Release Notes

# LCOS LX
## 6.20 RU1

Table of contents

LANCOM SYSTEMS

February 26th 2025, CBuersch

## 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 6.20 RU1, 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

**To update the AP model LANCOM LW-600 to LCOS LX 6.20, the migration firmware LCOS LX 6.14 RU2 must first be installed.**

**As part of security improvements, the negotiation of the DTLS protocol used for encrypting communication between WLCs and APs has been adapted. For this reason, at least LCOS version 10.80 RU3 is required on the WLC for WLC-managed operation of APs with LCOS LX 6.20.**

### LCOS LX - improvements 6.20.0139 RU1

**New features**

→ The attributes “framed-ip-address”, “framed-ipv6-address”, and “framed-ipv6-prefix” are now included in RADIUS accounting messages.

**Bug fixes**

→ It was possible to access the /assets/ directory and its subdirectories without first logging in as a user.

→ The IP address of the cloud-managed hotspot was only resolved once during the first connection. After changing the IP address of the cloud-managed hotspot, the access points could no longer reach it, meaning that the hotspot functionality was no longer available until the devices were restarted.
The cloud-managed hotspot is now resolved every five minutes.

→ When using the cloud-managed hotspot with an external captive portal and a specific port (e.g. :8443), the colon was not adopted. This meant that the captive portal could not be accessed.

→ If random channel selection was activated in each frequency band, this meant that the 6 GHz radio modules were not activated for SSIDs in which all three bands were used.

→ It could happen with the LANCOM LX-6400 and LX-6402 access points with hardware versions MOD-B00 and MOD-C00 that the 2.4 GHz radio on channel 5 had a permanently increased channel load.

→ It could happen with access points managed by the LMC that after a rollout in which an SSID was switched to inactive, not all SSIDs were taken over by the access point. As a result, some active SSIDs were not broadcast and could therefore not be used.

- Within an L2TP tunnel, the VLAN header was not removed for packets with certain sizes (16-byte steps - 1470 bytes, 1454 bytes etc.). Since WLAN clients can not process packets with VLAN headers, this led to severely restricted communication.
- A VLAN learned via Dynamic VLAN was not assigned to the L2TP interface in the bridge. This meant that clients connected via L2TP with Dynamic VLAN could not communicate via the L2TP tunnel.
- If the access point received an 'ICMP fragmentation needed' from the upstream gateway (because the client sent a packet that was too large via the L2TP tunnel), the access point terminated the L2TP tunnel.
- The access points only sent an 'ICMP fragmentation needed' via the LAN and WLAN interfaces, but not via an L2TP tunnel.
- When transmitting large packets, it could happen that the L2TP tunnel was broken down. In this case, the message "failed to send packet: Message too large" was displayed in an L2TP trace on the access point.
- If the IP parameters were assigned statically, the access point did not save the stored gateway. As a result, the access point could no longer communicate with the Internet (e.g. for time synchronization via NTP).
- If the 'Ant. gain mode' parameter in the access point table in the WLAN controller was set to 'User-defined' and the power reduction was also configured, the access point accepted these settings correctly.
  If the 'Ant. gain mode' was then set back to standard and the power reduction was deleted, the access point did not adopt these values, however, so that the previous values remained active.
- In a TACACS+ scenario, the spare server was also requested if the main server was available but refused the login. The spare server is now only requested if the main server is not available.
- After rolling out a new schedule to access points with LCOS LX, they remained permanently in test mode and the configuration could not be written. As a result, communication with the access points was not possible. The message "Check reachability" (after the first rollout attempt) or "Not accepted" (for further rollout attempts) was displayed in the LMC.
- The DHCP server of the LMC hotspot on an access point only supports IPv4. If the access point acted as a hotspot gateway and an IPv6 DNS server was assigned to it, the DHCP server on the access point rejected the DNS configuration. As a result, WLAN clients could not perform DNS resolution and the redirect to the hotspot did not work.
- In the '/Status/WLAN/Interfaces' path, the 'Beacon rate' value remained at 6 Mbps if another value was set which matched a value from the 'Supported rates' column (e.g. 12 Mbps).

