnel. If user data and an ARP request from the access point were sent via the L2TP tunnel at the same time, this led to a deadlock, as a result of which the access point was initially no longer accessible and later performed an unmediated restart.
- → If packets were transmitted via an L2TP tunnel that were the same size or larger than the MTU, this resulted in the tunnel being aborted.
  Furthermore, when using Static VLAN on the access point, no message was sent to the WLAN clients if the packets were too large.
- → If the commands to delete the wireless network were executed very quickly one after the other, it could happen that a wireless network was still being broadcast even though it was no longer present in the configuration.
- → If an access point sent a RADIUS challenge with a state ID to a RADIUS server, but the server did not respond to the challenge, the access point sent a RADIUS challenge with the same state ID to the backup RADIUS server. The RADIUS server acknowledged this accordingly with an error message.
- → Two or four 20 MHz wide Wi-Fi channels are combined to form virtual 40 MHz or 80 MHz wide channels (e.g. channels 52 and 56 are combined to form the 40 MHz wide channel 54). If a radar signal was detected when using 40 or 80 MHz wide Wi-Fi channels in the 5 GHz band, this resulted in the associated virtual 40 MHz or 80 MHz channel being entered in the console path 'Status/WLAN/Channel-Scan-Results' in addition to the 20 MHz wide Wi-Fi channels (e.g. virtual channel 54).
  The virtual channel is no longer listed in the table after radar detection.
- → When communicating with the LMC, the DF flag (Don't Fragment) was not always set. If the packets had to be fragmented due to the MTU, this resulted in the access points being displayed as offline in the LMC and no WEBconfig or terminal session could be started.

- After a DHCP renew, the access point retained its previously assigned IP address and did not release it. As a result, the access point was accessible via multiple IP addresses and the IP addresses obtained were no longer available in the DHCP address pool.
- The deactivated test mode when rolling out the device configuration via the LMC (e.g. in a maintenance project to configure the devices without Internet access) was ignored by the access point. As a result, the configuration was not accepted.
- In the 6 GHz band, the mixed IEEE 802.11 mode was incorrectly displayed with the value “11anacaxbe-mixed”, although the a, n, and ac modes are not supported.
- Access points managed by the LMC sent a DNS request to the address ‘hotspot.lmc.de’ every second.
- In Australia and New Zealand, the automatic channel selection also selected channel 149, which is not permitted there.

7. General notes

Disclaimer

LANCOM Systems GmbH does not take any guarantee and liability for software not developed, manufactured or distributed by LANCOM Systems GmbH, especially not for shareware and other extraneous software.

Backing up the current configuration

Before upgrading your LANCOM devices to a new LCOS LX version it is essential to backup the configuration data!
Due to extensive features it is **not possible to downgrade** to a previous firmware without using the backup configuration.
Please see the LCOS LX reference manual for instructions on how to upgrade the firmware.

We strongly recommend updating productive systems in client environment only after internal tests. Despite intense internal and external quality assurance procedures possibly not all risks can be eliminated by LANCOM Systems.

LANCOM Systems GmbH
A Rohde & Schwarz Company
Adenauerstr. 20/B2
52146 Wuerselen | Germany
info@lancom.de | lancom-systems.com