RELEASE NOTES

LCOS LX

7.20 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 7.20.0087 Rel

06 **7. General notes**
06 Disclaimer
06 Backing up the current configuration

ROHDE&SCHWARZ
Make ideas real

1. Preface

The LCOS family of operating systems—LCOS, LCOS SX, LCOS LX, and LCOS FX—forms the trusted basis for the entire R&S®LANCOM range of products. Within the scope of the hardware specified by the products, the latest firmware version is available for all R&S®LANCOM products and is offered by Rohde & Schwarz Networks and Cybersecurity for download free of charge.

Rohde & Schwarz Networks and Cybersecurity keeps program libraries used in LCOS firmware up to date with the latest security patches and fixes security vulnerabilities even if they cannot be exploited in the firmware.

This document describes the innovations within LCOS LX software release 7.20 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.

2. The release tag in the software name

Release Candidate (RC)

A release candidate has been extensively tested by Rohde & Schwarz Networks and Cybersecurity 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 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 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

R&S®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 Lifecycle policies.

4. Notes on LCOS LX

Information on default settings

Devices delivered with LCOS LX automatically connect to the R&S®LANCOM Management Cloud (R&S®LMC). This functionality provides zero-touch installation for new devices. In case you do not want to use the R&S®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 R&S®LMC whenever you want.

5. Known restrictions

- Local configuration changes are not transferred to the R&S®LMC.
- The scripting of the device from the R&S®LMC is currently not supported, but the use of add-ins is.

6. History LCOS LX

LCOS LX - improvements 7.20.0087 Rel

For WLC-managed operation of an access point running LCOS LX 7.20, the R&S®LANCOM WLC must be running at least LCOS version 10.94.

New features

General

- The operational restrictions for the R&S®LANCOM LX-7400 with 802.3at PoE have been adjusted:
  - The Ethernet speed of ETH1 is limited to 1 Gbps
  - USB can not be used
  - 6 GHz Wi-Fi streams are reduced from 4x4 to 2x2

  Further restrictions do not apply.
- If a master device password or user passwords were manually created in the past using the outdated MD5 or DES hashing algorithms, they can no longer be used with LCOS LX 7.20 and above. In this case, reset the passwords **before the update**, for example, using LANconfig or the "passwd" command. The SHA256 hashing algorithm is used for this.

  Info: These outdated hashing methods could only be used at the user's explicit request; by default, all LCOS LX versions use the SHA256 algorithm.
- Additional administrators and separate user permissions can now be configured.
- Support for public key authentication in SSH
- Support for cron jobs for scheduling actions

Wi-Fi

- Support for the Wi-Fi end-to-end test for evaluation of the Wi-Fi networks performance by simulating a Wi-Fi client
- Revision of the client management for client distribution via 802.11k/v
- Support for a firewall to filter traffic to and from Wi-Fi networks at IP level, including DNS support
- Wi-Fi driver update for improved stability and compatibility

Bugfixes / improvements

- Fix for CVE-2026-98432
- When using an access point running LCOS LX version 7.12 or later on a WLAN controller running LCOS 10.94 with transmit power reduction configured, the reduction was not applied—the access point continued to transmit at full power.
- PoE negotiation via LLDP takes some time. As a result, the Wi-Fi service started before PoE negotiation via LLDP was completed. When LW-700, LX-7200, and LX-7400 were powered via PoE on a switch that, prior to PoE negotiation via LLDP, supplied only 802.3af at 15.4 W, this caused the access points' radio modules to fail to start after a reboot. The status of the modules remained ‚Module inactive'.
- If a tagged management VLAN was configured on an access point and the '802.1X Multi Auth' authentication

method was set on the switch port, 802.1X authentication failed.