- → In LCOS LX 6.20 Rel, the access points no longer sent the 'Host Name' in the DHCP request.
- → A device configuration downloaded via WEBconfig, which was changed after downloading, could not be loaded back into the device via WEBconfig.
- → If a WLAN client connected to a cloud-managed hotspot with an external captive portal but was not yet authenticated, the client could use the Internet without restrictions via IPv6 if the access point was also connected via IPv6 in addition to the blocked IPv4 (due to non-existent authentication).
- → When using TACACS+, a fallback to the local users takes place in the standard configuration if the TACACS+ server cannot be reached. However, the fallback to the local users also takes place if the TACACS+ server was accessible.

## LCOS LX - improvements 6.20.0078 Rel

### New features

**General**

→ Support for the TACACS+ protocol
→ Various improvements in the WEBconfig onboarding dialog
→ IEEE 802.3az / EEE is now configurable.
→ A separate IP/VLAN interface can be configured for Digital Signage / ESL.
→ The SSH host key length can be configured.
→ The message authenticator attribute can now be enforced in RADIUS messages.

**Wi-Fi**

→ Update of the wireless driver for increased stability and compatibility
→ Support of the LANCOM Sustainability Mode / Wi-Fi energy-saving mode with the LANCOM Management Cloud
→ The DTIM period is now configurable.
→ New Wi-Fi country settings: Canada, Liechtenstein
→ The 'Basic Rates' and 'Supported Rates' announced in Beacons are now configurable.
→ Random Wi-Fi channel selection can be configured.
→ Adjustment wizard for Wi-Fi antennas in WEBconfig

**LMC operation**

→ When using the LMC hotspot, the login status of the users is shared between the individual APs of the hotspot in the LAN to enable faster roaming.
→ Support for Frederix Hotspot

**WLC operation**

→ WLC scripts are now supported.
→ In WLC operation, L2TPv3 tunnels are now supported as an alternative to WLC L3 tunnels.
→ In active-active scenarios, the AC-IPv4-List element is now evaluated in order to learn further WLCs of the active-active cluster.

### Bugfixes / improvements

- If an SSID was configured with LEPS-MAC but no encryption was used for it, the blacklist or whitelist did not work.
- A security vulnerability in the UTF32Encoding.cpp of the POCO library has been fixed (CVE-2023-52389).
- If a LANCOM LX-6500(E) was operated via PoE and received too little power (802.3at), the second port was throttled to 100 Mbps. As a result, the LACP could no longer function, as the same port speeds are required here. However, the LACP was still displayed as active, although this was not the case.
- If the same VLAN ID was used in an SSID with Dynamic VLAN and in another SSID, the VLAN ID could not be assigned via Dynamic VLAN. This meant that communication was not possible in this SSID.
- If the command ‘set <profile name> ?’ was entered in an SSH console session in the path ‘Setup/WLAN/Rate-Selection’ (e.g. ‘set Network-Name ?’), this ended the session.
- In the detailed configuration of the LMC, it was not permitted to use a ‘#’ in the LEPS WPA passphrase, although this is permitted in LCOS LX.
- If several additional VLANs were added to a WDS connection, the connection subsequently lost its VLAN configuration. As a result, communication via the WDS connection was only possible to a very limited extent or not at all.
- It was not possible to set the value ‘Only-Without-WLC’ in the console path ‘Setup/LMC’.
- A security vulnerability in wpa_supplicant has been fixed (CVE-2023-52160).
- The antenna gain could only be set between 0 and 15 dBi. This was changed to 0 to max. 30 dBi.

- → For wireless clients connected to a network with a statically assigned VLAN ID, the VLAN ID was not displayed in the 'Status/WLAN/Station-Table' table.
- → The permitted 6 GHz channels for Bulgaria and Hungary were missing in the 'Status/WLAN/Channels-Allowed-By-Regulator' path.
- → When reading out an SNMPv2 MIB, the information for location and administrator name was not read out in the path 'Setup/Config/Location' and transferred to the MIB file.
- → With U-APSD activated, voice dropouts occurred during the roaming process when using Ascom wireless phones.
- → When using WDS without an additional SSID, the status 'off' was displayed in the console path 'Status/WLAN/Radios' for the Wi-Fi module with the WDS link.

## 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

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