Release Notes

LCOS LX
5.36 RU3

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 5.36 RU3, 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 https://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 has been extensively and successfully tested in practice. It contains new features and improvements over previous LANCOM operating system versions. Recommended for use in productive environments.

Release Update (RU)
This is a further development of an initial release version and contains minor improvements, 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.

3. Device-specific compatibility to LCOS LX

LANCOM products regularly receive major firmware releases throughout their life-time 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 https://www.lancom-systems.com/products/lcos/lifecycle-management/product-tables/

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. History LCOS LX 5.x / 4.x

LCOS LX improvements 5.36.0137 RU3

Bugfixes / improvements

→ The ‘DHCP lease time’ of the cloud-managed hotspot has been reduced from 24 hours to 8 hours.

→ In scenarios with 802.1X authentication and simultaneous use of FT (Fast Transition), a PMK is now cached per station and BSSID.

→ During the initial Wi-Fi login of a client in an 802.1X scenario using FT (Fast Transition), the PMK (Pairwise Master Key) was only created for the Wi-Fi interface on the currently used frequency band, but not for Wi-Fi interfaces with the same SSID on a different frequency band. If the wireless client tried to connect to the SSID on a different frequency band at a later time, this caused either the login to fail (when using FT) or the complete key negotiation to have to be gone through again.

→ If a channel change was made for an SSID that the access point was already broadcasting, the changed channels were not used.

→ It was not possible to edit the encryption profiles for WPA2-802.1X via the ‘Edit RADIUS profiles’ menu item. An empty window was displayed here instead of the selectable data. Furthermore, the time frame in the menu ‘Wi-Fi configuration - SSID’ could not be edited either.

→ If no gateway was stored (learned via DHCP), there was no route for multicast packets. This meant that IAPP packets could not be transmitted and roaming therefore did not function without interruption.

→ Due to an error in the handling of Pairwise Master Keys (PMKs), LCOS LX access points experienced a memory shortage. As a result, an access point restarted abruptly.

→ The user name transmitted by a wireless client could be entered in the Wi-Fi station table with a maximum of 32 characters. Names with up to 64 characters are now possible.

→ A misbehavior in the bridge caused an access point to receive again an IP packet that it had sent itself. This meant that the access point could no longer be reached and, for example, lost the connection to a WLAN controller.

→ It was not possible to enter an LMC domain containing a number in WEBconfig (e.g. lmc.test1.de).

→ If a base speed was configured in the AP profile of a WLC, a speed of 1 Mbps was always used regardless of the configured value.

→ In the configuration of an access point, a network profile transmitted by the WLC remained empty if the configured Wi-Fi password contained a space character.

→ In a WLC scenario, the PMK of a wireless client was only transmitted to the WLC after about 25 seconds. As a result, roaming problems occurred.

→ If the CAPWAP service of an access point was unable to interpret the configuration transmitted by the WLAN controller (for example, due to an incorrect parameter), the access point did not report this to the WLAN controller. This meant that the WLAN controller kept sending the configuration to the access point until a timeout expired.
The CAPWAP service now sends an error message directly to the WLAN controller in case of an error.

→ The CAPWAP service in an access point could not process an ‘Update Request’ received from a WLAN controller with an empty ‘WTP Name’. This resulted in the access point no longer being able to be managed.

→ When using an ‘Untagged-VLAN’, packets from VLAN 1 (INTRANET) were also transmitted within this VLAN.

LCOS LX improvements 5.36.0129 SU2

Bugfixes / improvements

→ Security improvements due to an update of the OpenSSL version to 1.1.1t (CVE-2023-0286, CVE-2022-4304, CVE-2023-0215 and CVE-2022-4450)

LCOS LX improvements 5.36.0103 SU1

Bugfixes / improvements

→ Fixed CVE-2022-24810, CVE-2022-24809, CVE-2022-24808, CVE-2022-24807, CVE-2022-24806, and CVE-2022-24805.