- In a WLAN controller scenario, the access points report newly connected clients to the WLAN controller (add station event). In these reports, the interfaces were swapped. As a result, neither the correct total number of connected clients was reported to the WLAN controller (Status/WLAN Management/Client Count on the WLAN controller) nor the number of clients per Wi-Fi interface (Status/WLAN Management/AP Status/Active Radios on the WLAN Controller).
- In the 'Station Table' and 'IAPP Table' status tables and the 'Interfaces' table (all located in the console path 'Status/WLAN'), it was not possible to enter an empty SSID. When using a hidden SSID (closed network), this meant that the SSID could not be stored in the aforementioned tables. As a result, the 'Station Table' also contained no entries for clients connected to the hidden SSID.
- The DHCPv6 IAID (Identity Association Identifier) in DHCPv6 requests was generated randomly instead of being set statically.
- The DHCPv6 IAID is now generated based on the interface MAC address.
- The DHCPv6 client sent DHCPv6 solicit packets at very short intervals when no DHCPv6 server responded. The timer for sending DHCPv6 solicit packets is now counting up.
- When using a WLC tunnel with a VLAN, a Wi-Fi client could not be assigned a different VLAN via Dynamic VLAN. This resulted in the client gaining access to the wrong network.
- During a DHCP renewal, changes to the DNS servers were not applied.
- When powering an LX-7500 via dual-PoE, some 802.3at-compatible switches might cause the access point to no longer request 25.5 W on the second Ethernet port after a reboot, resulting in only 13 W being allocated. This led to limited functionality of the access point and prevented Wi-Fi broadcasting.
- If the hotspot table in the access point contained more than 512 entries, access via the web interface was no longer possible, and configuration rollouts via LMC also failed.
- If a 'Managed Address Configuration Flag' (M-Flag) was already present in the IPv6 Router Advertisement, the access point would ignore any 'Autonomous Address Configuration Flag' (A-Flag) that might be present. As a result, the access point could obtain an IPv6 address via DHCPv6 but could not generate its own IPv6 address via SLAAC for the prefixes.
- In a WLAN controller scenario, if a country was set that the access point did not support, the access point would set the country to Europe instead of rejecting the change.
  An access point without a Wi-Fi profile now sends a corresponding error message to the WLAN controller if the country setting is invalid, and the Wi-Fi signal is not broadcast.
  An access point with an existing Wi-Fi profile that includes a valid country setting will also send an error message to the WLAN controller if the country setting is changed to an invalid one. The Wi-Fi signal will continue to be broadcast using the previous valid country setting.
- ‚Client isolation' now also supports IPv6 and is therefore no longer limited to IPv4. However, gateways are not yet automatically detected based on router advertisements and DHCPv6 responses and must therefore be entered manually.
- On the R&S®LANCOM LW-600, packet capture in raw mode did not work due to hardware limitations and was therefore removed.

Rohde & Schwarz Networks and Cybersecurity GmbH
Adenauerstr. 20/B2
52146 Wuerselen | Germany
info.rs-nc@rohde-schwarz.com | www.rohde-schwarz.com/networks-and-cybersecurity

R&S and Rohde & Schwarz are trademarks of Rohde & Schwarz GmbH & Co. KG, registered or used, among others, in Germany, the EU, the USA, China, and other countries. Other names or designations used may be registered trademarks of different companies or owners. This document contains forward-looking statements regarding products and product features. The publisher reserves the right to change these at any time without stating reasons. No liability is accepted for technical inaccuracies or omissions.

ROHDE&SCHWARZ
Make ideas real

7. General notes

Disclaimer

Rohde & Schwarz Networks and Cybersecurity does not take any guarantee and liability for software not developed, manufactured or distributed by Rohde & Schwarz Networks and Cybersecurity, especially not for shareware and other extraneous software.

Backing up the current configuration

Before upgrading your R&S®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 Rohde & Schwarz Networks and Cybersecurity.

Rohde & Schwarz Networks and Cybersecurity GmbH
Adenauerstr. 20/B2
52146 Wuerselen | Germany
info.rs-nc@rohde-schwarz.com | www.rohde-schwarz.com/networks-and-cybersecurity

R&S and Rohde & Schwarz are trademarks of Rohde & Schwarz GmbH & Co. KG, registered or used, among others, in Germany, the EU, the USA, China, and other countries. Other names or designations used may be registered trademarks of different companies or owners. This document contains forward-looking statements regarding products and product features. The publisher reserves the right to change these at any time without stating reasons. No liability is accepted for technical inaccuracies or omissions.

ROHDE&SCHWARZ
Make ideas real