

Release Notes

LCOS LX

6.20 Rel

Table of contents

02	1. Preface
02	2. The release tag in the software name
03	3. Device-specific compatibility to LCOS LX
03	4. Notes on LCOS LX
03	Information on default settings
03	5. Known restrictions
04	6. History LCOS LX
04	LCOS LX - improvements 6.20.0078 Rel
07	7. General notes
07	Disclaimer
07	Backing up the current configuration



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 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 features. 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 6.20.0078 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

Wi-Fi

- A security vulnerability in the RADIUS protocol (VU#456537) has been fixed.
- When connecting an LCOS LX access point to a LANCOM router as a supplicant, the router tries to send the access point an identity request as a unicast. The LCOS-LX access point could not interpret this and did not send a response.
- 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.

