Release Notes

LCOS LX

6.10 RU1

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 6.10 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 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 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 6.10.0042 RU1

Bugfixes / improvements

→ During the initial configuration rollout by the LMC, a device restart could occur if an automatic firmware update took place at the same time.

→ If the redirect mechanism to a private LMC instance was used for a zero-touch commissioning by the LMC, the LMC domain was removed from the configuration at the next device restart.

LCOS LX improvements 6.10.0040 Rel

New features

→ Preparation for LANCOM Active Radio Control 2.0

→ Support for point-to-point connections

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).

→ When using the 802.1X preauthentication function, the VLAN ID of a Wi-Fi client was not written to the cache and could then not be assigned when roaming to another access point.

→ If, for example, the country setting ‘Australia’ was used in a 6 GHz wireless network and channel 1 was set, an abrupt restart could occur. This behavior also occurred with other country settings.

→ If the CAPWAP connection to a LANCOM WLAN controller was terminated, all connected Wi-Fi clients were disconnected from the wireless network after the connection was re-established.

→ In a scenario where dynamic VLAN was used, blocking multicasts did not work.

→ When using OKC (Opportunistic Key Caching) in a WLC managed 802.1X network, no entry was created in the PMK SA cache if an ‘IAPP Handover Request’ contained a PMK (Pairwise Master Key).

→ When negotiating the WPA3 ‘4-Way handshake’ of a WDS connection (Wi-Fi point-to-point), it could happen that the ‘accesspoint’ generated a new PMK while the ‘station’ used an already existing PMK from the cache. This caused the ‘4-Way handshake’ to fail and the WDS connection could not be established.

→ The RADIUS backup server for an 802.1X wireless LAN was not used, so it was not possible to log on to the wireless LAN if the RADIUS server failed.

→ The channel scheme for the ‘Preferred Scanning Channels’ (PSC) in the 6 GHz band was not used. This meant that Wi-Fi end devices could not find the wireless LAN during a scan if they only scanned the PSC channels.

→ SNR (Signal-to-Noise Ratio) was used as the ‘Min. client signal strength’ in an SSID instead of RSSI (Received Signal Strength Indicator). Depending on the value used, it could happen that only ‘beacon’ packets could be transmitted in this SSID, but no ‘probe’ packets. As a result, Wi-Fi end devices could no longer register in the Wi-Fi network.

→ 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 wireless client login 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 resulted in either the login failing (when using FT) or the complete key negotiation having to be gone through again.

LCOS LX improvements 6.10.0011 RC1

New features

→ Support for WDS / point-to-point connections
→ Support for LACP
→ Support for L2TPv3
→ Support for client isolation
→ WLAN driver update for increased stability and compatibility
→ The list of SSH algorithms used has been adjusted. Supported are: curve25519-sha256, diffie-hellman-group14-sha256 (key exchange); ssh-ed25519, rsa-sha2-256 (host key algorithms); chacha20-poly1305, aes128-ctr, aes256-ctr (encryption); hmac-sha2-256 (MAC).

Bugfixes / improvements

→ When using Dynamic VLAN (RADIUS), the access point sent the 'LLC announcement' twice. Furthermore, the LLC announcements were already sent by the access point before the RADIUS negotiation was finished.
→ Preferred channels can be stored in the 'Channel list' (Setup/WLAN/Radio). During automatic channel selection, one channel is then selected from the list instead of all possible channels. However, the 'Channel list' was not taken into account, so that all channels could still be selected.
→ Although the 'Configuration-Via-DHCP' option was disabled in the '/Setup/LMC/' path, the LMC-DHCP option was evaluated.
→ In rare cases it could happen that a LANCOM LX access point managed via WLC displayed the LED blinking pattern of an unmanaged access point.

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