LCOS LX improvements 5.36.0069 Rel

Bugfixes / improvements

→ A vulnerability in the zlib library has been fixed (CVE-2018-25032).

→ A vulnerability in the OpenSSL library has been fixed (CVE-2022-0778).

→ When an access point tried to connect to a LANCOM WLAN controller operating in a remote network, the connection could sporadically fail because the WLAN controller rejected the connection request due to a parameter in the DTLS protocol used that was unknown to the LCOS.

→ When a LANCOM WLAN controller tried to enable the 'Multicast-to-Unicast' function on a managed LANCOM LW-500, this failed because the LANCOM LW-500 did not use the correct Multicast protocol.

→ When using the Fast Roaming function, access points could sporadically restart without warning due to a memory leak.

→ An access point has different MAC addresses for the two Wi-Fi interfaces. In a WLAN controller scenario, the access points each reported the MAC address of a different Wi-Fi interface (WTP MAC) to the WLAN controller when adding and deleting Wi-Fi end devices, so that these did not match. This resulted in a discrepancy between the Wi-Fi end devices registered in the station table on the WLAN controller and the access points.

→ When trying to connect via LL2M with specification of the correct interface, it could happen that the specification of the interface was not recognized and the options available for LL2M were output instead. The connection setup via LL2M failed as a result.
→ If only one change was made to the netmask in the IP parameter profile in the LANCOM WLAN controller, the WLC transferred this change to the access point. The access point did not accept the change due to a missing comparison function (actual state/setpoint state) and continued to use the old netmask.
→ Sporadic packet loss could occur within a WLC tunnel.

LCOS LX improvements 5.36.0047 RC1

New Features

→ LL2M protocol support
→ Support for proxy ARP / ARP handling in wireless LAN
→ Untagged VLAN/access port configuration of additional Ethernet ports on access points

Bugfixes / improvements

→ RADIUS access requests in the context of a MAC address check are now provided with the RADIUS service type ‘Framed’ as well as with the attributes NAS port and NAS port ID.
→ In a WLAN controller scenario, when using a time frame for the wireless LAN profile in use, it could happen that the SSID was not correctly associated with the bridge after deactivation and subsequent activation of the wireless LAN profile by the time frame. This meant that Wi-Fi end devices could not obtain an IP address via DHCP and could not communicate via this access point.
→ If a WLAN controller and an access point are in different networks, the access point attempts to reach the WLAN controller via the DNS name ‚WLC-Address‘. If a DNS suffix was already stored in the configuration of the access point and the DNS suffix was also distributed by the WLAN controller, this resulted in the DNS suffix being appended to ‚WLC-Address‘ twice. As a result, the access point could no longer resolve the IP address of the WLAN controller and communication between the devices was no longer possible.

→ An access point attempts to reach a WLAN controller via the DNS name ‚WLC-Address' when the controller is located in another network. However, a DNS suffix assigned by the WLAN controller was not stored boot-persistently and was therefore no longer available after a reboot. This meant that the access point could no longer reach the WLAN controller if the DNS server only resolved ‚WLC-Address.DNS-Suffix'.

→ On the command line, found BLE beacons can be listed with the command 'ls st/lbs/ble'. However, it could happen that no BLE beacons were displayed in this list, although there were some in the vicinity of the access point.

→ In WEBconfig, improvements have been made to the function and display of a BLE scan.

→ Due to memory loss, the LANCOM LCOS LX access points could 'freeze' and stop working. Restarting the devices fixed the behavior until the next memory loss. This behavior occurred more frequently with devices of the LANCOM LW series (LW-500 & LW-600).

6. Known restrictions

→ When using both LAN ports for passing through data traffic only untagged data traffic or data traffic tagged with the management VLAN tag is passed through.
→ 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.

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
Adenauerstr. 20/B2
52146 Wuerselen | Germany
info@lancom.de
www.lancom-systems.com