Release Notes

LCOS LX

6.12 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 6.12 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 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 6.12.0024 Rel

New features

→ Client mode for flexible network extensions and P2P routes
→ Re-design of the ‚System configuration' tab in WEBconfig
→ Adjustable speed for the Ethernet ports
→ Signaling in case of insufficient PoE power supply
→ Capture extension (Wi-Fi header can be optionally captured)
→ WLC configuration extensions

Bugfixes / improvements

→ 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.
→ 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 caused the WLAN controller to keep 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 the event of an error.
→ The console command 'startlmc' can be used in LCOS to pair with the LMC by specifying the serial number and the cloud pin. When executing the 'startlmc' command in LCOS LX, an activation code from the LMC was also requested by mistake.
→ The 'libcurl' program library has been updated to version 8.1.2 to fix vulnerabilities CVE-2023-27538, CVE-2023-27537, CVE-2023-27535, and CVE-2023-27536.
→ The packet capture feature was not available for WDS interfaces.
→ Channels 149, 153, 157 and 161 were limited to a bandwidth of 20 MHz. As a result, these channels could not be combined to form an 80 MHz bandwidth.
→ The trace function for the automatic firmware update did not generate any output because the log level of the trace message was not output.
→ When updating the firmware via the WEBconfig interface, an error message about a timeout appeared after some time, which had no meaning.
→ If the country USA was set in the Wi-Fi configuration and channel 13 was set for an SSID on WLAN-1, the access point restarted immediately.

→ The following issues in the BLE interface have been fixed:
- the BLE API returned incorrect RSSID values
- Access points stopped transmitting data to BLE sensors after some time
- transmitted payload data was sent in a non-valid JSON format

→ In the wireless network configuration (SSID), nothing could be entered in the table field ‘Maximum number of clients’ if the 6 GHz mode was used.

→ After executing the console command ‘beginscript’, certain subsequently executed commands (such as ‘ping’) were acknowledged with the message “Finished script successfully” or “Finished script with error (invalid command)”.

→ In LCOS LX 6.10 beacons were always sent with 6 Mbps, even if the ‘Beacon Rate’ was set to a different value.

→ If a large number of LEPS-U users (several hundred) were transferred from the WLAN controller to the access points in a WLAN controller scenario, the transfer stopped after some time because the access point calculated the preshared keys and this caused delays. Furthermore, the access points were subsequently no longer accessible in the network.
The LEPS configuration is now first transmitted from the WLAN controller to the access point and only then LEPS is activated, so that the calculation of the preshared keys takes place afterwards.

→ During a scan on the 6 GHz band, the channel bandwidth was always displayed as 20 MHz in the status tables ‘Status/WLAN/Environment-Scan-Results’ and ‘Status/WLAN/Competing-Networks’.

→ In an 802.1X scenario using FT (Fast Transition), PMK cache entries were missing when a Wi-Fi client repeatedly logged on via ‘FT Initial Mobility Domain Association’ to different Wi-Fi modules of an access point. Furthermore, the assignment between PMK and Wi-Fi module was not correct in the cache entry of the Wi-Fi module where the first login took place. As a result, the Wi-Fi client may have been rejected by the AP during a subsequent fast transition, and the key negotiation process had to be completely rerun.

→ Improvements in the area of dynamic assignment of a VLAN via RADIUS (Dynamic-VLAN):
- If a Wi-Fi client logged off from the wireless LAN and then logged on again a short time later, no VLAN ID was assigned to the Wi-Fi client.
- The first packet of a session with the ToS flag set was transmitted without the configured VLAN ID, so this packet was sent to the wrong network.

→ Wi-Fi clients were logged out of the wireless LAN after the RADIUS session timeout expired, instead of performing a new 802.1X authentication as in LCOS.

→ If a LANCOM LX-6400 / LX-6402 is powered via PoE with 802.3af, the access point operates with limited functionality (low power mode). In this case, the speed of the Ethernet port was fixed at 1 Gbps. This meant that the access point could not be used on a 100 Mbps switch.
In Low Power Mode, auto-negotiation with a maximum of 1 Gbps is now active for the Ethernet port.

→ If an SSID was reactivated by time frame in a WLAN controller scenario with WLC tunnel, WLAN clients could communicate with local networks via the bridge instead of only via the WLC tunnel.

→ If no PSK was stored for a LEPS MAC user, the VLAN ID entered could not be assigned to this user. This resulted in the user connecting to the wrong network.

Known issues

→ If several changes are made to the RADIUS client profile in Wi-Fi client mode with 802.1X authentication, the device does not always apply them correctly. The behavior can be remedied by restarting the access point.

→ If an antenna with a gain of more than 20 dBi is used, the access point correctly regulates the transmit power down. However, in the console path ‘Status/WLAN/Radios’ the values for ‘Transmit-Power’ and ‘EIRP’ are not displayed correctly.

→ When using 802.1X to authenticate Wi-Fi clients, the RADIUS server is addressed from the management network. If the management VLAN is changed, the access point does not recognize this and continues to use the previous management VLAN for the affected SSIDs, so that no communication with the RADIUS server is possible. For the new management VLAN to be used, the SSIDs with 802.1X authentication must be deactivated and then reactivated.

LCOS LX improvements 6.10.0043 RU2

Bugfixes / improvements

→ For access points managed via LMC, the wireless LAN was stopped after a Wi-Fi configuration change and then reinitialized. This resulted in the wireless LAN being unavailable for the duration of the reinitialization (max. 60 seconds).

→ In individual cases it could happen with LANCOM access points of the types LX-6200 and OW-602 that the channel load in both frequency bands permanently increased to 100 %. This meant that no beacons could be sent and the SSID was not visible to wireless clients.

→ 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 selectable data. Furthermore, the time frame in the menu ‘WLAN configuration - SSID’ could not be edited either.

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

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.

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

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

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

→ 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